# Cisco IOS Quality of Service Solutions Command Reference

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2013 Cisco Systems, Inc. All rights reserved.

# CONTENTS


CHAPTER 1 **A through C** 1

access-list rate-limit 3

account 6

atm-address (qos) 8

attribute 10

auto discovery qos 11

auto qos 13

auto qos voip 15

auto qos voip (6500) 18

bandwidth (policy-map class) 22

bandwidth qos-reference 32

bandwidth remaining ratio 35

bump 40

bundle 44

bundle svc 46

class (EtherSwitch) 48

class (policy-map) 51

class-map arp-peruser 58

class-bundle 59

class-map 62

class-map arp-peruser 69

class type tag 70

clear control-plane 72

clear ip nbar 74

clear ip nbar protocol-discovery 76

clear ip rsvp authentication 78

clear ip rsvp counters 80

clear ip rsvp hello instance counters 82

clear ip rsvp hello instance statistics 84
clear ip rsvp hello statistics 86
clear ip rsvp high-availability counters 88
clear ip rsvp msg-pacing 89
clear ip rsvp reservation 91
clear ip rsvp sender 93
clear ip rsvp signalling fast-local-repair statistics 95
clear ip rsvp signalling rate-limit 96
clear ip rsvp signalling refresh reduction 97
clear mls qos 98
clear service-group traffic-stats 101
compression header ip 102
control-plane 104
copy interface 109
custom-queue-list 111

CHAPTER 2 D through F 115

default ip nbar protocol-pack 117
description (class-map) 118
description (service group) 120
df 121
disconnect qdm 122
drop 124
dscp 126
estimate bandwidth 129
exponential-weighting-constant 131
fair-queue (class-default) 133
fair-queue (DWFQ) 136
fair-queue (policy-map class) 139
fair-queue (WFQ) 141
air-queue aggregate-limit 148
fair-queue individual-limit 150
fair-queue limit 152
fair-queue qos-group 154
fair-queue tos 156

fair-queue weight 158
feedback 160
frame-relay interface-queue priority 162
frame-relay ip rtp compression-connections 165
frame-relay ip rtp header-compression 167
frame-relay ip rtp priority 169
frame-relay ip tcp compression-connections 173
frame-relay ip tcp header-compression 175
frame-relay map ip compress 177
frame-relay map ip nocompress 179
frame-relay map ip rtp header-compression 181
group (service group) 184
hw-module slot (ESP Scheduling) 186
hw-module subslot (Channelized SPA Scheduling) 189

CHAPTER 3 **identity policy policy-map through ip rsvp pq-profile 191**
identity policy (policy-map) 194
ingress-class-map 196
ip header-compression disable-feedback 198
ip header-compression max-header 200
ip header-compression max-period 202
ip header-compression max-time 204
ip header-compression recoverable-loss 206
ip header-compression old-iphc-comp 208
ip header-compression old-iphc-decomp 209
ip nbar attribute-map 210
ip nbar attribute-set 212
ip nbar classification tunneled-traffic 214
ip nbar custom 215
ip nbar pdlm 219
ip nbar port-map 221
ip nbar protocol-discovery 223
ip nbar protocol-pack 225
ip nbar resources 227
ip nbar resources protocol 228

ip nbar resources system 230
ip options 232
ip rsvp admission-control compression predict 234
ip rsvp aggregation ip 236
ip rsvp aggregation ip map 238
ip rsvp aggregation ip reservation dscp 241
ip rsvp aggregation ip role interior 244
ip rsvp atm-peak-rate-limit 246
ip rsvp authentication 248
ip rsvp authentication challenge 250
ip rsvp authentication key 252
ip rsvp authentication key-chain 254
ip rsvp authentication lifetime 256
ip rsvp authentication neighbor 258
ip rsvp authentication type 262
ip rsvp authentication window-size 264
ip rsvp bandwidth 266
ip rsvp bandwidth ignore 271
ip rsvp bandwidth percent 272
ip rsvp burst policing 275
ip rsvp data-packet classification none 276
ip rsvp dsbm candidate 278
ip rsvp dsbm non-resv-send-limit 280
ip rsvp flow-assist 282
ip rsvp layer2 overhead 284
ip rsvp listener 287
ip rsvp listener outbound 290
ip rsvp msg-pacing 293
ip rsvp neighbor 295
ip rsvp policy cops minimal 297
ip rsvp policy cops report-all 298
ip rsvp policy cops servers 300
ip rsvp policy cops timeout 302
ip rsvp policy default-reject 303
ip rsvp policy identity 305

ip rsvp policy local 308
ip rsvp policy preempt 316
ip rsvp policy vrf 317
ip rsvp pq-profile 320

CHAPTER 4 **ip rsvp precedence through load protocol 323**

ip rsvp precedence 325
ip rsvp qos 328
ip rsvp reservation 329
ip rsvp reservation-host 333
ip rsvp resource-provider 337
ip rsvp sender 339
ip rsvp sender-host 342
ip rsvp signalling dscp 345
ip rsvp signalling fast-local-repair notifications 347
ip rsvp signalling fast-local-repair rate 349
ip rsvp signalling fast-local-repair wait-time 351
ip rsvp signalling hello (configuration) 353
ip rsvp signalling hello (interface) 354
ip rsvp signalling hello dscp 356
ip rsvp signalling hello graceful-restart 358
ip rsvp signalling hello graceful-restart dscp 360
ip rsvp signalling hello graceful-restart mode 362
ip rsvp signalling hello graceful-restart mode help-neighbor 364
ip rsvp signalling hello graceful-restart neighbor 366
ip rsvp signalling hello graceful-restart refresh interval 368
ip rsvp signalling hello graceful-restart refresh misses 370
ip rsvp signalling hello graceful-restart send 372
ip rsvp signalling hello refresh interval 374
ip rsvp signalling hello refresh misses 376
ip rsvp signalling hello reroute dscp 378
ip rsvp signalling hello reroute refresh interval 380
ip rsvp signalling hello reroute refresh misses 382
ip rsvp signalling hello statistics 384
ip rsvp signalling initial-retransmit-delay 385

ip rsvp signalling patherr state-removal 386
ip rsvp signalling rate-limit 388
ip rsvp signalling refresh interval 390
ip rsvp signalling refresh misses 392
ip rsvp signalling refresh reduction 394
ip rsvp signalling refresh reduction ack-delay 396
ip rsvp snooping 397
ip rsvp source 399
ip rsvp svc-required 401
ip rsvp tos 403
ip rsvp transport 406
ip rsvp transport sender-host 408
ip rsvp tunnel overhead-percent 410
ip rsvp udp-multicasts 412
ip rsvp udp neighbor 414
ip rtp compression-connections 416
ip rtp header-compression 418
ip rtp priority 422
ip tcp compression-connections 426
ip tcp header-compression 428
iphc-profile 431
lane client qos 435
lane qos database 437
load protocol 439

CHAPTER 5 **match access-group through mls ip pbr 443**
mac packet-classify 446
mac packet-classify use vlan 448
map ip 450
map ipv6 453
map mpls 455
match access-group 457
match application (class-map) 461
match any 465
match atm-clp 467

match atm oam 469
match atm-vci 471
match class-map 473
match cos 476
match cos inner 479
match destination-address mac 481
match discard-class 483
match dscp 485
match field 488
match flow pdp 491
match fr-dlci 493
match input vlan 495
match input-interface 499
match ip dscp 502
match ip precedence 503
match ip rtp 504
match mpls experimental 506
match mpls experimental topmost 509
match not 511
match packet length (class-map) 513
match port-type 516
match precedence 518
match protocol 522
match protocol attribute application-group 536
match protocol attribute category 539
match protocol attribute encrypted 541
match protocol attribute sub-category 543
match protocol attribute tunnel 546
match protocol (NBAR) 548
match protocol citrix 649
match protocol fasttrack 651
match protocol gnutella 653
match protocol http 655
match protocol pppoe-discovery 661
match protocol rtp 663

match qos-group 665
match source-address mac 668
match start 670
match tag (class-map) 673
match vlan (QoS) 674
match vlan inner 676
maximum (local policy) 678
maximum bandwidth ingress 680
maximum bandwidth percent 682
maximum header 684
max-reserved-bandwidth 686
metadata application-params 690
metadata flow 693
metadata flow (troubleshooting) 695
mls ip pbr 697

CHAPTER 6 mls qos global configuration mode through mpls experimental 699
mls qos (global configuration mode) 701
mls qos (interface configuration mode) 703
mls qos 10g-only 704
mls qos aggregate-policer 706
mls qos bridged 710
mls qos channel-consistency 711
mls qos cos 712
mls qos cos-mutation 715
mls qos dscp-mutation 716
mls qos exp-mutation 717
mls qos loopback 718
mls qos map 719
mls qos map cos-dscp 722
mls qos map cos-mutation 724
mls qos map dscp-cos 726
mls qos map dscp-exp 728
mls qos map dscp-mutation 730
mls qos map exp-dscp 732

mls qos map exp-mutation 734
mls qos map ip-prec-dscp 736
mls qos map policed-dscp 738
mls qos marking ignore port-trust 740
mls qos marking statistics 741
mls qos mpls trust experimental 742
mls qos police redirected 744
mls qos police serial 745
mls qos protocol 746
mls qos queueing-only 749
mls qos queue-mode mode-dscp 751
mls qos rewrite ip dscp 752
mls qos statistics-export (global configuration) 754
mls qos statistics-export (interface configuration) 755
mls qos statistics-export aggregate-policer 757
mls qos statistics-export class-map 759
mls qos statistics-export delimiter 762
mls qos statistics-export destination 763
mls qos statistics-export interval 766
mls qos supervisor 10g-only 768
mls qos trust 770
mls qos trust extend 773
mls qos tunnel gre input uniform-mode 775
mls qos vlan-based 776
monitor pids 778
mpls experimental 779

CHAPTER 7 N through P 783

non-tcp 785
non-tcp contexts 786
oam-bundle 788
platform ip features sequential 791
platform ipsec fips-mode 794
platform ipsec llq 795
platform punt-police queue 796

platform qos marker-statistics 799
platform qos match-statistics per-ace 801
platform qos match-statistics per-filter 803
platform vfi dot1q-transparency 805
plim qos input 807
plim qos input map 810
plim qos input map cos (classify CoS values for VLAN) 815
police 819
police (EtherSwitch) 829
police (percent) 831
police (policy map) 840
police (two rates) 848
police rate (control-plane) 855
police rate pdp 861
policy-map 865
policy-map copp-peruser 872
precedence 873
precedence (WRED group) 876
preempt-priority 879
priority 881
priority (10000 series) 885
priority (SIP400) 888
priority-group 891
priority level 894
priority-list default 896
priority-list interface 898
priority-list protocol 900
priority-list queue-limit 905
priority-queue cos-map 907
priority-queue queue-limit 909
pvc-bundle 911

CHAPTER 8 Q through R 915

qos police order parent-first 917
qos pre-classify 918

qos shape-timer 920
queue-depth 922
queue-limit 924
queue-limit atm clp 929
queue-list default 931
queue-list interface 933
queue-list lowest-custom 935
queue-list protocol 937
queue-list queue byte-count 940
queue-list queue limit 942
random-detect 944
random-detect (per VC) 949
random-detect aggregate 953
random-detect atm-clp-based 956
random-detect clp 958
random-detect cos-based 960
random-detect discard-class 962
random-detect discard-class-based 966
random-detect dscp 967
random-detect dscp (aggregate) 975
random-detect ecn 980
random-detect exponential-weighting-constant 981
random-detect flow 985
random-detect flow average-depth-factor 987
random-detect flow count 989
random-detect prec-based 991
random-detect precedence 993
random-detect precedence (aggregate) 998
random-detect-group 1002
rate-limit 1005
rcv-queue bandwidth 1010
rcv-queue cos-map 1012
rcv-queue queue-limit 1014
rcv-queue random-detect 1016
rcv-queue threshold 1018

recoverable-loss 1021
redirect interface 1023
refresh max-period 1025
refresh max-time 1027
refresh rtp 1029
rtp 1031

CHAPTER 9 send qdm message through show atm bundle svc statistics 1033

send qdm message 1035
service-group 1037
service-policy 1038
service-policy (class-map) 1048
service-policy (control-plane) 1050
service-policy (policy-map class) 1053
service-policy (service group) 1056
service-policy type qos 1057
set atm-clp 1059
set cos 1061
set cos cos-inner (policy-map configuration) 1065
set cos-inner 1068
set cos-inner cos 1070
set discard-class 1072
set dscp 1074
set fr-de 1078
set ip dscp 1080
set ip dscp (policy-map configuration) 1081
set ip dscp tunnel 1084
set ip precedence (policy-map configuration) 1086
set ip precedence (policy-map) 1089
set ip precedence (route-map) 1090
set ip precedence tunnel 1093
set ip tos (route-map) 1095
set precedence 1098
set qos-group 1102
set vlan inner 1106

shape 1107
shape (percent) 1110
shape (policy-map class) 1114
shape adaptive 1120
shape fecn-adapt 1122
shape max-buffers 1124
show access-lists rate-limit 1126
show atm bundle 1128
show atm bundle stat 1130
show atm bundle svc 1132
show atm bundle svc stat 1134

CHAPTER 10 **show auto discovery qos through show ip rsvp hello client lsp detail** 1137

show auto discovery qos 1139
show auto qos 1143
show class-map 1148
show class-map type nat 1151
show class-map type port-filter 1153
show control-plane cef-exception counters 1155
show control-plane cef-exception features 1157
show control-plane counters 1159
show control-plane features 1161
show control-plane host counters 1163
show control-plane host features 1165
show control-plane host open-ports 1167
show control-plane transit counters 1169
show control-plane transit features 1171
show cops servers 1173
show crypto eng qos 1174
show crypto entropy status 1175
show frame-relay ip rtp header-compression 1177
show frame-relay ip tcp header-compression 1182
show interfaces fair-queue 1185
show interfaces random-detect 1188
show interfaces rate-limit 1191

show iphc-profile 1194
show ip nat translations rsvp 1196
show ip nbar attribute 1198
show ip nbar link-age 1200
show ip nbar pdlm 1202
show ip nbar port-map 1203
show ip nbar protocol activated 1205
show ip nbar protocol-attribute 1206
show ip nbar protocol-discovery 1208
show ip nbar protocol-id 1212
show ip nbar protocol-pack 1224
show ip nbar resources flow 1226
show ip nbar statistics 1227
show ip nbar trace 1228
show ip nbar unclassified-port-stats 1230
show ip nbar version 1233
show ip rsvp 1236
show ip rsvp aggregation ip 1244
show ip rsvp aggregation ip endpoints 1248
show ip rsvp atm-peak-rate-limit 1252
show ip rsvp authentication 1254
show ip rsvp counters 1261
show ip rsvp counters state teardown 1265
show ip rsvp fast bw-protect 1267
show ip rsvp fast detail 1270
show ip rsvp fast-reroute 1275
show ip rsvp fast-reroute bw-protect 1279
show ip rsvp fast-reroute detail 1283
show ip rsvp hello 1289
show ip rsvp hello client lsp detail 1291

CHAPTER 11 **show ip rsvp hello client lsp summary through show lane qos database** 1293

show ip rsvp hello client lsp summary 1295
show ip rsvp hello client nbr detail 1297
show ip rsvp hello client neighbor detail 1300

show ip rsvp hello client neighbor summary 1303
show ip rsvp hello graceful-restart 1305
show ip rsvp hello instance detail 1308
show ip rsvp hello instance summary 1312
show ip rsvp hello statistics 1315
show ip rsvp high-availability counters 1317
show ip rsvp high-availability database 1323
show ip rsvp high-availability summary 1342
show ip rsvp host 1347
show ip rsvp host vrf 1351
show ip rsvp ingress 1353
show ip rsvp installed 1355
show ip rsvp interface 1366
show ip rsvp interface detail 1384
show ip rsvp listeners 1387
show ip rsvp neighbor 1390
show ip rsvp p2mp counters 1394
show ip rsvp policy 1396
show ip rsvp policy cops 1398
show ip rsvp policy identity 1399
show ip rsvp policy local 1402
show ip rsvp policy vrf 1409
show ip rsvp precedence 1412
show ip rsvp request 1414
show ip rsvp reservation 1422
show ip rsvp sbm 1433
show ip rsvp sender 1436
show ip rsvp signalling 1467
show ip rsvp signalling blockade 1470
show ip rsvp signalling fast-local-repair 1474
show ip rsvp signalling rate-limit 1480
show ip rsvp signalling refresh 1482
show ip rsvp snooping 1484
show ip rsvp tos 1485
show ip rsvp transport 1487

show ip rsvp transport sender 1490
show ip rtp header-compression 1493
show ip tcp header-compression 1496
show ip vrf 1500
show lane qos database 1504

CHAPTER 12 show mls qos through wrr-queue threshold 1507

show metadata application table 1510
show metadata flow 1512
show mls qos 1519
show mls qos aggregate policer 1524
show mls qos free-agram 1526
show mls qos interface 1527
show mls qos maps 1529
show mls qos mpls 1533
show mls qos protocol 1536
show mls qos queuing interface 1538
show mls qos statistics-export info 1542
show platform hardware acl entry global-qos 1544
show platform hardware pp active infrastructure pi npd rx policer 1546
show platform hardware qfp active feature qos config global 1548
show platform lowq 1550
show platform qos policy-map 1551
show platform software infrastructure punt statistics 1554
show policy-manager events 1556
show policy-manager policy 1558
show policy-map 1560
show policy-map class 1576
show policy-map control-plane 1578
show policy-map interface 1582
show policy-map interface brief 1631
show policy-map interface service group 1640
show policy-map interface service instance 1642
show policy-map mgre 1647
show policy-map multipoint 1650

show policy-map session 1652
show policy-map target service-group 1660
show policy-map type access-control 1662
show policy-map type nat 1665
show policy-map type port-filter 1667
show protocol phdf 1670
show qbm client 1672
show qbm pool 1674
show qdm status 1677
show queue 1679
show queueing 1685
show queueing interface 1692
show random-detect-group 1697
show running-config service-group 1700
show service-group 1702
show service-group interface 1705
show service-group state 1707
show service-group stats 1708
show service-group traffic-stats 1711
show subscriber policy ppm-shim-db 1713
show table-map 1714
show tech-support nbar platform 1716
show tech-support rsvp 1730
show traffic-shape 1732
show traffic-shape queue 1735
show traffic-shape statistics 1740
show vrf 1743
show wrr-queue 1747
subscriber accounting accuracy 1748
svc-bundle 1749
table-map (value mapping) 1750
tcp 1753
tcp contexts 1754
traffic-shape adaptive 1756
traffic-shape fecn-adapt 1758

traffic-shape group 1760
traffic-shape rate 1763
trust 1766
tx-ring-limit 1768
vbr-nrt 1770
vc-hold-queue 1774
wrr-queue bandwidth 1776
wrr-queue cos-map 1778
awrr-queue dscp-map 1780
wrr-queue queue-limit 1782
wrr-queue random-detect 1784
wrr-queue threshold 1786

# A through C


- access-list rate-limit, page 3
- account, page 6
- atm-address (qos), page 8
- attribute, page 10
- auto discovery qos, page 11
- auto qos, page 13
- auto qos voip, page 15
- auto qos voip (6500), page 18
- bandwidth (policy-map class), page 22
- bandwidth qos-reference, page 32
- bandwidth remaining ratio, page 35
- bump, page 40
- bundle, page 44
- bundle svc, page 46
- class (EtherSwitch), page 48
- class (policy-map), page 51
- class-map arp-peruser, page 58
- class-bundle, page 59
- class-map, page 62
- class-map arp-peruser, page 69
- class type tag, page 70
- clear control-plane, page 72
- clear ip nbar, page 74
- clear ip nbar protocol-discovery, page 76

- clear ip rsvp authentication, page 78
- clear ip rsvp counters, page 80
- clear ip rsvp hello instance counters, page 82
- clear ip rsvp hello instance statistics, page 84
- clear ip rsvp hello statistics, page 86
- clear ip rsvp high-availability counters, page 88
- clear ip rsvp msg-pacing, page 89
- clear ip rsvp reservation, page 91
- clear ip rsvp sender, page 93
- clear ip rsvp signalling fast-local-repair statistics, page 95
- clear ip rsvp signalling rate-limit, page 96
- clear ip rsvp signalling refresh reduction, page 97
- clear mls qos, page 98
- clear service-group traffic-stats, page 101
- compression header ip, page 102
- control-plane, page 104
- copy interface, page 109
- custom-queue-list, page 111

# access-list rate-limit

To configure an access list for use with committed access rate (CAR) policies, use the **access-listrate-limit**command in global configuration mode. To remove the access list from the configuration, use the **no** form of this command.

**access-list rate-limit** *acl-index* {*precedence*| *mac-address*| *exp*| **mask** *mask*}

**no access-list rate-limit** *acl-index* {*precedence*| *mac-address*| *exp*| **mask** *mask*}

## Syntax Description

| | |
|---|---|
| *acl-index* | Access list number. To classify packets by<br>• IP precedence, use any number from 1 to 99<br>• MAC address, use any number from 100 to 199<br>• Multiprotocol Label Switching (MPLS) experimental field, use any number from 200 to 299 |
| *precedence* | IP precedence. Valid values are numbers from 0 to 7. |
| *mac-address* | MAC address. |
| *exp* | MPLS experimental field. Valid values are numbers from 0 to 7. |
| **mask** *mask* | Mask. Use this option if you want to assign multiple IP precedences or MPLS experimental field values to the same rate-limit access list. |

## Command Default

No CAR access lists are configured.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.1CC | This command was introduced. |
| 12.1(5)T | This command now includes an access list based on the MPLS experimental field. |
| 12.2(2)T | This command was integrated into Cisco IOS Release 12.2(2)T. |

| Release | Modification |
|---|---|
| 12.2(4)T | This command was implemented on the Cisco MGX 8850 switch and the MGX 8950 switch with a Cisco MGX RPM-PR card. |
| 12.2(4)T2 | This command was implemented on the Cisco 7500 series. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use this command to classify packets by the specified IP precedence, MAC address, or MPLS experimental field values for a particular CAR access list. You can then apply CAR policies, using the **rate-limit** command, to individual rate-limit access lists. When packets in an access list are classified in this manner, the packets with different IP precedences, MAC addresses, or MPLS experimental field values are treated differently by the CAR process.

You can specify only one command for each rate-limit access list. If you enter this command multiple times using the same access list number, the new command overwrites the previous command.

Use the **mask** keyword to assign multiple IP precedences or MPLS experimental field values to the same rate-limit list. To ascertain the **mask** value, perform the following steps.

1. Decide which precedences you want to assign to this rate-limit access list.
2. Convert the precedences or MPLS experimental field values into 8-bit numbers with each bit corresponding to one value. For example, an MPLS experimental field value of 0 corresponds to 00000001; 1 corresponds to 00000010; 6 corresponds to 01000000; and 7 corresponds to 10000000.
3. Add the 8-bit numbers for the selected MPLS experimental field values. For example, the mask for MPLS experimental field values 1 and 6 is 01000010.
4. The **access-listrate-limit** command expects hexadecimal format. Convert the binary mask into the corresponding hexadecimal number. For example, 01000010 becomes 42 and is used in the command. Any packets that have an MPLS experimental field value of 1 or 6 will match this access list.

A mask of FF matches any precedence, and 00 does not match any precedence.

## Examples

In the following example, MPLS experimental fields with the value of 7 are assigned to the rate-limit access list 200:

```
Router(config)# access-list rate-limit 200 7
```

You can then use the rate-limit access list in a **rate-limit** command so that the rate limit is applied only to packets matching the rate-limit access list.

```
Router(config)# interface atm4/0.1 mpls
Router(config-if)# rate-limit input access-group rate-limit 200 8000 8000 8000
conform-action set-mpls-exp-transmit 4 exceed-action set-mpls-exp-transmit 0
```

## Related Commands

| Command | Description |
|---|---|
| **rate-limit** | Configures CAR and DCAR policies. |
| **show access-lists rate-limit** | Displays information about rate-limit access lists. |

# account

To enable collection of statistics for packets matching the traffic class where this command is configured, use the **account** command in policy-map class configuration mode. To disable statistics collection, use the **no** form of this command.

**account [drop]**

**no account**

## Syntax Description

| | |
|---|---|
| **drop** | (Optional) Enables the collection of statistics for packets dropped for the traffic class where it is configured. This is the default behavior. |

## Command Default

When the **account** command is configured, the default behavior is collection of drop statistics. No statistics are collected if the **account** command is not configured.

## Command Modes

Policy-map class (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 2.6 | This command was introduced. |

## Usage Guidelines

The **account** command was implemented as part of the QoS: Policies Aggregation Enhancements feature in Cisco IOS XE Release 2.6 on the Cisco ASR 1000 Series Aggregation Services Routers to support the collection of per-subscriber statistics.

By default when configured, the command enables collection of drop statistics for traffic in the class where it is configured. Therefore, the optional **drop** keyword is not required to enable collection of drop statistics.

You can display the subscriber statistics collected for a certain traffic class using the **showpolicy-mapinterface** command.

## Examples

The following example shows enabling of drop statistics collection (the default) for the EF traffic class for the subscriber policy-map:

```
Router(config)# policy-map subscriber
Router(config-pmap)# class EF
Router(config-pmap-c)# account
```

## Related Commands

| Command | Description |
|---|---|
| **class (policy-map)** | Specifies the name of the class whose policy you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy. |
| **policy-map** | Enters policy-map configuration mode and creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **show policy-map interface** | Displays the statistics and the configurations of the input and output policies that are attached to an interface. |

# atm-address (qos)

To specify the QoS parameters associated with a particular ATM address, use the **atm-address** command in LANE QoS database configuration mode. To revert to the default value, use the **no** form of this command.

**atm-address** *atm-address* [**ubr**+ **pcr** *value* **mcr** *value*]

**no atm-address** *atm-address* [**ubr**+ **pcr** *value* **mcr** *value*]

## Syntax Description

| | |
|---|---|
| *atm-address* | Control ATM address. |
| **ubr+** | (Optional) Unspecified bit rate plus virtual channel connection (VCC). |
| **pcr** | (Optional) Peak cell rate (PCR). |
| *value* | (Optional) UBR+ pcr value in kbps. |
| **mcr** *value* | (Optional) Minimum cell rate (MCR) value in kbps |

## Command Default

No default ATM address.

## Command Modes

LANE QoS database configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(2)E | This command was introduced. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Examples

The following example shows how to enter the required QoS parameters using PCR and MCR values on a specific ATM address. This command is entered from LANE QoS database configuration mode.

```
Router(lane-qos)# atm-address 47.009181000000061705B0C01.00E0B0951A40.0A ubr+ pcr 500000
mcr 100000
```

## Related Commands

| Command | Description |
|---|---|
| **lane client qos** | Applies a QoS over LANE database to an interface. |
| **lane qos database** | Begins the process of building a QoS over LANE database. |
| **show lane qos database** | Displays the contents of a specific QoS over LANE database. |
| **ubr+ cos** | Maps a CoS value to a UBR+ VCC. |

# attribute

To add attributes to an attribute profile, use the **attribute** command in attribute map configuration mode.

**attribute** *attribute-name attribute-value*

## Syntax Description

| | |
|---|---|
| *attribute-name* | Name of the attribute that you want to configure for your profile. |
| *attribute-value* | Value of the attribute. |

## Command Modes

Attribute map configuration (config-attribute-map)

## Command History

| Release | Modification |
|---|---|
| 15.2(4)M2 | This command was introduced. |
| Cisco IOS XE Release 3.8S | This command was integrated into Cisco IOS XE Release 3.8S. |

## Usage Guidelines

This command does not have a **no** form.

## Examples

The following example shows how to add application-group attributes for your profile:

```
Device# configure terminal
Device(config)# ip nbar attribute-map nntp-attrib
Device(config-attribute-map)# attribute application-group aol-group
Device(config-attribute-map)# end
```

## Related Commands

| Command | Description |
|---|---|
| **ip nbar attribute-map** | Configures attributes for protocols. |
| **ip nbar attribute-set** | Attaches a new attribute profile to a protocol. |

# auto discovery qos

To begin discovering and collecting data for configuring the AutoQoS for the Enterprise feature, use the **autodiscoveryqos** command in interface configuration mode. To stop discovering and collecting data, use the **no** form of this command.

**auto discovery qos [trust]**

**no auto discovery qos**

## Syntax Description

| | |
|---|---|
| **trust** | (Optional) Indicates that the differentiated services code point (DSCP) markings of a packet are trust (that is, relied on) for classification of the voice, video, and data traffic.<br>If the optional **trust** keyword is not specified, the voice, video, and data traffic is classified using network-based application recognition (NBAR), and the packets are marked with the appropriate DSCP value. |

## Command Default

No data collection is performed.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(7)T | This command was introduced. |
| 12.3(11)T | The trust mode was modified to classify packets by DSCP value rather than by protocol type. |

## Usage Guidelines

The **autodiscoveryqos** command initiates the Auto-Discovery (data collection) phase of the AutoQoS for the Enterprise feature. This command invokes NBAR protocol discovery to collect data and analyze the traffic at the egress direction of the interface.

The **noautodiscoveryqos**command terminates the Auto-Discovery phase and removes any data collection reports generated.

The **trust** keyword is used for the trusted model based on the specified DSCP marking. For more information, see the “Trusted Boundary” section of the *AutoQoS for the Enterprise* feature module, Cisco IOS Release 12.3(7)T.

## Examples

The following is a sample configuration showing the Auto-Discovery (data collection) phase of the AutoQoS for the Enterprise feature enabled on a serial2/1/1 subinterface.

```
Router> enable
Router# configure terminal
Router(config)# interface serial2/1.1
Router(config-if)# frame-relay interface-dlci 58
Router(config-if)# auto discovery qos
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **auto qos** | Installs the QoS class maps and policy maps created by the AutoQoS for the Enterprise feature. |
| **service policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **show auto qos** | Displays the interface configurations, policy maps, and class maps created by AutoQoS on a specific interface or all interfaces. |

# auto qos

To install the quality-of-service (QoS) class maps and policy maps created by the AutoQoS for the Enterprise feature, use the **autoqos** command in interface configuration mode. To remove the QoS policies, use the **no** form of this command.

**auto qos**

**no auto qos**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No QoS policies are installed.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.3(7)T | This command was introduced. |

## Usage Guidelines

The class maps and policy maps are created from the templates that are automatically generated by the AutoQoS for the Enterprise feature. These templates (and the resulting class maps and policy maps) are generated on the basis of the data collected during the Auto-Discovery phase of the AutoQoS for the Enterprise feature. For more information about the Auto-Discovery phase, see the "Configuration Phases" section of the *AutoQoS for the Enterprise* feature module, Cisco IOS Release 12.3(7)T.

The **noautoqos** command removes any AutoQoS-generated class maps and policy maps installed on the interface.

The**autoqos** command is not supported on gigabit interfaces.

## Examples

The following is a sample configuration showing the AutoQoS for the Enterprise feature enabled on a serial2/1/1 subinterface. In this configuration, the AutoQoS class maps and policy maps will be installed on the serial2/1 interface.

```
Router> enable
Router# configure terminal
Router(config)# interface serial2/1
Router(config-if)# frame-relay interface-dlci 58
Router(config-if)# auto qos
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **service policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **show auto qos** | Displays the interface configurations, policy maps, and class maps created by AutoQoS on a specific interface or all interfaces. |

# auto qos voip

To configure the AutoQoS--VoIP feature on an interface, use the **autoqosvoip** command in interface configuration mode or Frame Relay DLCI configuration mode. To remove the AutoQoS--VoIP feature from an interface, use the **no** form of this command.

**auto qos voip [trust] [fr-atm]**

**no auto qos voip [trust] [fr-atm]**

## Syntax Description

| | |
|---|---|
| **trust** | (Optional) Indicates that the differentiated services code point (DSCP) markings of a packet are trusted (relied on) for classification of the voice traffic. If the optional **trust** keyword is not specified, the voice traffic is classified using network-based application recognition (NBAR), and the packets are marked with the appropriate DSCP value. |
| **fr-atm** | (Optional) Enables the AutoQoS--VoIP feature for Frame-Relay-to-ATM links. This option is available on the Frame Relay data-link connection identifiers (DLCIs) for Frame-Relay-to-ATM interworking only. |

## Command Default

Default mode is disabled.

## Command Modes

Interface configuration (config-if) Frame Relay DLCI configuration (for use with Frame Relay DLCIs) (config-fr-dlci)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

To enable the AutoQoS--VoIP feature for Frame-Relay-to-ATM interworking, the **fr-atm**keyword must be configured explicitly. However, the **fr-atm** keyword affects low-speed DLCIs *only* . It does not affect high-speed DLCIs.

**Note** DLCIs with link speeds lower than or equal to 768 kbps are considered low-speed DLCIs; DLCIs with link speeds higher than 768 kbps are considered high-speed DLCIs.

Depending on whether the **trust** keyword has been configured for this command, the AutoQoS--VoIP feature automatically creates one of the following two policy maps:

- "AutoQoS-Policy-Trust" (created if the **trust** keyword is configured)
- "AutoQoS-Policy-UnTrust" (created if the **trust** keyword is *not* configured)

Both of these policy maps are designed to handle the Voice over IP (VoIP) traffic on an interface or a permanent virtual circuit (PVC) and can be modified to suit the quality of service (QoS) requirements of the network. To modify these policy maps, use the appropriate Cisco IOS command.

These policy maps should not be attached to an interface or PVC by using the **service-policy** command. If the policy maps are attached in this manner, the AutoQoS--VoIP feature (that is, the policy maps, class maps, and access control lists [ACLs]) will not be removed properly when the**noautoqosvoip** command is configured.

For low-speed Frame Relay DLCIs that are interconnected with ATM PVCs in the same network, the **fr-atm** keyword must be explicitly configured in the **autoqosvoip** command to configure the AutoQoS--VoIP feature properly. That is, the command must be configured as **autoqosvoipfr-atm**.

For low-speed Frame Relay DLCIs that are configured with Frame-Relay-to-ATM, Multilink PPP (MLP) over Frame Relay (MLPoFR) is configured automatically. The subinterface must have an IP address. When MLPoFR is configured, this IP address is removed and put on the MLP bundle. The AutoQoS--VoIP feature must also be configured on the ATM side by using the **autoqosvoip** command.

The **autoqosvoip**command is not supported on subinterfaces or gigabit interfaces.

The **autoqosvoip** command is available for Frame Relay DLCIs.

**Disabling AutoQoS--VoIP**

The **noautoqosvoip** command disables the AutoQoS--VoIP feature and removes the configurations associated with the feature.

When the **noautoqosvoip** command is used, the **no** forms of the individual commands originally generated by the AutoQoS--VoIP feature are configured. With the use of individual **no** forms of the commands, the system defaults are reinstated. The **no** forms of the commands will be applied just as if the user had entered the commands individually. As the configuration reinstating the default setting is applied, any messages resulting from the processing of the commands are displayed.

**Note** If you delete a subinterface or PVC (either ATM or Frame Relay PVCs) without configuring the **noautoqosvoip** command, the AutoQoS--VoIP feature will not be removed properly.

## Examples

The following example shows the AutoQoS--VoIP feature configured on serial point-to-point subinterface 4/1.2. In this example, both the **trust** and **fr-atm**keywords are configured.

```
Router> enable
Router# configure terminal
Router(config)# interface serial4/1.2 point-to-point
Router(config-if)# bandwidth 100
Router(config-if)# ip address 192.168.0.0 255.255.255.0
```

```
Router(config-if)# frame-relay interface-dlci 102
Router(config-fr-dlci)# auto qos voip trust fr-atm
Router(config-fr-dlci)# end
Router(config-if#

exit
```

## Related Commands

| Command | Description |
|---|---|
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **show auto qos** | Displays the configurations created by the AutoQoS--VoIP feature on a specific interface or all interfaces. |

# auto qos voip (6500)

To configure AutoQoS on a voice over IP (VoIP) port interface, use the **autoqosvoip** command in interface configuration mode. To remove AutoQos from the configuration, use the **no** form of this command.

**auto qos voip** {**cisco-phone**| **cisco-softphone**| **trust**}

**no auto qos voip** {**cisco-phone**| **cisco-softphone**| **trust**}

## Syntax Description

| | |
|---|---|
| **cisco-phone** | Enables the quality of service (QoS) ingress macro for the Cisco IP Phone. |
| **cisco-softphone** | Enables the QoS ingress macro for the Cisco IP SoftPhone. |
| **trust** | Specifies AutoQoS for ports trusting differentiated services code point (DSCP) and class of service (CoS) traffic markings. |

## Command Default

AutoQos trusts DSCP and CoS traffic markings.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXH | This command was introduced. |

## Usage Guidelines

The **autoqosvoip**command is not supported on gigabit interfaces.

The automation of QoS (AutoQoS) allows you to specify the type of QoS parameters desired on a particular port. For example, entering the **autoqosvoipcisco-softphone** command enables the QoS ingress macro for the Cisco IP SoftPhone.

The Smartports feature provides a set of tools for configuring all switch settings related to a specific application with a single command. For example, entering the **autoqosvoipcisco-phone**command configures all the settings necessary to connect an IP phone to the switch.

You can enter the**showautoqos** command to display the configured AutoQoS macros.

AutoQoS and Smartports are supported on the following modules:

- WS-X6548-RJ45
- WS-X6548-RJ21

- WS-X6148-GE_TX
- WS-X6548-GE-TX-CR
- WS-X6148-RJ45V
- WS-X6148-RJ21V
- WS-X6348-RJ45
- WS-X6348-RJ21
- WS-X6248-TEL

**Note** The **noautoqosvoip** interface configuration command does not disable QoS globally or delete the received CoS-to-internal-DSCP maps created by AutoQoS.

The **autoqosvoipcisco-phone** and the **autoqosvoipcisco-softphone**commands allow you to enable the inbound QoS configuration macros for AutoQoS on an interface. In some cases, the interface-specific **autoqosvoip**commands also generate configuration commands that are applied globally.

You must configure the interface with the **switchport** command if you enter the **autoqosvoipcisco-phone** command. You cannot configure the interface with the **switchport** command if you enter the **autoqosvoipcisco-softphone** command.

If you configure an interface with the **switchport**command, AutoQoS configures the interface to trust CoS. If you do not configure the interface with the **switchport** command, AutoQoS configures the interface to trust DSCP.

AutoQoS uses a nondefault CoS-to-DSCP map. For this reason, you must configure port trust on a per-port-ASIC basis.

When you enter the **autoqosvoipcisco-phone** command, the following behavior occurs:

- QoS is enabled if it is disabled.
- The port is changed to port-based QoS.
- The appropriate CoS map is set.
- All ports are changed to port-based mode (if applicable).
- A trust-CoS QoS policy is created and applied for the ports that need a trust-CoS QoS policy (COIL2 and COIL1).
- A trusted boundary is enabled on the port.
- The CoS value for a trust boundary is set to zero.
- The port trust is set to trust-cos.
- Only 10/100 ports and 10/100/1000 ports are supported.
- A warning message is displayed if the CDP version is not version 2.

When you enter the **autoqosvoipcisco-softphone** command, the following behavior occurs:

- The **cisco-softphone**macro is a superset of the **cisco-phone** macro and configures all features that are required for a Cisco IP Phone to work properly on the Catalyst 6500 series switch.

- The global settings for AutoQoS policy maps, class maps, and access lists are created to classify VoIP packets and to put them in the priority queue or another low-latency queue. The interface settings are created depending on the type of interface and the link speed.
- Two rate limiters are associated with the interface on which the cisco-softphone port-based autoqos macro is executed. The two rate limiters ensure that all inbound traffic on a cisco-softphone port have the following characteristics:
  - The rate of DCSP 46 is at or less than that of the expected softphone rate.
  - The rate of DSCP 26 is at or less than the expected signaling rate.
  - All other traffic is re-marked to DSCP 0 (default traffic).
- DSCP 46 is policed at the rate of 320 kbps with a burst of 2 Kb. DSCP 26 is policed at 32 kbps with a burst of 8 Kb.
- The port is set to untrusted for all port types. The policed-dscp-map is set to ensure that DSCP 46 is marked down to DSCP 0 and DSCP 26 is marked down to DSCP 0. The default QoS IP ACL re-marks all other traffic to DSCP 0.

When you enter the **autoqosvoipsoft-phone** command, the following behavior occurs:

- Enables QoS if QoS is disabled.
- Changes the port to port-based QoS.
- Sets the appropriate police-dscp-map.
- Sets the appropriate CoS-to-DSCP map.
- Changes all ports to port-based mode (if applicable).
- Creates a trust-dscp QoS policy for the ports that need it (COIL2 and COIL1).
- Applies the trust-dscp QoS policy to the port (COIL2 and COIL1).
- Disables a trusted boundary on the port.
- Changes trust to untrusted.
- Allows 10/100 ports and 10/100/1000 ports only.
- Applies two rate limiters, one for DSCP 46 and one for DSCP 26 inbound traffic, and trusts only inbound DSCP 46 and DSCP 26 traffic.
- Marks violations of either rate limiter results in traffic down to DSCP 0.
- Re-marks all other (non-DSCP 26 and 46) inbound traffic to DSCP 0.

When you enter the **autoqosvoiptrust**command, the following applies:

- The DSCP and the CoS markings are trusted for classification of the voice traffic.
- Enables QoS if QoS is disabled.
- Changes the port to port-based QoS.
- Changes all ports to port-based mode (if applicable).
- Creates a trust-dscp and a trust-cos QoS policy for the ports that need it (COIL2 and COIL1).

- Applies the trust-dscp and a trust-cos QoS policy to the port (COIL2 and COIL1).
- Disables the trusted boundary on the port.
- Sets port trust to trust-cos.
- All ports are supported.
- Bases queueing for all ports that allow dscp-to-q mapping on DSCP. If not, queueing is based on CoS.

## Examples

The following example shows how to enable the QoS ingress macro for the Cisco IP Phone:

```
Router(config-if)# auto qos voip cisco-phone
```

## Related Commands

| Command | Description |
|---|---|
| **show auto qos** | Displays AutoQoS information. |
| **show running-config interface** | Displays the status and configuration of the interface. |
| **switchport** | Configures the LAN interface as a Layer 2 switched interface. |

# bandwidth (policy-map class)

To specify or modify the bandwidth allocated for a class belonging to a policy map, or to enable ATM overhead accounting, use the **bandwidth** command in QoS policy-map class configuration mode. To remove the bandwidth specified for a class or disable ATM overhead accounting, use the **no** form of this command.

**bandwidth** {*kbps*| [**remaining**] **percent** *percentage*} [**account** {**qinq**| **dot1q**} **aal5** *subscriber-encapsulation*]

**no bandwidth**

### Cisco 10000 Series Router (PRE3)

**bandwidth** {*kbps*| [**remaining**] **percent** *percentage*} **account** {**qinq**| **dot1q**} {**aal5**| **aal3**} *subscriber-encapsulation***user-defined** *offset* **[atm]**

**no bandwidth**

## Syntax Description

| | |
|---|---|
| *kbps* | Amount of bandwidth, in kilobits per second (kbps), to be assigned to the class. The amount of bandwidth varies according to the interface and platform in use. The value must be between 1 and 2,000,000 kbps. |
| **remaining** | (Optional) Specifies that the percentage of guaranteed bandwidth is based on a relative percent of available bandwidth. |
| **percent** *percentage* | Specifies the percentage of guaranteed bandwidth based on an absolute percent of available bandwidth to be set aside for the priority class or on a relative percent of available bandwidth. The valid range is 1 to 100. |
| **account** | (Optional) Enables ATM overhead accounting. |
| **qinq** | (Optional) Specifies queue-in-queue encapsulation as the broadband aggregation system (BRAS) to digital subscriber line access multiplexer (DSLAM) encapsulation type for ATM overhead accounting. |
| **dot1q** | (Optional) Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type for ATM overhead accounting. |
| **aal5** | (Optional) Specifies ATM Adaptation Layer 5 and the encapsulation type at the subscriber line for ATM overhead accounting. AAL5 supports connection-oriented variable bit rate (VBR) services. See the “Usage Guidelines” section for valid encapsulation types. |

| | |
|---|---|
| *subscriber-encapsulation* | The subscriber line encapsulation type. See the "Usage Guidelines" section for valid encapsulation types. |
| **aal3** | Specifies the ATM Adaptation Layer 5 that supports both connectionless and connection-oriented links. You must specify either **aal3** or **aal5**. |
| **user-defined** *offset* | Specifies the offset size that the router uses when calculating ATM overhead.<br>Valid values are from –127 to127 bytes; 0 is not a valid value.<br>**Note** The router configures the offset size if you do not specify the **user-defined** *offset* option. |
| **atm** | Applies ATM cell tax in the ATM overhead calculation.<br>**Note** Configuring both the *offset* and **atm** options adjusts the packet size to the offset size and then adds ATM cell tax. |

## Command Default

No bandwidth is specified.

ATM overhead accounting is disabled.

## Command Modes

QoS policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE and implemented on Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers. |
| 12.0(7)T | This command was modified. The **percent** keyword was added. |
| 12.0(17)SL | This command was integrated into Cisco IOS Release 12.0(17)SL and implemented on Cisco 10000 series routers. |
| 12.0(22)S | This command was modified. Support for the **percent** keyword was added on Cisco 10000 series routers. |
| 12.0(23)SX | This command was modified. Support for the**remaining percent** keyword was added on Cisco 10000 series routers. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T and implemented on VIP-enabled Cisco 7500 series routers. |

| Release | Modification |
|---|---|
| 12.2(2)T | This command was modified. The **remaining percent** keyword was added. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on Cisco 10000 series routers. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.0(17)SL and implemented on the PRE3 for the Cisco 10000 series router, and was enhanced for ATM overhead accounting on the Cisco 10000 series router for the PRE3. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(31)SB6 | This command was modified to specify an offset size when calculating ATM overhead and implemented on the Cisco 10000 series router for the PRE3. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC and implemented on Cisco 7600 series routers. |
| 12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on Cisco 7300 series routers. |
| 12.4(20)T | This command was modified. Support was added for hierarchical queueing framework (HQF) using the modular quality of service (QoS)CLI (MQC). |
| 15.1(1)T | This command was modified. The allowed values for the *kbps* argument were changed. The value must be from 8 to 2000000. |
| 15.2(1)T | This command was modified. The allowed values for the offset argument and kbps arguments were changed. |

## Usage Guidelines

### Configuring a Policy Map

Use the **bandwidth** command when you configure a policy map for a class defined by the **class-map** command. The **bandwidth** command specifies the bandwidth for traffic in that class. Class-based weighted fair queueing (CBWFQ) derives the weight for packets belonging to the class from the bandwidth allocated to the class. CBWFQ then uses the weight to ensure that the queue for the class is serviced fairly.

### Configuring Strict Priority with Bandwidth

You can configure only one class with strict priority. Other classes cannot have priority or bandwidth configuration. To configure minimum bandwidth for another class, use the**bandwidthremainingpercent** command.

### Specifying Bandwidth as a Percentage for All Supported Platforms Except the Cisco 10000 Series Routers

Besides specifying the amount of bandwidth in kilobits per second (kbps), you can specify bandwidth as a percentage of either the available bandwidth or the total bandwidth. During periods of congestion, the classes are serviced in proportion to their configured bandwidth percentages. The bandwidth percentage is based on the interface bandwidth. Available bandwidth is equal to the interface bandwidth minus the sum of all bandwidths reserved by the Resource Reservation Protocol (RSVP) feature, the IP RTP Priority feature, and the low latency queueing (LLQ) feature.

**Note** It is important to remember that when the **bandwidth remaining percent** command is configured, hard bandwidth guarantees may not be provided and only relative bandwidths are assured. That is, class bandwidths are always proportional to the specified percentages of the interface bandwidth. When the link bandwidth is fixed, class bandwidth guarantees are in proportion to the configured percentages. If the link bandwidth is unknown or variable, the router cannot compute class bandwidth guarantees in kbps.

### Specifying Bandwidth as a Percentage for the Cisco 10000 Series Routers

Besides specifying the amount of bandwidth in kilobits per second (kbps), you can specify bandwidth as a percentage of either the available bandwidth or the total bandwidth. During periods of congestion, the classes are serviced in proportion to their configured bandwidth percentages. The minimum bandwidth percentage is based on the nearest parent shape rate.

**Note** It is important to remember that when the **bandwidth remaining percent** command is configured, hard bandwidth guarantees may not be provided and only relative bandwidths are assured. That is, class bandwidths are always proportional to the specified percentages of the interface bandwidth. When the link bandwidth is fixed, class bandwidth guarantees are in proportion to the configured percentages. If the link bandwidth is unknown or variable, the router cannot compute class bandwidth guarantees in kbps.

The router converts the specified bandwidth to the nearest multiple of 1/255 (ESR-PRE1) or 1/65535 (ESR-PRE2) of the interface speed. Use the **show policy-map interface** command to display the actual bandwidth.

### Restrictions for All Supported Platforms

The following restrictions apply to the **bandwidth** command:

- The amount of bandwidth configured should be large enough to also accommodate Layer 2 overhead.
- A policy map can have all the class bandwidths specified in either kbps or percentage, but not both, in the same class. However, the unit for the **priority**command in the priority class can be different from the bandwidth unit of the nonpriority class.
- When the **bandwidth percent** command is configured, and a policy map containing class policy configurations is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed. If a policy map cannot be attached to a particular interface because of insufficient interface bandwidth, the policy is removed from all interfaces to which it was successfully attached. This restriction does not apply to the **bandwidth remaining percent** command.

**Note** With CSCsy73939, if the **bandwidth percent** command results in a bandwidth value that is lower than the valid range then the policy map specifying this value cannot be attached to an interface, and the router displays the following error message: "service-policy output parent Configured Percent results in out of range kbps. Allowed range is *min-value–max-value*. The present CIR value is *n*."

For more information on bandwidth allocation, see the "Congestion Management Overview" module in the *Cisco IOS Quality of Service Solutions Configuration Guide.*

Note that when the policy map containing class policy configurations is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed. If a policy map cannot be attached to a particular interface because of insufficient interface bandwidth, then the policy is removed from all interfaces to which it was successfully attached.

### Modular QoS CLI Queue Limits

The **bandwidth** command can be used with MQC to specify the bandwidth for a particular class. When used with MQC, the **bandwidth** command uses a default queue limit for the class. This queue limit can be modified using the **queue-limit** command, thereby overriding the default set by the **bandwidth** command.

**Note** To meet the minimum bandwidth guarantees required by interfaces, modify the default queue limit of high-speed interfaces by using the **queue-limit** command.

### Cisco 10000 Series Router

The Cisco 10000 series routers supports the **bandwidth** command on outbound interfaces only. They do not support this command on inbound interfaces.

On the PRE2, you specify a bandwidth value and a unit for the bandwidth value. Valid values for the bandwidth are from 1 to 2488320000. The units are bps, kbps, mbps, and gbps. The default unit is kbps. For example, the following commands configure a bandwidth of 10000 bps and 10000 kbps on the PRE2:

```
bandwidth 10000 bps
bandwidth 10000
```

On the PRE3, youspecify only a bandwidth value. Because the unit is always kbps, the PRE3 does not support the unit argument. Valid values are from 1 to 2000000. For example, the following command configures a bandwidth of 128,000 kbps on the PRE3:

```
bandwidth 128000
```

The PRE3 accepts the PRE2 **bandwidth** command only if the command is used without the unit argument. The PRE3 rejects the PRE2 **bandwidth** command if the specified bandwidth is outside the valid PRE3 bandwidth value range (1 to 2000000).

Besides specifying the amount of bandwidth in kilobits per second (kbps), you can specify bandwidth as a percentage of either the available bandwidth or the total bandwidth. During periods of congestion, the classes are serviced in proportion to their configured bandwidth percentages. The bandwidth percentage is based on the interface bandwidth. However, in a hierarchical policy the minimum bandwidth percentage is based on the nearest parent shape rate.

**Note** When the **bandwidth remaining percent** command is configured, hard bandwidth guarantees may not be provided and only relative bandwidths are assured. Class bandwidths are always proportional to the specified percentages of the interface bandwidth. When the link bandwidth is fixed, class bandwidth guarantees are in proportion to the configured percentages. If the link bandwidth is unknown or variable, the router cannot compute class bandwidth guarantees in kbps.

The router converts the specified bandwidth to the nearest multiple of 1/255 (PRE1) or 1/65535 (PRE2, PRE3) of the interface speed. Use the **show policy-map interface** command to display the actual bandwidth.

#### Overhead Accounting for ATM (Cisco 10000 Series Router)

When configuring ATM overhead accounting, you must specify the BRAS-DSLAM, DSLAM-CPE, and subscriber line encapsulation types. The router supports the following subscriber line encapsulation types:

- mux-1483routed
- mux-dot1q-rbe
- snap-pppoa
- mux-rbe
- snap-1483routed
- snap-dot1q-rbe
- mux-pppoa
- snap-rbe

The router calculates the offset size unless you specify the **user-defined** *offset* option.

For hierarchical policies, configure ATM overhead accounting in the following ways:

- Enabled on parent--If you enable ATM overhead accounting on a parent policy, you are not required to enable accounting on the child policy.
- Enabled on child and parent--If you enable ATM overhead accounting on a child policy, then you must enable ATM overhead accounting on the parent policy.

The encapsulation types must match for the child and parent policies.

The user-defined offset values must match for the child and parent policies.

## Examples

## Examples

In the following example, the policy map named VLAN guarantees 30 percent of the bandwidth to the class named Customer1 and 60 percent of the bandwidth to the class named Customer2. If you apply the VLAN policy map to a 1-Mbps link, 300 kbps (30 percent of 1 Mbps) is guaranteed to class Customer1 and 600 kbps (60 percent of 1 Mbps) is guaranteed to class Customer2, with 100 kbps remaining for the class-default class. If the class-default class does not need additional bandwidth, the unused 100 kbps is available for use by class Customer1 and class Customer2. If both classes need the bandwidth, they share it in proportion to the configured rates. In this example, the sharing ratio is 30:60 or 1:2:

```
router(config)# policy-map VLAN
```

```
router(config-pmap)# class Customer1
router(config-pmap-c)# bandwidth percent 30
router(config-pmap-c)# exit
router(config-pmap)# class Customer2
router(config-pmap-c)# bandwidth percent 60
```

## Examples

The following example shows how to create a policy map with two classes, shows how bandwidth is guaranteed when only CBWFQ is configured, and shows how to attach the policy to serial interface 3/2/1:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# exit
Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth percent 25
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial3/2/1
Router(config-if)# service output policy1
Router(config-if)# end
```

The following output from the **show policy-map** command shows the configuration for the policy map named policy1:

```
Router# show policy-map policy1

Policy Map policy1
 Class class1
  Weighted Fair Queuing
   Bandwidth 50 (%) Max Threshold 64 (packets)
 Class class2
  Weighted Fair Queuing
   Bandwidth 25 (%) Max Threshold 64 (packets)
```

The output from the **show policy-map interface**command shows that 50 percent of the interface bandwidth is guaranteed for the class named class1, and 25 percent is guaranteed for the class named class2. The output displays the amount of bandwidth as both a percentage and a number of kbps.

```
Router# show policy-map interface serial3/2

Serial3/2
Service-policy output:policy1
Class-map:class1 (match-all)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match:none
 Weighted Fair Queuing
  Output Queue:Conversation 265
  Bandwidth 50 (%)
  Bandwidth 772 (kbps) Max Threshold 64 (packets)
  (pkts matched/bytes matched) 0/0
  (depth/total drops/no-buffer drops) 0/0/0
Class-map:class2 (match-all)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match:none
 Weighted Fair Queuing
  Output Queue:Conversation 266
  Bandwidth 25 (%)
  Bandwidth 386 (kbps) Max Threshold 64 (packets)
  (pkts matched/bytes matched) 0/0
  (depth/total drops/no-buffer drops) 0/0/0
Class-map:class-default (match-any)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match:any
```

In this example, serial interface 3/2 has a total bandwidth of 1544 kbps. During periods of congestion, 50 percent (or 772 kbps) of the bandwidth is guaranteed to the class named class1, and 25 percent (or 386 kbps) of the link bandwidth is guaranteed to the class named class2.

## Examples

In the following example, the interface has a total bandwidth of 1544 kbps. During periods of congestion, 50 percent (or 772 kbps) of the bandwidth is guaranteed to the class named class1, and 25 percent (or 386 kbps) of the link bandwidth is guaranteed to the class named class2.

The following sample output from the **show policy-map** command shows the configuration of a policy map named p1:

```
Router# show policy-map p1
Policy Map p1
 Class voice
  Weighted Fair Queuing
   Strict Priority
   Bandwidth 500 (kbps) Burst 12500 (Bytes)
 Class class1
  Weighted Fair Queuing
   Bandwidth remaining 50 (%) Max Threshold 64 (packets)
 Class class2
  Weighted Fair Queuing
   Bandwidth remaining 25 (%) Max Threshold 64 (packets)
```

The following output from the **show policy-map interface** command on serial interface 3/2 shows that 500 kbps of bandwidth is guaranteed for the class named voice1. The classes named class1 and class2 receive 50 percent and 25 percent of the remaining bandwidth, respectively. Any unallocated bandwidth is divided proportionally among class1, class2, and any best-effort traffic classes.

**Note** In this sample output (unlike many of the others earlier in this section) the bandwidth is displayed only as a percentage for class 1 and class 2. Bandwidth expressed as a number of kbps is not displayed because the **percent** keyword was used with the **bandwidth remaining** command. The **bandwidth remaining percent** command allows you to allocate bandwidth as a relative percentage of the total bandwidth available on the interface.

```
Router# show policy-map interface serial3/2

Serial3/2
Service-policy output:p1
 Class-map:voice (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:ip precedence 5
  Weighted Fair Queuing
   Strict Priority
   Output Queue:Conversation 264
   Bandwidth 500 (kbps) Burst 12500 (Bytes)
   (pkts matched/bytes matched) 0/0
   (total drops/bytes drops) 0/0
 Class-map:class1 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:none
  Weighted Fair Queuing
   Output Queue:Conversation 265
   Bandwidth remaining 50 (%) Max Threshold 64 (packets)
   (pkts matched/bytes matched) 0/0
   (depth/total drops/no-buffer drops) 0/0/0
 Class-map:class2 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
```

```
  Match:none
  Weighted Fair Queuing
   Output Queue:Conversation 266
   Bandwidth remaining 25 (%) Max Threshold 64 (packets)
   (pkts matched/bytes matched) 0/0
   (depth/total drops/no-buffer drops) 0/0/0
Class-map:class-default (match-any)
 0 packets, 0 bytes
 5 minute offered rate 0 bps, drop rate 0 bps
 Match:any
```

## Examples

When a parent policy has ATM overhead accounting enabled, you are not required to enable ATM overhead accounting on a child traffic class that does not contain the **bandwidth** or **shape** command. In the following configuration example, ATM overhead accounting is enabled for bandwidth on the gaming and class-default class of the child policy map named subscriber_classes and on the class-default class of the parent policy map named subscriber_line. The voip and video classes do not have ATM overhead accounting explicitly enabled; these priority queues have overhead accounting implicitly enabled because ATM overhead accounting is enabled on the parent policy. Notice that the features in the parent and child policies use the same encapsulation type.

```
Router(config)# policy-map subscriber_classes
Router(config-pmap)# class voip
Router(config-pmap-c)# priority level 1
Router(config-pmap-c)# police 8000
Router(config-pmap-c)# exit
Router(config-pmap)# class video
Router(config-pmap-c)# priority level 2
Router(config-pmap-c)# police 20
Router(config-pmap-c)# exit
Router(config-pmap)# class gaming
Router(config-pmap-c)# bandwidth remaining percent 80 account aal5 snap-rbe-dot1q
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth remaining percent 20 account aal5 snap-rbe-dot1q
Router(config-pmap-c)# policy-map subscriber_line
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth remaining ratio 10 account aal5 snap-rbe-dot1q
Router(config-pmap-c)# shape average 512 account aal5 snap-rbe-dot1q
Router(config-pmap-c)# service policy subscriber_classes
```

In the following example, the router uses 20 overhead bytes and ATM cell tax in calculating ATM overhead. The child and parent policies contain the required matching offset values. The parent policy is attached to virtual template 1.

```
Router(config)# policy-map child
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 500 account user-defined 20 atm
Router(config-pmap-c)# exit
Router(config-pmap)# class class2
Router(config-pmap-c)# shape average 30000 account user-defined 20 atm
Router(config-pmap)# exit
Router(config)# exit
Router(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **class (policy-map)** | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy. |

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **max-reserved-bandwidth** | Changes the percent of interface bandwidth allocated for CBWFQ, LLQ, and IP RTP Priority. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **priority** | Specifies the priority of a class of traffic belonging to a policy map. |
| **queue-limit** | Specifies or modifies the maximum number of packets the queue can hold for a class policy configured in a policy map. |
| **random-detect (interface)** | Enables WRED or DWRED. |
| **random-detect exponential-weighting- constant** | Configures the WRED and DWRED exponential weight factor for the average queue size calculation. |
| **random-detect precedence** | Configures WRED and DWRED parameters for a particular IP precedence. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# bandwidth qos-reference

To configure bandwidth to be used as a reference for calculating rates of quality of service (QoS) percent configurations on a physical or logical interface, use the **bandwidthqos-reference** command in interface configuration or subinterface configuration mode. To remove this explicitly specified reference bandwidth, use the **no** form of this command.

**bandwidth qos-reference** *bandwidth-amount*

**no bandwidth qos-reference** *bandwidth-amount*

## Syntax Description

| | |
|---|---|
| *bandwidth-amount* | Amount of bandwidth in kilobits per second (kb/s). Valid values are 1 to 10000000. |

## Command Default

This command is disabled. Reference bandwidth for a logical interface is derived from the main interface or the main interface QoS policy.

## Command Modes

Interface configuration (config-if) Subinterface configuration (config-subif)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)XNE | This command was introduced. |
| 15.1(3)T | Support for logical interfaces is expanded to include the main interface, subinterface, and Frame Relay. |

## Usage Guidelines

The **bandwidthqos-reference**command is used only as reference for calculating rates of QoS percent configurations on a logical interface. This command does not actually allocate a specified amount of bandwidth for a logical interface.

**Note** In Cisco IOS Release 12.2(33)XNE, the **bandwidthqos-reference**command is supported only on a tunnel logical interface. In Cisco IOS Release 15.1(3)T, support is expanded to include main interface, subinterface, and Frame Relay as well as tunnel logical interfaces.

### Compatibility with the shape (percent) and the police (percent) Commands

The **bandwidthqos-reference**command is compatible with and related to the **shape**(percent) and **police**(percent) commands. The **shape**(percent) command allows you to configure average-rate or peak-rate traffic shaping on the basis of a percentage of bandwidth available on an interface. The **police**(percent) command allows you to configure traffic policing on the basis of a percentage of bandwidth available on an interface.

The **bandwidthqos-reference**command interacts with the**shape**(percent) and **police** (percent) commands in the following ways:

- If the **bandwidthqos-reference**command is used to specify the bandwidth, the**shape** (percent) command and the **police** (percent) commands will use this specified amount to calculate the respective bandwidth percentages.
- If the **bandwidthqos-reference**command is *not* used to specify the bandwidth, the **shape** (percent) command and the **police**(percent) commands will use the amount of bandwidth available on the interface to calculate the respective bandwidth percentages.

### Compatibility with bandwidth (interface) Command

The **bandwidth**(interface) command allows you to set the inherited and received bandwidth values for an interface.

If both the **bandwidth** (interface) and **bandwidthqos-reference**commands are enabled on any interface, the value specified by the **bandwidthqos-reference**command is used as the reference for calculating rates for QoS percent configurations on that particular physical or logical interface. The value specified by the **bandwidth**(interface) command is disregarded.

In the sample configuration shown below, the value for the **bandwidthqos-reference** command is entered as 8000 kb/s, and the value for the **bandwidth** (interface) command is entered as 900 kb/s. The value for the **shapeaveragepercent** command is set to 50. The effect is seen in the output for the **targetshaperate** command, which is set to 4000000 bits per second (50 percent of 8000 kb/s):

```
Router(config)# interface e0/1
Router(config-if)# bandwidth qos-reference 8000
Router(config-if)# bandwidth 900

Router(config)# interface e0/1
Router(config-if)# bandwidth 900
Router(config-if)# end
Router# show running-config interface e0/1
interface Ethernet0/1
 bandwidth 900
 bandwidth qos-reference 8000
 no ip address
 load-interval 30
end
Router(config-if)# policy-map test
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average percent 50
Router(config-pmap-c)# interface e0/1
Router(config-if)# service-policy out test
Router# show policy-map interface
 Ethernet0/1
Service-policy output: test
 Class-map: class-default (match-any)
  79 packets, 7837 bytes
  30 second offered rate 0 bps, drop rate 0 bps
  Match: any
  Queueing
  queue limit 64 packets
  (queue depth/total drops/no-buffer drops) 0/0/0
  (pkts output/bytes output) 79/7837
  shape (average) cir 4000000, bc 40000, be 40000
  target shape rate 4000000
```

## Examples

The following example shows how to configure the**bandwidthqos-reference**command to allocate 2000 kb/s of bandwidth as a reference rate for tunnel interface 1:

```
Router> enable
Router# configure terminal
Router(config)# interface tunnel1
Router#(config-if)# bandwidth qos-reference 2000
```

The following example shows how to configure the**bandwidthqos-reference**command to use 700 kb/s of bandwidth as a reference rate for the main interface e0/1:

```
Router(config)# interface e0/1
Router(config-if)# bandwidth qos-ref 700
Router(config-if)# policy-map test
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average percent 50
Router(config-pmap-c)# interface e0/1
Router(config-if)# service-policy out test
```

The following example shows how to configure the**bandwidthqos-reference**command to use 500 kb/s of bandwidth as a reference rate for the subinterface e0/1.1:

```
Router(config-subif)# interface e0/1
Router(config-if)# no service-policy out test
Router(config-if)# interface e0/1.1
Router(config-subif)# bandwidth qos-ref 500
Router(config-subif)# service-policy ou test
```

The following example shows how to configure the**bandwidthqos-reference**command to use 400 kb/s of bandwidth as a reference rate for the Frame Relay interface s6/0.1:

```
Router(config)# no policy-map test
Router(config)# policy-map test
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average percent 50
Router(config-pmap-c)# map-class frame-relay fr1
Router(config-map-class)# service-policy out test
Router(config-map-class)# end
Router# configure terminal
Router(config)# interface s6/0.1
Router(config-subif)# bandwidth qos-ref 400
Router(config-subif)# end
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth** (interface) | Sets the inherited and received bandwidth values for an interface. |
| **police** (percent) | Configures traffic policing on the basis of a percentage of bandwidth available on an interface. |
| **shape** (percent) | Specifies average-rate or peak-rate traffic shaping on the basis of a percentage of bandwidth available on an interface. |

# bandwidth remaining ratio

To specify a bandwidth-remaining ratio for class-level or subinterface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to nonpriority queues, use the**bandwidthremainingratio** command in policy-map class configuration mode. To remove the bandwidth-remaining ratio, use the **no** form of this command.

**bandwidth remaining ratio** *ratio*

**no bandwidth remaining ratio** *ratio*

**bandwidth remaining ratio** *ratio* [**account** {**qinq**| **dot1q**} **[aal5]** {*subscriber-encapsulation*| **user-defined** *offset*}]

**no bandwidth remaining ratio** *ratio* [**account** {**qinq**| **dot1q**} **[aal5]** {*subscriber-encapsulation*| **user-defined** *offset*}]

**bandwidth remaining ratio** *ratio*

**no bandwidth remaining ratio** *ratio*

## Syntax Description

| | |
|---|---|
| *ratio* | Relative weight of this subinterface or class queue with respect to other subinterfaces or class queues. Valid values are from 1 to 1000. At the subinterface level, the default value is platform dependent. At the class queue level, the default is 1. |
| Cisco 7300 Series Router, Cisco 7600 Series Router, and Cisco 10000 Series Router | |
| *ratio* | Relative weight of this subinterface or class queue with respect to other subinterfaces or class queues.<br>**Note** For the Cisco 7300 series router and 7600 series router, valid values are from 1 to 10000, and the default value is 1.<br>**Note** For the Cisco 10000 series router, valid values are from 1 to 1000, and the default is 1. |
| **account** | (Optional) Enables ATM overhead accounting. |
| **qinq** | (Optional) Specifies queue-in-queue encapsulation as the Broadband Remote Access Server - Digital Subscriber Line Access Multiplexer (BRAS-DSLAM) encapsulation type. |
| **dot1q** | (Optional) Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type. |

| | |
|---|---|
| **aal5** | (Optional) Specifies the ATM adaptation layer 5 that supports connection-oriented variable bit rate (VBR) services. |
| *subscriber-encapsulation* | (Optional) Specifies the encapsulation type at the subscriber line. Encapsulation type varies according to subscriber line. |
| **user-defined** *offset* | (Optional) Specifies the offset size, in bytes, that the router uses when calculating the ATM overhead.<br>**Note** For the Cisco 7300 series router and 7600 series router, valid values are from -48 to +48.<br>**Note** For the Cisco 10000 series router, valid values are from -63 to +63. |
| Cisco ASR 1000 Series Routers | |
| *ratio* | Relative weight of this subinterface or class queue with respect to other subinterfaces or class queues. Valid values are from 1 to 1000. At the subinterface level and class-queue level, the default is 1. |

For most platforms, the default bandwidth ratio is 1.

## Command Default

When you use default bandwidth-remaining ratios at the subinterface level, the Cisco 10000 series router distinguishes between interface types. At the subinterface level, the default bandwidth-remaining ratio is 1 for VLAN subinterfaces and Frame Relay Data Link Connection Identifiers (DLCI). For ATM subinterfaces, the router computes the default bandwidth-remaining ratio based on the subinterface speed.

When you use default bandwidth-remaining ratios at the class level, the Cisco 10000 series router makes no distinction between interface types. At the class level, the default bandwidth-remaining ratio is 1.

## Command Modes

Policy-map class (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SB2 | This command was introduced. This command was implemented on the Cisco 10000 series router for the PRE3. |
| 12.2(33)SRC | This command was modified. It was implemented on the Cisco 7600 series routers. Additional keywords and arguments were added to support ATM overhead accounting (optional) on the Cisco 7600 series router and the Cisco 10000 series router for the PRE3. |

| Release | Modification |
|---|---|
| 12.2(33)SB | This comand was modified. Support for the Cisco 7300 series routers was added. The additional keyword and arguments associated with ATM overhead accounting were also supported. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |

## Usage Guidelines

### Cisco 10000 Series Router

The scheduler uses the ratio specified in the **bandwidthremainingratio** command to determine the amount of excess bandwidth (unused by priority traffic) to allocate to a class-level queue or a subinterface-level queue during periods of congestion. The scheduler allocates the unused bandwidth relative to other queues or subinterfaces.

The **bandwidthremainingratio** command cannot coexist with another **bandwidth** command in different traffic classes of the same policy map. For example, the following configuration is not valid and causes an error message to display:

```
policy-map Prec1
 class precedence_0
  bandwidth remaining ratio 10
 class precedence_2
  bandwidth 1000
```

For the PRE2, the **bandwidthremainingratio** command can coexist with another **bandwidth** command in the same class of a policy map. On the PRE3, the **bandwidthremainingratio** command cannot coexist with another **bandwidth**command in the same class. For example, the following configuration is not valid on the PRE3 and causes an error message to display:

```
policy-map Prec1
 class precedence_0
  bandwidth 1000
  bandwidth remaining ratio 10
```

In a hierarchical policy map in which the parent policy has only the class-default class defined with a child queuing policy applied, the router accepts only the **bandwidthremainingratio** form of the **bandwidth** command in the class-default class.

The **bandwidthremainingratio** command cannot coexist with the **priority** command in the same class. For example, the following configuration is not valid and causes an error message to display:

```
policy-map Prec1
 class precedence_1
  priority
  police percent 30
  bandwidth remaining ratio 10
```

All of the queues for which the **bandwidthremainingratio** command is not specified receive the platform-specified minimum bandwidth-remaining ratio. The router determines the minimum committed information rate (CIR) based on the configuration.

### ATM Overhead Accounting (Optional)

The **bandwidthremainingratio** command can also be used to enable ATM overhead accounting. To enable ATM overhead accounting, use the **account** keyword and the subsequent keywords and arguments as documented in the Syntax Description table.

### Cisco 7200 Series Routers

The**bandwidthremainingratio** command is not supported on the Cisco 7200 series routers. If you have upgraded from Cisco IOS Release 12.2(33)SRD to Cisco IOS Release 12.2(33)SRE, you may see parser errors when you run this command. You can use the **bandwidthremainingpercent** command in place of the **bandwidthremainingratio**command on Cisco 7200 series routers to achieve the same functionality.

## Examples

## Examples

The following example shows how to configure a bandwidth-remaining ratio on an ATM subinterface. In the example, the router guarantees a peak cell rate of 50 Mbps for the variable bit rate nonreal-time (VBR-nrt) PVC 0/200. During periods of congestion, the subinterface receives a share of excess bandwidth (unused by priority traffic) based on the bandwidth-remaining ratio of 10, relative to the other subinterfaces configured on the physical interface.

```
policy-map Child
 class precedence_0
  bandwidth 10000
 class precedence_1
  shape average 100000
  bandwidth 100
!
policy-map Parent
 class class-default
  bandwidth remaining ratio 10
  shape average 20000000
  service-policy Child
!
interface ATM2/0/3.200 point-to-point
 ip address 10.20.1.1 255.255.255.0
 pvc 0/200
 protocol ip 10.20.1.2
 vbr-nrt 50000
 encapsulation aal5snap
 service-policy output Parent
```

The following example shows how to configure bandwidth remaining ratios for individual class queues. Some of the classes configured have bandwidth guarantees and a bandwidth-remaining ratio explicitly specified. When congestion occurs within a subinterface level, the class queues receive excess bandwidth (unused by priority traffic) based on their class-level bandwidth-remaining ratios: 20, 30, 120, and 100, respectively, for the precedence_0, precedence_1, precedence_2, and precedence_5 classes. Normally, the precedence_3 class (without a defined ratio) would receive bandwidth based on the bandwidth-remaining ratio of the class-default class defined in the Child policy. However, in the example, the Child policy does not define a class-default bandwidth remaining ratio. Therefore, the router uses a ratio of 1 to allocate excess bandwidth to precedence_3 traffic.

```
policy-map Child
 class precedence_0
  shape average 100000
  bandwidth remaining ratio 20
 class precedence_1
  shape 10000
  bandwidth remaining ratio 30
 class precedence_2
  shape average 200000
  bandwidth remaining ratio 120
 class precedence_3
  set ip precedence 3
 class precedence_5
  set ip precedence 5
  bandwidth remaining ratio 100
policy-map Parent
 class class-default
  bandwidth remaining ratio 10
  service-policy Child
```

```
!
interface GigabitEthernet 2/0/1.10
 encapsulation dot1q 10
 service-policy output Parent
```

## Examples

The following example shows how to configure overhead accounting by using the optional **account**keyword and associated keywords and arguments:

```
policy-map subscriber_line
 class class-default
  bandwidth remaining ratio 10 account dot1q aal5 snap-rbe-dot1q
  shape average 512 account dot1q
aal5 snap-rbe-dot1q
  service policy subscriber_classes
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth remaining percent** | Specifies a bandwidth-remaining percentage for class-level or subinterface-level queues to be used during congestion to determine the amount of excess bandwidth (unused by priority traffic) to allocate to nonpriority queues. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# bump

To configure the bump ing rules for a virtual circuit (VC) class that can be assigned to a VC bundle, use the **bump** command in VC-class configuration mode. To remove the explicit bumping rules for the VCs assigned to this class and return to the default condition of implicit bumping, use the **nobumpexplicit**commandor the **bumpimplicit** command. To specify that the VC bundle members do not accept any bumped traffic, use the **no**form of thiscommand.

To configure the bumping rules for a specific VC or permanent virtual circuit (PVC) member of a bundle, use the **bump** command in bundle-vc or SVC-bundle-member configuration mode. To remove the explicit bumping rules for the VC or PVC bundle member and return to the default condition of implicit bumping, use the **bumpimplicit**command. To specify that the VC or PVC bundle member does not accept any bumped traffic, use the **nobumptraffic**command.

**bump** {**explicit** *precedence-level*| **implicit**| **traffic**}

**no bump** {**explicit** *precedence-level*| **implicit**| **traffic**}

## Syntax Description

| | |
|---|---|
| **explicit** *precedence-level* | Specifies the precedence level to which traffic on a VC or PVC will be bumped when the VC or PVC goes down. Valid values for the *precedence-level* argument are numbers from 0 to 7. |
| **implicit** | Applies the implicit bumping rule, which is the default, to a single VC or PVC bundle member or to all VCs in the bundle (VC-class mode). The implicit bumping rule stipulates that bumped traffic is to be carried by a VC or PVC with a lower precedence level. |
| **traffic** | Specifies that the VC or PVC accepts bumped traffic (the default condition). The **no**form stipulates that the VC or PVC does not accept any bumped traffic. |

## Command Default

Implicit bumping

Permit bumping (VCs accept bumped traffic)

## Command Modes

VC-class configuration (for a VC class) Bundle-vc configuration (for an ATM VC bundle member) SVC-bundle-member configuration (for an SVC bundle member)

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |

| Release | Modification |
|---|---|
| 12.2(4)T | This command was made available in SVC-bundle-member configuration mode. |
| 12.0(23)S | This command was made available in VC-class and bundle-vc configuration modes on the 8-port OC-3 STM-1 ATM line card for Cisco 12000 series Internet routers. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S and implemented on the Cisco 10000 series router. |
| 12.2(16)BX | This command was implemented on the ESR-PRE2. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **bump** command in bundle-vc configuration mode (for an ATM VC bundle member) or SVC-bundle-member configuration mode (for an SVC bundle member) to configure bumping rules for a discrete VC or PVC bundle member. Use the **bump** command in VC-class configuration mode to configure a VC class that can be assigned to a bundle member.

The effects of different bumping configuration approaches are as follows:

- Implicit bumping--If you configure implicit bumping, bumped traffic is sent to the VC or PVC configured to handle the next lower precedence level. When the original VC or PVC that bumped the traffic comes back up, the traffic that it is configured to carry is restored to it. If no other positive forms of the **bump** command are configured, the **bumpimplicit**commandtakes effect.
- Explicit bumping--If you configure a VC or PVC with the **bumpexplicit** command, you can specify the precedence level to which traffic will be bumped when that VC or PVC goes down, and the traffic will be directed to a VC or PVC mapped with that precedence level. If the VC or PVC that picks up and carries the traffic goes down, the traffic is subject to the bumping rules for that VC or PVC. You can specify only one precedence level for bumping.
- Permit bumping--The VC or PVC accepts bumped traffic by default. If the VC or PVC has been previously configured to reject bumped traffic, you must use the **bumptraffic** command to return the VC or PVC to its default condition.
- Reject bumping--To configure a discrete VC or PVC to reject bumped traffic when the traffic is directed to it, use the **nobumptraffic** command.

**Note** When no alternative VC or PVC can be found to handle bumped traffic, the bundle is declared down. To avoid this occurrence, configure explicitly the bundle member VC or PVC that has the lowest precedence level.

To use this command in VC-class configuration mode, you must enter the **vc-classatm** global configuration command before you enter this command.

To use this command to configure an individual bundle member in bundle-VC configuration mode, first issue the **bundle** command to enter bundle configuration mode for the bundle to which you want to add or modify the VC member to be configured. Then use the **pvc-bundle** command to specify the VC to be created or modified and enter bundle-vc configuration mode.

This command has no effect if the VC class that contains the command is attached to a standalone VC; that is, if the VC is not a bundle member. In this case, the attributes are ignored by the VC.

VCs in a VC bundle are subject to the following configuration inheritance guidelines (listed in order of next-highest precedence):

- VC configuration in bundle-vc mode
- Bundle configuration in bundle mode (with the effect of assigned VC-class configuration)
- Subinterface configuration in subinterface mode

## Examples

The following example configures the class called “five” to define parameters applicable to a VC in a bundle. If the VC goes down, traffic will be directed (bumped explicitly) to a VC mapped with precedence level 7:

```
vc-class atm five
 ubr 5000
 precedence 5
 bump explicit 7
```

The following example configures the class called “premium-class” to define parameters applicable to a VC in a bundle. Unless overridden with a bundle-vc **bump** configuration, the VC that uses this class will not allow other traffic to be bumped onto it:

```
vc-class atm premium-class
 no bump traffic
 bump explicit 7
```

## Related Commands

| Command | Description |
|---|---|
| **bundle** | Enters bundle configuration mode to create a bundle or modify an existing bundle. |
| **class** | Assigns a map class or VC class to a PVC or PVC bundle member. |
| **class-vc** | Assigns a VC class to an ATM PVC, SVC, or VC bundle member. |

| Command | Description |
|---|---|
| **dscp (frame-relay vc-bundle-member)** | Specifies the DSCP value or values for a specific Frame Relay PVC bundle member. |
| **precedence** | Configures precedence levels for a VC or PVC class that can be assigned to a VC or PVC bundle and thus applied to all members of that bundle. |
| **protect** | Configures a VC or PVC class with protected group or protected VC or PVC status for application to a VC or PVC bundle member. |
| **pvc-bundle** | Adds a PVC to a bundle as a member of the bundle and enters bundle-vc configuration mode in order to configure that PVC bundle member. |
| **pvc (frame-relay vc-bundle)** | Creates a PVC and PVC bundle member and enters frame-relay vc-bundle-member configuration mode. |
| **svc-bundle** | Creates or modifies a member of an SVC bundle. |
| **ubr** | Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member. |
| **ubr+** | Configures UBR QoS and specifies the output peak cell rate and output minimum guaranteed cell rate for an ATM PVC, SVC, VC class, or VC bundle member. |
| **vbr-nrt** | Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member. |
| **vc-class atm** | Configures a VC class or an ATM VC or interface. |

# bundle

To create a bundle or modify an existing bundle to enter bundle configuration mode, use the **bundle** command in subinterface configuration mode. To remove the specified bundle, use the **no**form of this command.

**bundle** *bundle-name*

**no bundle** *bundle-name*

## Syntax Description

| | |
|---|---|
| *bundle-name* | The name of the bundle to be created. The limit is 16 alphanumeric characters. |

## Command Default

No bundle is specified.

## Command Modes

Subinterface configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S and implemented on the Cisco 10000 series router. |
| 12.2(16)BX | This command was implemented on the ESR-PRE2. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

From within bundle configuration mode you can configure the characteristics and attributes of the bundle and its members, such as the encapsulation type for all virtual circuits (VCs) in the bundle, the bundle management parameters, and the service type. Attributes and parameters you configure in bundle configuration mode are applied to all VC members of the bundle.

VCs in a VC bundle are subject to the following configuration inheritance guidelines (listed in order of next highest precedence):

- VC configuration in bundle-vc mode

- Bundle configuration in bundle mode
- Subinterface configuration in subinterface mode

To display status on bundles, use the **showatmbundle** and **showatmbundlestatistics**commands.

## Examples

The following example shows how to configure a bundle called bundle1. The example specifies the IP address of the subinterface and the router protocol--the router uses Intermediate System-to-Intermediate System (IS-IS) as an IP routing protocol--then configures the bundle:

```
interface atm1/0.1 multipoint
 ip address 10.0.0.1 255.255.255.0
 ip router isis
 bundle bundle1
```

## Related Commands

| Command | Description |
|---|---|
| **class-bundle** | Configures a VC bundle with the bundle-level commands contained in the specified VC class. |
| **oam-bundle** | Enables end-to-end F5 OAM loopback cell generation and OAM management for all VC members of a bundle, or for a VC class that can be applied to a VC bundle. |
| **pvc-bundle** | Adds a PVC to a bundle as a member of the bundle and enters bundle-vc configuration mode in order to configure that PVC bundle member. |
| **show atm bundle** | Displays the bundle attributes assigned to each bundle VC member and the current working status of the VC members. |
| **show atm bundle statistics** | Displays statistics on the specified bundle. |

# bundle svc

To create or modify a switched virtual circuit (SVC) bundle, use the **bundlesvc**command in interface configuration mode. To remove the specified bundle, use the **no**form of this command.

**bundle svc** *bundle-name* **nsap** *nsap-address*

**no bundle svc** *bundle-name* **nsap** *nsap-address*

## Syntax Description

| | |
|---|---|
| *bundle-name* | Unique bundle name that identifies the SVC bundle in the router. The bundle names at each end of the virtual circuit (VC) must be the same. Length limit is 16 alphanumeric characters. |
| **nsap** *nsap-address* | Destination network services access point (NSAP) address of the SVC bundle. |

## Command Default

No SVC bundle is created or modified.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(4)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command causes the system to enter SVC-bundle configuration mode. The bundle name must be the same on both sides of the VC.

From SVC-bundle configuration mode, you can configure the characteristics and attributes of the bundle and its members, such as the encapsulation type for all virtual circuits (VCs) in the bundle, the bundle management parameters, the service type, and so on. Attributes and parameters you configure in SVC-bundle configuration mode are applied to all VC members of the bundle.

VCs in a VC bundle are subject to the following configuration inheritance guidelines (listed in order of next-highest precedence):

- VC configuration in bundle-VC mode

- Bundle configuration in bundle mode
- Subinterface configuration in subinterface mode

To display the status of bundles, use the **showatmbundlesvc** and **showatmbundlesvcstatistics**commands.

## Examples

The following example shows how to configure an SVC bundle called “sanfrancisco”:

```
interface ATM1/0.1 multipoint
 ip address 10.0.0.1 255.255.255.0
 atm esi-address 111111111111.11
 bundle svc sanfrancisco nsap 47.0091810000000003E3924F01.999999999999.99
  protocol ip 10.0.0.2
broadcast
 oam retry 4 3 10
 encapsulation aal5snap
 oam-bundle manage
 svc-bundle seven
  class-vc seven
 svc-bundle six
  class-vc six
 svc-bundle five
  class-vc five
 svc-bundle four
  class-vc four
 svc-bundle three
  class-vc three
 svc-bundle two
  class-vc two
 svc-bundle one
  class-vc one
 svc-bundle zero
  class-vc zero
```

## Related Commands

| Command | Description |
|---|---|
| **class-bundle** | Configures a VC bundle with the bundle-level commands contained in the specified VC class. |
| **oam-bundle** | Enables end-to-end F5 OAM loopback cell generation and OAM management for all VC members of a bundle, or for a VC class that can be applied to a VC bundle. |
| **pvc-bundle** | Adds a PVC to a bundle as a member of the bundle and enters bundle-vc configuration mode in order to configure that PVC bundle member. |
| **show atm bundle svc** | Displays the bundle attributes assigned to each bundle VC member and the current working status of the VC members. |
| **show atm bundle svc statistics** | Displays statistics on the specified bundle. |

# class (EtherSwitch)

To define a traffic classification for a policy to act on using the class-map name or access group, use the class command in policy-map configuration mode. To delete an existing class map, use the **no**form of this command.

**class** *class-map-name* [**access-group** *acl-index-or-name*]

**no class** *class-map-name*

## Syntax Description

| | |
|---|---|
| *class-map-name* | Name of the class map. |
| **access-group** *acl-index-or-name* | (Optional) Number or name of an IP standard or extended access control list (ACL). For an IP standard ACL, the index range is 1 to 99 and 1300 to 1999; for an IP extended ACL, the index range is 100 to 199 and 2000 to 2699. |

## Command Default

No policy-map class maps are defined.

## Command Modes

Policy-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(6)EA2 | This command was introduced. |
| 12.2(15)ZJ | This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |

## Usage Guidelines

Before you use the **class** (EtherSwitch) command, use the **policy-map** global configuration command to identify the policy map and to enter policy-map configuration mode. After you specify a policy map, you can configure a policy for new classes or modify a policy for any existing classes in that policy map. You attach the policy map to an interface by using the **service-policy**interface configuration command; however, you cannot attach one that uses an ACL classification to the egress direction.

The class name that you specify in the policy map ties the characteristics for that class to the class map and its match criteria as configured by using the **class-map** global configuration command.

The **class** (EtherSwitch) command performs the same function as the**class-map**global configuration command. Use the **class** (EtherSwitch) command when a new classification, which is not shared with any other ports, is needed. Use the **class-map** command when the map is shared among many ports.

**Note** In a policy map, the class named "class-default" is not supported. The Ethernet switch network module does not filter traffic on the basis of the policy map defined by the **classclass-default** policy-map configuration command.

After entering the **class** (EtherSwitch) command, you enter policy-map class configuration mode. When you are in this mode, these configuration commands are available:

- **default** --Sets a command to its default.
- **exit** --Exits policy-map class configuration mode and returns to policy-map configuration mode.
- **no** --Returns a command to its default setting.
- **police** --Defines a policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information, see the **police** command.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

**Note** For more information about configuring IP ACLs, refer to the "Configuring IP Services" chapter in the Cisco IOS IP Application Services Configuration Guide.

## Examples

The following example shows how to create a policy map named "policy1." When attached to the ingress port, it matches all the incoming traffic defined in class1 and polices the traffic at an average rate of 1 Mbps and bursts at 131072 bytes. Traffic exceeding the profile is dropped.

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# police 1000000 131072 exceed-action drop
Router(config-pmap-c)# exit
```

You can verify your settings by entering the **showpolicy-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to the class whose name you specify. |
| **match (class-map configuration)** | Defines the match criteria to classify traffic. |
| **police** | Configures traffic policing. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple interfaces to specify a service policy. |

| Command | Description |
|---|---|
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **show policy-map** | Displays QoS policy maps. |

# class (policy-map)

To specify the name of the class whose policy you want to create or change or to specify the default class (commonly known as the class-default class) before you configure its policy, use the **class**command in policy-map configuration mode. To remove a class from the policy map, use the **no** form of this command.

**class** {*class-name*| **class-default** [**fragment** *fragment-class-name*]} [**insert-before** *class-name*] [**service-fragment** *fragment-class-name*]

**no class** {*class-name*| **class-default**}

## Syntax Description

| | |
|---|---|
| *class-name* | Name of the class to be configured or whose policy is to be modified. The class name is used for both the class map and to configure a policy for the class in the policy map. |
| **class-default** | Specifies the default class so that you can configure or modify its policy. |
| **fragment** *f ragment-class-name* | (Optional) Specifies the default traffic class as a fragment, and names the fragment traffic class. |
| **insert-before** *class-name* | (Optional) Adds a class map between any two existing class maps.<br>Inserting a new class map between two existing class map provides more flexibility when modifying existing policy map configurations. Without this option, the class map is appended to the end of the policy map.<br>This keyword is supported only on flexible packet matching (FPM) policies. |
| **service-fragment** *fragment-class-name* | (Optional) Specifies that the class is classifying a collection of fragments. The fragments being classified by this class must all share the same *fragment-class-name*. |

## Command Default

No class is specified.

## Command Modes

Policy-map configuration (config-pmap)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE. |
| 12.0(7)S | This command was integrated into Cisco IOS Release 12.0(7)S. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.2(14)SX | Support for this command was introduced on Cisco 7600 routers. |
| 12.2(17d)SXB | This command was implemented on the Cisco 7600 router and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(18)SXE | The **class-default** keyword was added to the Cisco 7600 router. |
| 12.4(4)T | The**insert-before***class-name* option was added. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(31)SB2 | This command was introduced on the PRE3 for the Cisco 10000 series router. |
| 12.2(18)ZY | The **insert-before***class-name* option was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA). |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers. The **fragment***fragment-class-name* and *service-fragmentfragment-class-name* options were introduced. |

## Usage Guidelines

### Policy Map Configuration Mode

Within a policy map, the **class**(policy-map)command can be used to specify the name of the class whose policy you want to create or change. First, the policy map must be identified.

To identify the policy map (and enter the required policy-map configuration mode), use the **policy-map** command before you use the **class**(policy-map)command. After you specify a policy map, you can configure policy for new classes or modify the policy for any existing classes in that policy map.

### Class Characteristics

The class name that you specify in the policy map ties the characteristics for that class--that is, its policy--to the class map and its match criteria, as configured using the **class-map** command.

When you configure policy for a class and specify its bandwidth and attach the policy map to an interface, class-based weighted fair queueing (CBWFQ) determines if the bandwidth requirement of the class can be satisfied. If so, CBWFQ allocates a queue for the bandwidth requirement.

When a class is removed, available bandwidth for the interface is incremented by the amount previously allocated to the class.

The maximum number of classes that you can configure for a router--and, therefore, within a policy map--is 64.

**Predefined Default Class**

The **class-default** keyword is used to specify the predefined default class called class-default. The class-default class is the class to which traffic is directed if that traffic does not match any of the match criteria in the configured class maps.

**Tail Drop or WRED**

You can define a class policy to use either tail drop by using the **queue-limit** command or Weighted Random Early Detection (WRED) by using the **random-detect** command. When using either tail drop or WRED, note the following points:

- The **queue-limit** and **random-detect** commands cannot be used in the same class policy, but they can be used in two class policies in the same policy map.
- You can configure the **bandwidth** command when either the **queue-limit** command or the **random-detect** command is configured in a class policy. The **bandwidth** command specifies the amount of bandwidth allocated for the class.
- For the predefined default class, you can configure the **fair-queue** (class-default) command. The **fair-queue** command specifies the number of dynamic queues for the default class. The **fair-queue** command can be used in the same class policy as either the **queue-limit** command or the **random-detect** command. It cannot be used with the **bandwidth** command.

**Fragments**

A default traffic class is marked as a fragment within a policy map class statement using the **fragment**keyword. Multiple fragments can then be classified collectively in a separate policy map that is created using the **service-fragment** keyword. When fragments are used, default traffic classes marked as fragments have QoS applied separately from the non-default traffic classes.

When using fragments, note the following guidelines:

- Only default traffic classes can be marked as fragments.
- The**fragment***fragment-class-name*option within a default class statement marks that default class as a fragment.
- The**service-fragment***fragment-class-name*option when defining a class in a policy map is used to specify a class of traffic within the Modular QoS CLI that contains all fragments sharing the same *fragment-class-name*.
- Fragments can only be used within the same physical interface. Policy maps with fragments sharing the same *fragment-class-name* on different interfaces cannot be classified collectively using a class with the **service-fragment***fragment-class-name* option.

**Cisco 10000 Series Router**

The PRE2 allows you to configure 31 class queues in a policy map.

In a policy map, the PRE3 allows you to configure one priority level 1 queue, plus one priority level 2 queue, plus 12 class queues, plus one default queue.

**Cisco ASR 1000 Series Routers**

The maximum number of classes that you can configure for a Cisco ASR 1000 Series Router--and, therefore, within a policy map--is 8.

## Examples

The following example shows how to configure three class policies included in the policy map called policy1. Class1 specifies policy for traffic that matches access control list 136. Class2 specifies policy for traffic on interface ethernet101. The third class is the default class to which packets that do not satisfy configured match criteria are directed:

```
! The following commands create class-maps class1 and class2
! and define their match criteria:
class-map class1
 match access-group 136
class-map class2
 match input-interface ethernet101
! The following commands create the policy map, which is defined to contain policy
! specification for class1, class2, and the default class:
policy-map policy1
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap-c)# queue-limit 40
Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap-c)# random-detect
Router(config-pmap-c)# random-detect exponential-weighting-constant 10
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 16
Router(config-pmap-c)# queue-limit 20
```

- Class1--A minimum of 2000 kbps of bandwidth is expected to be delivered to this class in the event of congestion, and the queue reserved for this class can enqueue 40 packets before tail drop is enacted to handle additional packets.
- Class2--A minimum of 3000 kbps of bandwidth is expected to be delivered to this class in the event of congestion, and a weight factor of 10 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop.
- The default class--16 dynamic queues are reserved for traffic that does not meet the match criteria of other classes whose policy is defined by the policy map called policy1, and a maximum of 20 packets per queue is enqueued before tail drop is enacted to handle additional packets.

**Note** When the policy map that contains these classes is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed, taking into account all class policies and Resource Reservation Protocol (RSVP), if configured.

The following example shows how to configure policy for the default class included in the policy map called policy8. The default class has these characteristics:20 dynamic queues are available for traffic that does not meet the match criteria of other classes whose policy is defined by the policy map called policy8, and a weight factor of 14 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop:

```
Router(config)# policy-map policy8
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 20
Router(config-pmap-c)# random-detect exponential-weighting-constant 14
```

The following example shows how to configure policy for a class called acl136 included in the policy map called policy1. Class acl136 has these characteristics:a minimum of 2000 kbps of bandwidth is expected to be delivered to this class in the event of congestion, and the queue reserved for this class can enqueue 40 packets before tail drop is enacted to handle additional packets. Note that when the policy map that contains this class is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed, taking into account all class policies and RSVP, if configured:

```
Router(config)# policy-map policy1
Router(config-pmap)# class acl136
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap-c)# queue-limit 40
```

The following example shows how to configure policy for a class called int101 included in the policy map called policy8. Class int101 has these characteristics:a minimum of 3000 kbps of bandwidth are expected to be delivered to this class in the event of congestion, and a weight factor of 10 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop. Note that when the policy map that contains this class is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed:

```
Router(config)# policy-map policy8
Router(config-pmap)# class int101
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap-c)# random-detect exponential-weighting-constant 10
```

The following example shows how to configure policy for the **class-default** default class included in the policy map called policy1. The **class-default** default class has these characteristics:10 hashed queues for traffic that does not meet the match criteria of other classes whose policy is defined by the policy map called policy1; and a maximum of 20 packets per queue before tail drop is enacted to handle additional enqueued packets:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue
Router(config-pmap-c)# queue-limit 20
```

The following example shows how to configure policy for the **class-default** default class included in the policy map called policy8. The **class-default** default class has these characteristics:20 hashed queues for traffic that does not meet the match criteria of other classes whose policy is defined by the policy map called policy8; and a weight factor of 14 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop:

```
Router(config)# policy-map policy8
Router(config-pmap)# class class-default
Router(config-pmap-c)# fair-queue 20
Router(config-pmap-c)# random-detect exponential-weighting-constant 14
```

The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header:

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf
class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp
class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp
class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
Router(config-cmap)# match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster3
```

```
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030
policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
 drop
policy-map type access-control fpm-udp-policy
 class blaster3
 drop
policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy
interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

The following example shows how to create a fragment class of traffic to classify the default traffic class named BestEffort. All default traffic from the policy maps named subscriber1 and subscriber2 is part of the fragment default traffic class named BestEffort. This default traffic is then shaped collectively by creating a class called data that uses the **service-fragment** keyword and the **shape** command:

Note the following about this example:

- The *class-name* for each fragment default traffic class is “BestEffort.”
- The*class-name* of “BestEffort” is also used to define the class where the**service-fragment**keyword is entered. This class applies a shaping policy to all traffic forwarded using the fragment default traffic classes named “BestEffort.”

```
policy-map subscriber1
class voice
set cos 5
priority level 1
class video
set cos 4
priority level 2
class class-default fragment BestEffort
shape average 200
bandwidth remaining ratio 10
policy-map subscriber 2
class voice
set cos 5
priority level 1
class video
set cos 4
priority level 2
class class-default fragment BestEffort
shape average 200
bandwidth remaining ratio 10
policy-map input_policy
class class-default
set dscp default
policy-map main-interface
class data service-fragment BestEffort
shape average 400
interface portchannel1.1001
encapsulation dot1q 1001service-policy output subscriber1
service-policy input input_policy
interface portchannel1.1002
encapsulation dot1q 1002
service-policy output subscriber2
service-policy input input_policy
interface gigabitethernet 0/1
description member-link1
port channel 1
service-policy output main-interface
interface gigabitethernet 0/2
```

```
description member-link2
port channel 1
```
service-policy output main-interface

## Related Commands

| Command | Description |
|---|---|
| **bandwidth (policy-map class)** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map. |
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **fair-queue (class-default)** | Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **queue-limit** | Specifies or modifies the maximum number of packets the queue can hold for a class policy configured in a policy map. |
| **random-detect (interface)** | Enables WRED or DWRED. |
| **random-detect exponential-weighting-constant** | Configures the WRED and DWRED exponential weight factor for the average queue size calculation. |
| **random-detect precedence** | Configures WRED and DWRED parameters for a particular IP Precedence. |

# class-map arp-peruser

To create a class map to be used for matching Address Resolution Protocol (ARP) per-user packets, use the **class-maparp-perus**er command in global configuration mode. To disable this functionality, use the **no** form of the command.

**class-map arp-peruser**

**no class map arp-peruser**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No class map is configured.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRB | This command was introduced. |

## Usage Guidelines

Use this command to create an ARP class map when configuring CoPP.

## Examples

The following example shows how to create an ARP class-map:

```
Router(config)# class-map arp-peruser
Router(config-cmap)# match protocol arp
Router(config-cmap)# match subscriber access
```

## Related Commands

| Command | Description |
|---|---|
| **match protocol arp** | Matches ARP traffic to a policy map. |
| **match subscriber access** | Matches subscriber access traffic to a policy map. |

# class-bundle

To configure a virtual circuit (VC) bundle with the bundle-level commands contained in the specified VC class, use the **class-bundle** command in bundle or SVC-bundle configuration mode. To remove the VC class parameters from a VC bundle, use the **no** form of this command.

**class-bundle** *vc-class-name*

**no class-bundle** *vc-class-name*

## Syntax Description

| | |
|---|---|
| *vc-class-name* | Name of the VC class that you are assigning to your VC bundle. |

## Command Default

No VC class is assigned to the VC bundle.

## Command Modes

Bundle configuration SVC-bundle configuration

## Command History

| Release | Modification |
|---|---|
| 12.0T | This command was introduced, replacing the **class** command for configuring ATM VC bundles. |
| 12.0(26)S | This command was integrated into Cisco IOS Release 12.0(26)S and implemented on the Cisco 10000 series router. |
| 12.2(16)BX | This command was implemented on the ESR-PRE2. |
| 12.2(4)T | This command was made available in SVC-bundle configuration mode. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

To use this command, you must first enter the **bundle** or **bundlesvc**command to create the bundle and enter bundle or SVC-bundle configuration mode.

Use this command to assign a previously defined set of parameters (defined in a VC class) to an ATM VC bundle. Parameters set through bundle-level commands that are contained in a VC class are applied to the bundle and its VC members.

You can add the following commands to a VC class to be used to configure a VC bundle: **broadcast**, **encapsulation**, **inarp,oam-bundle**, **oamretry,** and **protocol**.

Bundle-level parameters applied through commands that are configured directly on a bundle supersede bundle-level parameters applied through a VC class by the **class-bundle** command. Some bundle-level parameters applied through a VC class or directly to the bundle can be superseded by commands that you directly apply to individual VCs in bundle-VC configuration mode.

## Examples

In the following example, a class called "class1" is created and then applied to the bundle called "bundle1":

```
! The following commands create the class class1:
vc-class atm class1
 encapsulation aal5snap
 broadcast
 protocol ip inarp
 oam-bundle manage 3
 oam 4 3 10
! The following commands apply class1 to the bundle called bundle1:
bundle bundle1
 class-bundle class1
```

With hierarchy precedence rules taken into account, VCs belonging to the bundle called "bundle1" will be characterized by these parameters: aal5snap, encapsulation, broadcast on, use of Inverse Address Resolution Protocol (Inverse ARP) to resolve IP addresses, and Operation, Administration, and Maintenance (OAM) enabled.

## Related Commands

| Command | Description |
|---|---|
| **broadcast** | Configures broadcast packet duplication and transmission for an ATM VC class, PVC, SVC, or VC bundle. |
| **bundle** | Creates a bundle or modifies an existing bundle to enter bundle configuration mode. |
| **bundle svc** | Creates an SVC bundle or modifies an existing SVC bundle. |
| **class-int** | Assigns a VC class to an ATM main interface or subinterface. |
| **class-vc** | Assigns a VC class to an ATM PVC, SVC, or VC bundle member. |
| **encapsulation** | Sets the encapsulation method used by the interface. |
| **inarp** | Configures the Inverse ARP time period for an ATM PVC, VC class, or VC bundle. |
| **oam-bundle** | Enables end-to-end F5 OAM loopback cell generation and OAM management for all VC members of a bundle, or for a VC class that can be applied to a VC bundle. |

| Command | Description |
|---|---|
| **oam retry** | Configures parameters related to OAM management for an ATM PVC, SVC, VC class, or VC bundle. |
| **protocol (ATM)** | Configures a static map for an ATM PVC, SVC, VC class, or VC bundle. Enables Inverse ARP or Inverse ARP broadcasts on an ATM PVC by configuring Inverse ARP either directly on the PVC, on the VC bundle, or in a VC class (applies to IP and IPX protocols only). |
| **pvc-bundle** | Adds a PVC to a bundle as a member of the bundle and enters bundle-vc configuration mode in order to configure that PVC bundle member. |

# class-map

To create a class map to be used for matching packets to a specified class and to enter QoS class-map configuration mode, use the **class-map** command in global configuration mode. To remove an existing class map from a device, use the **no** form of this command.

### Cisco 2600, 3660, 3845, 6500, 7200, 7401, and 7500 Series Routers

**class-map** [**type** {**stack**| **access-control**| **port-filter**| **queue-threshold**| **logging** *log-class*}] [**match-all**| **match-any**] *class-map-name*

**no class-map** [**type** {**stack**| **access-control**| **port-filter**| **queue-threshold**| **logging** *log-class*}] [**match-all**| **match-any**] *class-map-name*

### Cisco 7600 Series Routers

**class-map** *class-map-name* [**match-all**| **match-any**]

**no class-map** *class-map-name* [**match-all**| **match-any**]

### Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

**class-map** *class-map-name*

**no class-map** *class-map-name*

## Syntax Description

| | |
|---|---|
| **type** | (Optional) Specifies the class-map type. |
| **stack** | (Optional) Enables the flexible packet matching (FPM) functionality to determine the protocol stack to examine.<br>When you use the **load protocol** command to load protocol header description files (PHDFs) on the device, a stack of protocol headers can be defined so that the filter can determine which headers are present and in what order. |
| **access-control** | (Optional) Determines the pattern to look for in the configured protocol stack.<br>**Note** You must specify a stack class map (by using the **type stack** keywords) before specifying an access-control class map (by using the **type access-control** keywords). |
| **port-filter** | (Optional) Creates a port-filter class map that enables the TCP or UDP port policing of control plane packets. When this keyword is enabled, the command filters the traffic that is destined to specific ports on the control-plane host subinterface. |

| | |
|---|---|
| **queue-threshold** | (Optional) Enables queue thresholding, which limits the total number of packets for a specified protocol allowed in the control plane IP input queue. The queue-thresholding applies only to the control-plane host subinterface. |
| **logging** *log-class* | (Optional) Enables the logging of packet traffic on the control plane. The value for the *log-class* argument is the name of the log class. |
| **match-all** | (Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map based on the logical AND function. A packet must match all statements to be accepted. If you do not specify the **match-all** or **match-any** keyword, the default keyword used is **match-all**. |
| **match-any** | (Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map based on the logical OR function. A packet must match any of the match statements to be accepted. If you do not specify the **match-any** or **match-all** keyword, the default keyword is used **match-all**. |
| *class-map-name* | Name of the class for the class map. The class name is used for both the class map and to configure a policy for the class in the policy map.<br>**Note** You can enter the value for the *class-map-name* argument within quotation marks. The software does not accept spaces in a class map name entered without quotation marks. |

## Command Default

A class map is not configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE. |
| 12.0(7)S | This command was integrated into Cisco IOS Release 12.0(7)S. |

| Release | Modification |
|---|---|
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.2(14)SX | This command was integrated into Cisco IOS Release 12.2(14)SX and implemented on Cisco 7600 series routers. |
| 12.2(17d)SXB | This command was integrated into Cisco IOS Release 12.2(17d)SXB and implemented on Cisco 7600 series routers. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(4)T | This command was modified. The **stack** and **access-control** keywords were added to support FPM. The **port-filter** and **queue-threshold** keywords were added to support control-plane protection. |
| 12.4(6)T | This command was modified. The **logging** *log-class* keyword and argument pair was added to support control-plane packet logging. |
| 12.2(18)ZY | This command was modified. The **stack** and **access-control** keywords were integrated into Cisco IOS Release 12.2(18)ZY on Catalyst 6500 series switches equipped with the programmable intelligent services accelerator (PISA). |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 Series Aggregation Services Routers. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor with the *class-map-name* argument as the only syntax element available. |
| 12.2(58)SE | This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor with the *class-map-name* argument. |
| 12.2(33)SCF | This command was integrated into Cisco IOS Release 12.2(33)SCF. |
| 15.2(3)T | This command was modified. The software does not accept spaces in a class map name entered without quotation marks. |
| 15.1(2)SNG | This command was integrated into Cisco ASR 901 Series Aggregation Services Routers. |

## Usage Guidelines

### Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

Only the *class-map-name* argument is available.

### Cisco 2600, 3660, 3845, 6500, 7200, 7401, 7500, and ASR 1000 Series Routers

Use the **class-map** command to specify the class that you will create or modify to meet the class-map match criteria. This command enters QoS class-map configuration mode in which you can enter one or more **match**

commands to configure the match criteria for this class. Packets that arrive at either the input interface or the output interface (determined by how the **service-policy** command is configured) are checked against the match criteria that are configured for a class map to determine if packets belong to that class.

When configuring a class map, you can use one or more **match** commands to specify the match criteria. For example, you can use the **match access-group** command, the **match protocol** command, or the **match input-interface** command. The **match** commands vary according to the Cisco software release. For more information about match criteria and **match** commands, see the "Modular Quality of Service Command-Line Interface (CLI) (MQC)" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

### Cisco 7600 Series Routers

Apply the **class-map** command and commands available in QoS class-map configuration mode on a per-interface basis to define packet classification, marking, aggregating, and flow policing as part of a globally named service policy.

You can attach a service policy to an EtherChannel. Do not attach a service policy to a port that is a member of an EtherChannel.

When a device is in QoS class-map configuration mode, the following configuration commands are available:

- **description—**Specifies the description for a class-map configuration.
- **exit—**Exits from QoS class-map configuration mode.
- **match—**Configures classification criteria.
- **no—**Removes a match statement from a class map.

The following commands appear in the CLI help but are not supported on LAN interfaces or WAN interfaces on Optical Service Modules (OSMs):

- **destination-address mac** *mac-address*
- **input-interface** {*interface-type interface-number* | **null** *number* | **vlan** *vlan-id*}
- **protocol** *link-type*
- **source-address mac** *mac-address*

OSMs are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

Policy Feature Card (PFC) QoS does not support the following commands:

- **destination-address mac** *mac-address*
- **input-interface** {*interface-type interface-number* | **null** *number* | **vlan** *vlan-id*}
- **protocol** *link-type*
- **qos-group** *group-value*
- **source-address mac** *mac-address*

If you enter these commands, PFC QoS does not detect unsupported keywords until you attach a policy map to an interface. When you try to attach the policy map to an interface, an error message is generated. For additional information, see the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide* and Cisco IOS command references.

After configuring the class-map name and the device you can enter the **match access-group** and **match ip dscp** commands in QoS class-map configuration mode. The syntax for these commands is as follows:

**match** [**access-group** {*acl-index* | *acl-name*} | **ip dscp** | **precedence**} *value*]

See the table below for a description of **match** command keywords.

***Table 1: match command Syntax Description***

| Optional command | Description |
|---|---|
| **access-group** *acl-index* \| *acl-name* | (Optional) Specifies the access list index or access list names. Valid access list index values are from 1 to 2699. |
| **access-group** *acl-name* | (Optional) Specifies the named access list. |
| **ip dscp** *value1 value2 ... value8* | (Optional) Specifies IP differentiated services code point (DSCP) values to match. Valid values are from 0 to 63. You can enter up to eight DSCP values separated by spaces. |
| **ip precedence** *value1 value2 ... value8* | (Optional) Specifies the IP precedence values to match. Valid values are from 0 to 7. You can enter up to eight precedence values separated by spaces. |

## Examples

The following example shows how to specify class101 as the name of a class and define a class map for this class. The class named class101 specifies policy for the traffic that matches ACL 101.

```
Device(config)# class-map class101
Device(config-cmap)# match access-group 101
Device(config-cmap)# end
```

The following example shows how to define FPM traffic classes for slammer and UDP packets. The match criteria defined within class maps are for slammer and UDP packets with an IP length that does not exceed 404 (0x194) bytes, UDP port 1434 (0x59A), and pattern 0x4011010 at 224 bytes from the start of the IP header.

```
Device(config)# load protocol disk2:ip.phdf
Device(config)# load protocol disk2:udp.phdf
Device(config)# class-map type stack match-all ip-udp
Device(config-cmap)# description "match UDP over IP packets"
Device(config-cmap)# match field ip protocol eq 0x11 next udp
Device(config-cmap)#exit
Device(config)# class-map type access-control match-all slammer
Device(config-cmap)# description "match on slammer packets"
Device(config-cmap)# match field udp dest-port eq 0x59A
Device(config-cmap)# match field ip length eq 0x194
Device(config-cmap)# match start 13-start offset 224 size 4 eq 0x 4011010
Device(config-cmap)# end
```

The following example shows how to configure a port-filter policy to drop all traffic that is destined to closed or "nonlistened" ports except Simple Network Management Protocol (SNMP):

```
Device(config)# class-map type port-filter pf-class
Device(config-cmap)# match not port udp 123
```

```
Device(config-cmap)# match closed-ports
Device(config-cmap)# exit
Device(config)# policy-map type port-filter pf-policy
Device(config-pmap)# class pf-class
Device(config-pmap-c)# drop
Device(config-pmap-c)# end
```

The following example shows how to configure a class map named ipp5 and enter a match statement for IP precedence 5:

```
Device(config)# class-map ipp5
Device(config-cmap)# match ip precedence 5
```

## Examples

The following example shows how to set up a class map and match traffic classes for the 802.1p domain with packet class of service (CoS) values:

```
Device> enable
Device# configure terminal
Device(config)# class-map cos1
Device(config-cmap)# match cos 0
Device(config-pmap-c)# end
```

## Examples

The following example shows how to set up a class map and match traffic classes for the Multiprotocol Label Switching (MPLS) domain with packet experimental (EXP) values:

```
Device> enable
Device# configure terminal
Device(config)# class-map exp7
Device(config-cmap)# match mpls experimental topmost 2
Device(config-pmap-c)# end
```

## Related Commands

| Command | Description |
|---|---|
| **description** | Specifies the description for a class map or policy map configuration. |
| **drop** | Configures the traffic class to discard packets belonging to a specific class map. |
| **class (policy-map)** | Specifies the name of the class whose policy you want to create or change, and the default class before you configure its policy. |
| **load protocol** | Loads a PHDF onto a router. |
| **match** (**class-map**) | Configures the match criteria for a class map on the basis of port filter or protocol queue policies. |
| **match access-group** | Configures the match criteria for a class map on the basis of the specified ACL. |
| **match input-interface** | Configures a class map to use the specified input interface as a match criterion. |

| Command | Description |
|---|---|
| **match ip dscp** | Identifies one or more DSCP, AF, and CS value as a match criterion. |
| **match mpls experimental** | Configures a class map to use the specified EXP field value as a match criterion. |
| **match protocol** | Configures the match criteria for a class map on the basis of the specified protocol. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **protocol** | Configures a timer and authentication method for a control interface. |
| **qos-group** | Associates a QoS group value for a class map. |
| **service-policy** | Attaches a policy map to an input interface or VC or to an output interface or VC to be used as the service policy for that interface or VC. |
| **show class-map** | Displays class map information. |
| **show policy-map interface** | Displays statistics and configurations of input and output policies that are attached to an interface. |
| **source-address** | Configures the source-address control on a port. |

# class-map arp-peruser

To create a class map to be used for matching Address Resolution Protocol (ARP) per-user packets, use the **class-maparp-peruse**r command in global configuration mode. To disable, use the **no** form of the command.

**class-map arp-peruser**

**no class map arp-peruser**

## Syntax Description

| | |
|---|---|
| **arp per-user** | Specifies Address Resolution Protocol per user. |

## Command Default

Enabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRB | This command was introduced. |

## Usage Guidelines

Use this command to create an ARP class map when configuring CoPP.

## Examples

The following example shows creating an ARP class-map:

```
Router(config)#class-map arp-peruser
Router(config-cmap)#match protocol arp
Router(config-cmap)#match subscriber access
```

## Related Commands

| Command | Description |
|---|---|
| **match protocol arp** | Matches ARP traffic to a policy map. |
| **match subscriber access** | Matches subscriber access traffic to a policy map. |

# class type tag

To associate a class map with a policy map, use the **classtypetag**command in policy map configuration mode. To disassociate the command, use the **no** form of this command.

**class type tag** *class-name* [**insert-before** *class-name*]

**no class type tag** *class-name* [**insert-before** *class-name*]

## Syntax Description

| | |
|---|---|
| *class-name* | Name of the class map. |
| **insert-before** *class-name* | (Optional) Adds a class map between any two existing class maps.<br>**Note** Inserting a new class map between two existing class maps provides more flexibility when modifying existing policy map configurations. Without this option, the class map is appended to the end of the policy map. |

## Command Default

A class map is not associated with a policy map.

## Command Modes

Policy map configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

If this command is used and the class is not configured, an error is generated. The error may be something such as "% class map {*name* } not configured." If the class needs to be inserted before a specific class map, the **insert-before** keyword can be used. The **insert-before** keyword is typically needed if the administrator is configuring any per-host class maps and would like it inserted before a specific class map. The **classtypetag** command creates the policy-map class configuration mode. There can be multiple classes under the policy map.

## Examples

The following example shows how to associate the class map "usergroup1_class" with a policy map:

```
class type tag usergroup1_class
```

## Related Commands

| Command | Description |
|---|---|
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |

# clear control-plane

To clear counters for control-plane interfaces or subinterfaces, use the **clearcontrol-plane** command in privileged EXEC mode.

**clear control-plane** [*****| **aggregate**| **host**| **transit**| **cef-exception**]

## Syntax Description

| | |
|---|---|
| ***** | (Optional) Clears counters for all control-plane features. |
| **aggregate** | (Optional) Clears counters for all features on the control-plane aggregate path. |
| **host** | (Optional) Clears counters for all features on the control-plane host feature path. |
| **transit** | (Optional) Clears counters for all features on the control-plane transit feature path. |
| **cef-exception** | (Optional) Clears counters for all features on the control-plane CEF-exception feature path. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |

## Usage Guidelines

Use the **clearcontrol-plane** command to clear counters for all features on the control-plane interfaces or subinterfaces.

## Examples

The following example clears the counters for all features on the control-plane host feature path.

```
Router# clear control-plane host
```

## Related Commands

| Command | Description |
|---|---|
| **control-plane** | Enters control-plane configuration mode, which allows you to associate or modify attributes or parameters that are associated with the control plane of the device. |
| **debug control-plane** | Displays debugging output from the control-plane routines. |
| **show control-plane cef-exception counters** | Displays the control plane packet counters for the control-plane CEF-exception subinterface. |
| **show control-plane cef-exception features** | Displays the configured features for the control-plane CEF-exception subinterface. |
| **show control-plane counters** | Displays the control-plane packet counters for the aggregate control-plane interface. |
| **show control-plane features** | Displays the configured features for the aggregate control-plane interface. |
| **show control-plane host counters** | Displays the control-plane packet counters for the control-plane host subinterface. |
| **show control-plane host features** | Displays the configured features for the control-plane host subinterface. |
| **show control-plane host open-ports** | Displays a list of open TCP/UDP ports that are registered with the port-filter database. |
| **show control-plane transit counters** | Displays the control-plane packet counters for the control-plane transit subinterface. |
| **show control-plane transit features** | Displays the configured features for the control-plane transit subinterface. |

# clear ip nbar

To clear buffers, filters, and port statistics gathered by Network-Based Application Recognition (NBAR), use the **clear ip nbar** command in privileged EXEC mode.

**clear ip nbar** [**capture**| **filter**| **trace**{**detail**| **summary**}| **statistics**| **unclassified-port-stats**]

## Syntax Description

| | |
|---|---|
| **capture** | (Optional) Specifies the packet capture buffers. |
| **filter** | (Optional) Specifies the session selection filter. |
| **trace** | (Optional) Specifies state-graph tracing buffers. |
| **detail** | (Optional) Specifies detailed classification information of NBAR. |
| **summary** | (Optional) Specifies classification summary of NBAR. |
| **unclassified-port-stats** | (Optional) Specifies the port statistics for unclassified packets. |
| **statistics** | (Optional) Specifies NBAR statistics for packets. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRC | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SXI | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI. |
| 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |
| Cisco IOS XE Release 2.1 | This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers. |
| 15.2(4)M | This command was modified. The **statistics**, **trace**, and **detail** keywords were added. |

## Examples

The following example shows how to clear the port statistics gathered by NBAR:

```
Device# clear ip nbar unclassified-port-stats
```

The following example shows how to clear the statistics gathered by NBAR:

```
Device# clear ip nbar statistics
```

## Related Commands

| Command | Description |
|---|---|
| **clear ip nbar protocol-discovery** | Clears statistics gathered by the NBAR protocol discovery. |
| **show ip nbar statistics** | Displays statistics gathered by NBAR. |

# clear ip nbar protocol-discovery

To clear the statistics gathered by the network-based application recognition (NBAR) Protocol Discovery feature, use the **clearipnbarprotocol-discovery** command in privileged EXEC mode.

**clear ip nbar protocol-discovery** [**interface** *type number*]

## Syntax Description

| | |
|---|---|
| **interface** | (Optional) Specifies the type of interface to be configured. |
| *type* | (Optional) Type of interface. |
| *number* | (Optional) Interface or subinterface number. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M. |
| 12.2(33)SRC | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SXI | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI. |
| Cisco IOS XE Release 2.1 | This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers. |

## Usage Guidelines

Use the **clearipnbarprotocol-discovery** command to clear the statistics gathered by the NBAR Protocol Discovery feature. By default, this command clears the statistics for all the interfaces on which the protocol discovery feature is enabled.

## Examples

The following example shows how to clear the statistics gathered by the NBAR Protocol Discovery feature:

```
Router# clear ip nbar protocol-discovery interface serial 3/1
```

## Related Commands

| Command | Description |
|---|---|
| **clear ip nbar** | Clears the buffers, filters, and port statistics gathered by the NBAR feature. |

# clear ip rsvp authentication

To eliminate Resource Reservation Protocol (RSVP) security associations before their lifetimes expire, use the clear **iprsvpauthentication**command in privileged EXEC mode.

**clear ip rsvp authentication** [*ip-address*| *hostname*]

## Syntax Description

| | |
|---|---|
| *ip-address* | (Optional) Frees security associations with a specific neighbor. |
| *hostname* | (Optional) Frees security associations with a specific host. |

**Note** The difference between the*ip-address* and*hostname* arguments is the difference of specifying the neighbor by its IP address or by its name.

## Command Default

The default behavior is to clear all security associations.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

Use the clear **iprsvpauthentication** command for the following reasons:

- To eliminate security associations before their lifetimes expire
- To free up memory
- To resolve a problem with a security association being in some indeterminate state
- To force reauthentication of neighbors

You can delete all RSVP security associations if you do not enter an IP address or a hostname, or just the ones with a specific RSVP neighbor or host.

If you delete a security association, it is re-created as needed when the trusted RSVP neighbors start sending more RSVP messages.

## Examples

The following command shows how to clear all security associations before they expire:

```
Router# clear ip rsvp authentication
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp authentication lifetime** | Controls how long RSVP maintains security associations with other trusted RSVP neighbors. |
| **show ip rsvp authentication** | Displays the security associations that RSVP has established with other RSVP neighbors. |

# clear ip rsvp counters

To clear (set to zero) all IP Resource Reservation Protocol (RSVP) counters that are being maintained, use the **cleariprsvpcounters**command in privileged EXEC mode.

**clear ip rsvp counters [confirm]**

## Syntax Description

| | |
|---|---|
| **confirm** | (Optional) Requests a confirmation that all IP RSVP counters were cleared. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(14)ST | This command was introduced. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

This command allows you to set all IP RSVP counters to zero so that you can see changes easily.

## Examples

In the following example, all IP RSVP counters that are being maintained are cleared:

```
Router# clear ip rsvp counters
Clear rsvp counters [confirm]
```

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp counters** | Displays counts of RSVP messages that were sent and received. |

# clear ip rsvp hello instance counters

To clear (refresh) the values for hello instance counters, use the **cleariprsvphelloinstancecounters**command in privileged EXEC mode.

**clear ip rsvp hello instance counters**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(22)S | This command was introduced. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(31)SXH. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Examples

Following is sample output from the**showiprsvphelloinstancedetail** command and then the **cleariprsvphelloinstancecounters** command. Notice that the “Statistics” fields have been cleared to zero.

```
Router# show ip rsvp hello instance detail
Neighbor 10.0.0.2  Source  10.0.0.1
 State: UP      (for 2d18h)
 Type: PASSIVE  (responding to requests)
 I/F: Et1/1
 LSPs protecting: 0
 Refresh Interval (msec) (used when ACTIVE)
  Configured: 100
  Statistics: (from 2398195 samples)
   Min:      100
   Max:      132
   Average:  100
   Waverage: 100 (Weight = 0.8)
   Current:  100
 Src_instance 0xA9F07C13, Dst_instance 0x9BBAA407
 Counters:
 Communication with neighbor lost:
  Num times: 0
  Reasons:
   Missed acks:             0
   Bad Src_Inst received:   0
   Bad Dst_Inst received:   0
   I/F went down:           0
```

```
   Neighbor disabled Hello: 0
  Msgs Received:   2398194
   Sent:       2398195
   Suppressed: 0
Router# clear ip rsvp hello instance counters
Neighbor 10.0.0.2  Source  10.0.0.1
 State: UP      (for 2d18h)
 Type: PASSIVE  (responding to requests)
 I/F: Et1/1
 LSPs protecting: 0
 Refresh Interval (msec) (used when ACTIVE)
  Configured: 100
  Statistics:
   Min:        0
   Max:        0
   Average:    0
   Waverage:   0
   Current:    0
 Src_instance 0xA9F07C13, Dst_instance 0x9BBAA407
 Counters:
  Communication with neighbor lost:
  Num times: 0
  Reasons:
   Missed acks:             0
   Bad Src_Inst received:   0
   Bad Dst_Inst received:   0
   I/F went down:           0
   Neighbor disabled Hello: 0
  Msgs Received:   2398194
   Sent:       2398195
   Suppressed: 0
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello (configuration)** | Enables hello globally on a router. |
| **ip rsvp signalling hello (interface)** | Enables hello on an interface where you need Fast Reroute protection. |
| **ip rsvp signalling hello statistics** | Enables hello statistics on a router. |
| **show ip rsvp hello statistics** | Displays how long hello packets have been in the hello input queue. |

# clear ip rsvp hello instance statistics

To clear hello statistics for an instance, use the **cleariprsvphelloinstancestatistics**command in privileged EXEC mode.

**clear ip rsvp hello instance statistics**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Hello statistics are not cleared for an instance.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(22)S | This command was introduced. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(31)SXH. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Examples

This example shows sample output from the **showiprsvphellostatistics** command and the values in those fields after you enter the **cleariprsvphelloinstancestatistics** command.

```
Router# show ip rsvp hello statistics
 Status: Enabled
 Packet arrival queue:
  Wait times (msec)
   Current:0
   Average:0
   Weighted Average:0 (weight = 0.8)
   Max:4
  Current length: 0 (max:500)
 Number of samples taken: 2398525


Router# clear ip rsvp hello instance statistics
Status: Enabled
 Packet arrival queue:
  Wait times (msec)
   Current:0
   Average:0
```

```
  Weighted Average:0 (weight = 0.8)
  Max:0
 Current length: 0 (max:500)
Number of samples taken: 0
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello (configuration)** | Enables hello globally on a router. |
| **ip rsvp signalling hello (interface)** | Enables hello on an interface where you need Fast Reroute protection. |
| **ip rsvp signalling hello statistics** | Enables hello statistics on a router. |
| **show ip rsvp hello statistics** | Displays how long hello packets have been in the hello input queue. |

# clear ip rsvp hello statistics

To clear hello statistics globally, use the **cleariprsvphellostatistics**command in privileged EXEC mode.

**clear ip rsvp hello statistics**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Hello statistics are not globally cleared.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(22)S | This command was introduced. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2s | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(31)SXH. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

Use this command to remove all information about how long hello packets have been in the hello input queue.

## Examples

Following is sample output from the **showiprsvphellostatistics** command and the **cleariprsvphellostatistics** command. Notice that the values in the "Packet arrival queue" fields have been cleared.

```
Router# show ip rsvp hello statistics
Status: Enabled
 Packet arrival queue:
  Wait times (msec)
   Current:0
   Average:0
   Weighted Average:0 (weight = 0.8)
   Max:4
  Current length: 0 (max:500)
Number of samples taken: 2398525
Router# clear ip rsvp hello statistics
Status: Enabled
 Packet arrival queue:
  Wait times (msec)
   Current:0
   Average:0
```

```
  Weighted Average:0 (weight = 0.8)
  Max:0
 Current length: 0 (max:500)
Number of samples taken: 16
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello statistics** | Enables hello statistics on a router. |
| **show ip rsvp hello statistics** | Displays how long hello packets have been in the hello input queue. |

# clear ip rsvp high-availability counters

To clear (set to zero) the Resource Reservation Protocol (RSVP) traffic engineering (TE) high availability (HA) counters that are being maintained by a Route Processor (RP), use the **clear ip rsvp high-availability counters** command in privileged EXEC mode.

**clear ip rsvp high-availability counters**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was introduced. |
| 12.2(33)SRB | Support for In-Service Software Upgrade (ISSU) was added. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

Use the **clear ip rsvp high-availability counters**command to clear (set to zero) the HA counters, which include state, ISSU, resource failures, and historical information.

## Examples

The following example clears all the HA information currently being maintained by the RP:

```
Router# clear ip rsvp high-availability counters
```

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp high-availability counters** | Displays the RSVP TE HA counters that are being maintained by an RP. |

# clear ip rsvp msg-pacing

**Note** Effective with Cisco IOS Release 12.4(20)T, the **clearipr svpmsg-pacing**command is not available in Cisco IOS software. This command was replaced by the**clearipr svpsignallingrate-limit** command.

To clear the Resource Reservation Protocol (RSVP) message pacing output from the **showipr svpneighbor** command, use the **clearipr svpmsg-pacing** command in privileged EXEC mode.

**clear ip rsvp msg-pacing**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(14)ST | This command was introduced. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(13)T | This command was replaced by the**clearipr svpsignallingrate-limit** command. |
| 12.4(20)T | This command was removed. |

## Examples

The following example clears the RSVP message pacing output:

```
Router# clear ip rsvp msg-pacing
```

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp counters** | Displays the number of RSVP messages that were sent and received. |
| **show ip rsvp neighbor** | Displays the current RSVP neighbors and indicates whether the neighbor is using IP or UDP encapsulation for a specified interface or for all interfaces. |

# clear ip rsvp reservation

To remove Resource Reservation Protocol (RSVP) RESV-related receiver information currently in the database, use the **cleariprsvpreservation**command in EXEC mode.

**clear ip rsvp reservation** {*session-ip-address sender-ip-address* {**tcp**| **udp**| *ip-protocol*} *session-dport sender-sport*| ***}

## Syntax Description

| | |
|---|---|
| *session-ip-address* | For unicast sessions, this is the address of the intended receiver; for multicast sessions, it is the IP multicast address of the session. |
| *sender-ip-address* | The IP address of the sender. |
| **tcp** \| **udp** \| *ip-protocol* | TCP, User Datagram Protocol (UDP), or IP protocol in the range from 0 to 65535. |
| *session-dport* | The destination port.<br>**Note** Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If destination is zero, source must be zero, and the implication is that ports are not checked. If destination is nonzero, source must be nonzero (except for wildcard filter (wf) reservations, for which the source port is always ignored and can therefore be zero). |
| *sender-sport* | The source port.<br>**Note** Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If destination is zero, source must be zero, and the implication is that ports are not checked. If destination is nonzero, source must be nonzero (except for wildcard filter (wf) reservations, for which the source port is always ignored and can therefore be zero). |
| * | Wildcard used to clear all senders. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **clearipsvpreservation**command to remove the RESV-related sender information currently in the database so that when reservation requests arrive, based on the RSVP admission policy, the relevant ones can be reestablished.

Whenever you change the clockrate or bandwidth of an interface, RSVP does not update its database to reflect the change. This is because such a change requires that RSVP reestablish reservations based on the new clockrate or bandwidth value and arbitrarily dropping some reservations while retaining others is not desired. The solution is to clear the RESV state by issuing the **clearipsvpreservation**command.

The **clearipsvpreservation**command clears the RESV state from the router on which you issued the command and causes the router to send a PATH TEAR message to the upstream routers thereby clearing the RESV state for that reservation on all the upstream routers.

## Examples

The following example clears all the RESV-related receiver information currently in the database:

```
Router# clear ip rsvp reservation *
```

The following example clears all the RESV-related receiver information for a specified reservation currently in the database:

```
Router# clear ip rsvp reservation 10.2.1.1 10.1.1.2 udp 10 20
```

## Related Commands

| Command | Description |
|---|---|
| **clear ip rsvp sender** | Removes RSVP PATH-related sender information currently in the database. |

# clear ip rsvp sender

To remove Resource Reservation Protocol (RSVP) PATH-related sender information currently in the database, use the **clearipr svpsender**command in EXEC mode.

**clear ip rsvp sender** {*session-ip-address sender-ip-address* {**tcp**| **udp**| *ip-protocol*} *session-dport sender-sport*| *****}

## Syntax Description

| | |
|---|---|
| *session-ip-address* | For unicast sessions, this is the address of the intended receiver; for multicast sessions, it is the IP multicast address of the session. |
| *sender-ip-address* | The IP address of the sender. |
| **tcp** \| **udp** \| *ip-protocol* | TCP, User Datagram Protocol (UDP), or IP protocol in the range from 0 to 65535. |
| *session-dport* | The destination port.<br>**Note** Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If destination is zero, source must be zero, and the implication is that ports are not checked. If destination is nonzero, source must be nonzero (except for wildcard filter (wf) reservations, for which the source port is always ignored and can therefore be zero). |
| *sender-sport* | The source port.<br>**Note** Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If destination is zero, source must be zero, and the implication is that ports are not checked. If destination is nonzero, source must be nonzero (except for wildcard filter (wf) reservations, for which the source port is always ignored and can therefore be zero). |
| * | Wildcard used to clear all senders. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **clearipsvpsender** command to remove the PATH-related sender information currently in the database so that when reservation requests arrive, based on the RSVP admission policy, the relevant ones can be reestablished.

Whenever you change the clockrate or bandwidth of an interface, RSVP does not update its database to reflect the change. This is because such a change requires that RSVP reestablish reservations based on the new clockrate or bandwidth value and arbitrarily dropping some reservations while retaining others is not desired. The solution is to clear the PATH state by issuing the **clearipsvpsender** command.

The **clearipsvpsender** command clears the PATH state from the router on which you issued the command and causes the router to send a PATH TEAR message to the downstream routers thereby clearing the PATH state for that reservation on all the downstream routers.

## Examples

The following example clears all the PATH-related sender information currently in the database:

```
Router# clear ip rsvp sender *
```

The following example clears all the PATH-related sender information for a specified reservation currently in the database:

```
Router# clear ip rsvp sender 10.2.1.1 10.1.1.2 udp 10 20
```

## Related Commands

| Command | Description |
|---|---|
| **clear ip rsvp reservation** | Removes RSVP RESV-related receiver information currently in the database. |

# clear ip rsvp signalling fast-local-repair statistics

To clear (set to zero) the Resource Reservation Protocol (RSVP) fast local repair (FLR) counters, use the **cleariprsvpsignallingfast-local-repairstatistics** command in user EXEC or privileged EXEC mode.

**clear ip rsvp signalling fast-local-repair statistics**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The default is to clear all the RSVP FLR counters.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRB | This command was introduced. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

Use the **cleariprsvpsignallingfast-local-repairstatistics**command to set all the RSVP FLR counters to zero. The statistics include information about FLR procedures such as the current state, the start time, and the repair rate.

## Examples

The following example clears all the RSVP FLR counters being maintained in the database:

```
Router# clear ip rsvp signalling fast-local-repair statistics
```

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp signalling fast-local-repair** | Displays FLR-related information. |

# clear ip rsvp signalling rate-limit

To clear (set to zero) the number of Resource Reservation Protocol (RSVP) messages that were dropped because of a full queue, use the **cleariprsvpsignallingrate-limit** command in privileged EXEC mode.

**clear ip rsvp signalling rate-limit**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. This command replaces the **cleariprsvpmsg-pacing** command. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

Use the **cleariprsvpsignallingrate-limit** command to clear the counters recording dropped messages.

## Examples

The following command shows how to clear all dropped messages:

```
Router# clear ip rsvp signalling rate-limit
```

## Related Commands

| Command | Description |
|---|---|
| **debug ip rsvp rate-limit** | Displays debug messages for RSVP rate-limiting events. |
| **ip rsvp signalling rate-limit** | Controls the transmission rate for RSVP messages sent to a neighboring router during a specified amount of time. |
| **show ip rsvp signalling rate-limit** | Displays rate-limiting parameters for RSVP messages. |

# clear ip rsvp signalling refresh reduction

To clear (set to zero) the counters associated with the number of retransmissions and the number of out-of-order Resource Reservation Protocol (RSVP) messages, use the **clearipr svpsignallingrefreshreduction** command in EXEC mode.

**clear ip rsvp signalling refresh reduction**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |

## Usage Guidelines

Use the **clearipr svpsignallingrefreshreduction**command to clear the counters recording retransmissions and out-of-order RSVP messages.

## Examples

The following command shows how all the retransmissions and out-of-order messages are cleared:

```
Router# clear ip rsvp signalling refresh reduction
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling refresh reduction** | Enables refresh reduction. |
| **show ip rsvp signalling refresh reduction** | Displays refresh-reduction parameters for RSVP messages. |

# clear mls qos

To clear the multilayer switching (MLS) aggregate-quality of service (QoS) statistics, use the **clearmlsqos** command in privileged EXEC mode.

**clear mls qos** [**ip**| **ipx**| **mac**| **mpls**| **ipv6**| **arp** [*interface-type interface-number*| **null** *interface-number*| **port-channel** *number*| **vlan** *vlan-id*]]

## Syntax Description

| | |
|---|---|
| **ip** | (Optional) Clears MLS IP aggregate-QoS statistics. |
| **ipx** | (Optional) Clears MLS IPX aggregate-QoS statistics. |
| **mac** | (Optional) Clears MLS MAC aggregate-QoS statistics. |
| **mpls** | (Optional) Clears MLS MPLS aggregate-QoS statistics. |
| **ipv6** | (Optional) Clears MLS IPv6 aggregate QoS statistics. |
| **arp** | (Optional) Clears MLS ARP aggregate QoS statistics. |
| *interface-type* | (Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, and **tengigabitethernet**. See the "Usage Guidelines" section for additional valid values. |
| *interface-number* | (Optional) Module and port number; see the "Usage Guidelines" section for valid values. |
| **null** *interface-number* | (Optional) Specifies the null interface; the valid value is 0 . |
| **port-channel** *number* | (Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 256. |
| **vlan** *vlan-id* | (Optional) Specifies the VLAN ID; valid values are from 1 to 4094. |

## Command Default

This command has no default settings.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 2. |
| 12.2(17a)SX | This command was changed to include the **mpls** keyword . |
| 12.2(17d)SXB | Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB. |
| 12.2(18)SXD | This command was changed to include the **arp** keywor d. |
| 12.2(18)SXE | This command was changed to include the **ipv6**and **arp** k eywor ds on the Supervisor Engine 2 only. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

The valid values for *interface-type* include th e **ge-wan**, **atm**, and **pos** keywords that are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The **ipx** keyword is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

The **ipv6** and **arp** keywo r ds are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

If you enter the **clearmlsqos** command with no arguments, the global and per-interface aggregate QoS counters for all protocols are cleared.

If you do not enter an interface type, the protocol aggregate-QoS counters for all interfaces are cleared.

**Note** Entering the **clearmlsqos** command affects the policing token bucket counters and might briefly allow traffic to be forwarded that would otherwise be policed.

## Examples

This example shows how to clear the global and per-interface aggregate-QoS counters for all protocols:

```
Router# clear mls qos
```

This example shows how to clear the specific protocol aggregate-QoS counters for all interfaces:

```
Ro
uter# clear mls qos ip
```

## Related Commands

| Command | Description |
|---|---|
| **show mls qos** | Displays MLS QoS information. |

# clear service-group traffic-stats

To clear the traffic statistics for one or all service groups, use the **clearservice-grouptraffic-stats**command in privileged EXEC mode.

**clear service-group traffic-stats** [**group** *service-group-identifier*]

## Syntax Description

| | |
|---|---|
| **group** | (Optional) Service group. |
| *service-group-identifier* | (Optional) Service group number. Enter the number of the service group for which you want to clear statistics. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRE | This command was introduced. |

## Usage Guidelines

If a service group number is not specified, statistics for all service groups are cleared.

**Note** Clearing the traffic statistics for the service group does not clear the traffic statistics for the group members. To clear the traffic statistics for the group members, use the **clearethernetserviceinstance** command. For more information about the **clearethernetserviceinstance**command, see the *Cisco IOS Carrier Ethernet Command Reference*.

## Examples

The following shows how to clear the traffic statistics for all service groups:

```
Router> enable
Router# clear service-group traffic-stats
```

## Related Commands

| Command | Description |
|---|---|
| **clear ethernet service instance** | Clears Ethernet service instance attributes such as MAC addresses and statistics or purges Ethernet service instance errors. |

# compression header ip

To configure Real-Time Transport Protocol (RTP) or TCP IP header compression for a specific class, use the **compressionheaderip** command in policy-map class configuration mode. To remove RTP or TCP IP header compression for a specific class, use the **no** form of this command.

**compression header ip** [**rtp**| **tcp**]

**no compression header ip**

## Syntax Description

| | |
|---|---|
| **rtp** | (Optional) Configures RTP header compression. |
| **tcp** | (Optional) Configures TCP header compression. |

## Command Default

If you do not specify either RTP or TCP header compression (that is, you press the enter key after the command name) both RTP and TCP header compressions are configured. This is intended to cover the “all compressions” scenario.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |

## Usage Guidelines

Using any form of the **compressionheaderip**commandoverrides any previously entered form.

The **compressionheaderip**commandcan be used at any level in the policy map hierarchy configured with the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) feature.

## Examples

In the following example, the **compressionheaderip** command has been configured to use RTP header compression for a class called “class1”. Class1 is part of policy map called “policy1”.

```
Router(config)# policy-map policy1
Router(config-pmap)# class-map class1
Router(config-pmap-c)# compression header ip rtp
Router(config-pmap-c)# end
```

## Related Commands

| Command | Description |
|---|---|
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map class** | Displays the configuration for the specified class of the specified policy map. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# control-plane

To enter control-plane configuration mode, which allows users to associate or modify attributes or parameters (such as a service policy) that are associated with the control plane of the device, use the **control-plane**command in global configuration mode. To remove an existing control-plane configuration from the router, use the **no**form of this command.

### Syntax for T Releases

**control-plane** [**host**| **transit**| **cef-exception**]

**no control-plane** [**host**| **transit**| **cef-exception**]

### Syntax for 12.0S Releases

**control-plane** [**slot** *slot-number*] [**host**| **transit**| **cef-exception**]

**no control-plane** [**slot** *slot-number*] [**host**| **transit**| **cef-exception**]

### Syntax for 12.2S Releases for Cisco 7600 Series Routers

**control-plane**

**no control-plane**

### Syntax for ASR 1000 Series Routers

**control-plane [host]**

**no control-plane [host]**

## Syntax Description

| | |
|---|---|
| **host** | (Optional) Applies policies to host control-plane traffic. |
| **transit** | (Optional) Applies policies to transit control-plane traffic. |
| **cef-exception** | (Optional) Applies policies to CEF-exception control-plane traffic. |
| **slot** *slot-number* | (Optional) Specifies the slot number for the line card to which you want to attach a QoS policy to configure distributed Control-Plane (CP) services. |

## Command Default

No control-plane service policies are defined.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(18)S | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |
| 12.0(29)S | This command was integrated into Cisco IOS Release 12.0(29)S. |
| 12.0(30)S | The **slot***slot-number* parameter was added to configure distributed Control-Plane (CP) services. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.4(4)T | The **host**,**transit**, and **cef-exception**keywords were added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| Cisco IOS XE Release 2.2 | This command was implemented on Cisco ASR 1000 series routers. |

## Usage Guidelines

After you enter the **control-plane** command, you can apply a control-plane policing (CoPP), port-filter, or queue-threshold policy to police traffic destined for the control plane. You can define aggregate CoPPs for the route processor (RP) and configure a service policy to police all traffic destined to the control plane:

- From all line cards on the router (aggregate CP services)
- From all interfaces on a line card (distributed CP services)

Aggregate CP services manage traffic destined for the control plane and received on the central switch engine from all line cards in the router.

Distributed CP services manage CP traffic from interfaces on a specified line card before CP packets are forwarded to the central switch engine where aggregate CP services are applied.

**Note** On the Cisco 12000 series Internet router, you can combine distributed and aggregate CP services to protect the control plane from DoS attacks and provide packet QoS. The **slot***slot-number* parameter is used only for distributed CP services configurations.

Control-plane policing includes enhanced control-plane functionality. It provides a mechanism for early dropping of packets directed toward closed or nonlistened Cisco IOS TCP/UPD ports on the router. It also provides the ability to limit protocol queue usage such that no single misbehaving protocol process can wedge the control-plane interface hold queue.

**Note** The **control-plane**command is supported by Cisco IOS Release 12.2S only for the Cisco 7600 router. For other Cisco IOS releases, the Cisco 7600 supports only the **nocontrol-plane** command to discontinue a previously existing configuration condition.

With this enhancement, you can classify control-plane traffic into different categories of traffic. These categories are as follows:

- Control-plane host subinterface--Subinterface that receives all control-plane IP traffic that is directly destined for one of the router interfaces. Examples of control-plane host IP traffic include tunnel termination traffic, management traffic, or routing protocols such as SSH, SNMP, BGP, OSPF, and EIGRP. All host traffic terminates on and is processed by the router. Most control-plane protection features and policies operate strictly on the control-plane host subinterface. Since most critical router control-plane services, such as routing protocols and management traffic, are received on the control-plane host subinterface, it is critical to protect this traffic through policing and protection policies. CoPP, port-filtering, and per-protocol queue thresholding protection features can be applied on the control-plane host subinterface.
- Control-plane transit subinterface--Subinterface that receives all control-plane IP traffic that is software switched by the route processor. This means packets not directly destined to the router itself but rather traffic traversing through the router. Nonterminating tunnels handled by the router are an example of this type of control-plane traffic. Control-plane protection allows specific aggregate policing of all traffic received at this subinterface.
- Control-plane CEF-exception subinterface--Subinterface that receives all traffic that is either redirected as a result of a configured input feature in the CEF packet forwarding path for process switching or directly enqueued in the control-plane input queue by the interface driver (for example, ARP, L2 keepalives, and all non-IP host traffic). Control-plane protection allows specific aggregate policing of this specific type of control-plane traffic.

## Examples

The following example shows how to configure trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 to forward Telnet packets to the control plane without constraint, while allowing all remaining Telnet packets to be policed at the specified rate. The QoS policy is then applied for aggregate CP services to all packets that are entering the control plane from all line cards in the router.

```
! Allow 10.1.1.1 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate-limit all other Telnet traffic.
Router(config)# access-list 140 permit tcp any any eq telnet
! Define class map “telnet-class.”
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-in
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define aggregate control-plane service for the active route processor.
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-in
Router(config-cp)# end
```

The next example also shows how to configure trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 to forward Telnet packets to the control plane without constraint, while allowing all remaining Telnet packets that enter through slot 1 to be policed at the specified rate. The QoS policy is applied for distributed CP services to all packets that enter through the interfaces on the line card in slot 1 and that are destined for the control plane:

```
! Allow 10.1.1.1 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate-limit all other Telnet traffic.
Router(config)# access-list 140 permit tcp any any eq telnet
! Define class map “telnet-class.”
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-in
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define aggregate control-plane service for the active route processor.
Router(config)# control-plane slot 1
Router(config-cp)# service-policy input control-plane-in
Router(config-cp)# end
```

The following example shows how to apply an aggregate CoPP policy to the host control-plane traffic by applying it to the host control-plane feature path:

```
Router(config)# control-plane host
Router(config-cp)# service-policy input cpp-policy-host
```

The following example shows how to apply an aggregate CoPP policy to the transit control-plane traffic by applying it to the control-plane transit feature path:

```
Router(config)# control-plane transit
Router(config-cp)# service-policy input cpp-policy-transit
```

The following example shows how to apply an aggregate CoPP policy to the CEF-exception control-plane traffic by applying it to the control-plane CEF-exception feature path:

```
Router(config)# control-plane cef-exception
Router(config-cp)# service-policy input cpp-policy-cef-exception
```

## Related Commands

| Command | Description |
|---|---|
| **class (policy-map)** | Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy. |
| **class-map** | Accesses the QoS class-map configuration mode to configure QoS class maps. |
| **drop** | Configures a traffic class to discard packets that belonging to a specific class. |
| **match access-group** | Configures the match criteria for a class map on the basis of the specified ACL. |

| Command | Description |
|---|---|
| **policy-map** | Accesses QoS policy-map configuration mode to configure the QoS policy map. |
| **service-policy (control-plane)** | Attaches a policy map to the control plane for aggregate or distributed control-plane services. |
| **show policy-map control-plane** | Displays the configuration of a class or all classes for the policy map attached to the control plane. |

# copy interface

To configure a traffic class to copy packets belonging to a specific class to the interface that is specified in the command, use the **copyinterface** command in policy-map class configuration mode. To prevent the packets from getting copied, use the **no** form of the command.

**copy interface** *interface type number*

**no copy interface** *interface type number*

## Syntax Description

| | |
|---|---|
| *interface type number* | Type and number of the interace to which the packets need to be sent. |

## Command Default

If this command is not specified, the packets are not copied to an interface.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.2(18)ZYA1 | This command was introduced. |

## Usage Guidelines

Use this command to copy packets to a predefined interface. The original packet goes to the predefined destination and the copied packet goes to the target interface. You can also configure the **copyinterface** command with the**log** command but not with a **drop** or **redirectinterface**command. This command cannot be configured with a service policy for a stack class. The packets can be copied only to the following interfaces:

- Ethernet
- Fast Ethernet
- Gigabit Ethernet
- Ten Gigabit Ethernet

## Examples

In the following example, a traffic class called cmtest has been created and configured for use in a policy map called pmtest. The policy map (service policy) is attached to FastEthernet interface 4/18. All packets in the cmtest class are copied to FastEthernet interface 4/15.

```
Router(config)# policy-map type access-control pmtest
Router(config-pmap)# class cmtest
Router(config-pmap-c)# copy interface FastEthernet 4/15
Router(config-pmap-c)# log
Router(config-pmap-c)# exit
Router(config)# interface FastEthernet 4/18
```

```
Router(config-if)#
service-policy input pmtest
```

## Related Commands

| Command | Description |
|---|---|
| **log** | Generates a log of messages in the policy-map class configuration mode or class-map configuration mode. |
| **show class-map** | Displays all class maps and their matching criteria. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# custom-queue-list

**Note** Effective with Cisco IOS XE Release 2.6 and Cisco IOS Release 15.1(3)T, the **custom-queue-list** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

**Note** Effective with Cisco IOS XE Release 3.2S, the **custom-queue-list**command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To assign a custom queue list to an interface, use the**custom-queue-list** command in interface configuration mode. To remove a specific list or all list assignments, use the **no** form of this command.

**custom-queue-list** [ *list-number* ]

**no custom-queue-list** [ *list-number* ]

## Syntax Description

| | |
|---|---|
| *list-number* | Any number from 1 to 16 for the custom queue list. |

## Command Default

No custom queue list is assigned.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.6 | This command was modified. This command was hidden. |

| Release | Modification |
|---|---|
| 15.1(3)T | This command was modified. This command was hidden. |
| Cisco IOS XE Release 3.2S | This command was replaced by an MQC command (or sequence of MQC commands). |

## Usage Guidelines

Only one queue list can be assigned per interface. Use this command in place of the **priority-listinterface**command (not in addition to it). Custom queueing allows a fairness not provided with priority queueing. With custom queueing, you can control the bandwidth available on the interface when the interface is unable to accommodate the aggregate traffic enqueued. Associated with each output queue is a configurable byte count, which specifies how many bytes of data should be delivered from the current queue by the system before the system moves on to the next queue. When a particular queue is being processed, packets are sent until the number of bytes sent exceeds the queue byte count or until the queue is empty.

Use the**showqueueingcustom**and**showinterfaces** commands to display the current status of the custom output queues.

## Examples

In the following example, custom queue list number 3 is assigned to serial interface 0:

```
interface serial 0
 custom-queue-list 3
```

## Related Commands

| Command | Description |
|---|---|
| **priority-list interface** | Establishes queueing priorities on packets entering from a given interface. |
| **queue-list default** | Assigns a priority queue for those packets that do not match any other rule in the queue list. |
| **queue-list interface** | Establishes queueing priorities on packets entering on an interface. |
| **queue-list queue byte-count** | Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle. |
| **queue-list queue limit** | Designates the queue length limit for a queue. |
| **show interfaces** | Displays statistics for all interfaces configured on the router or access server. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# D through F


- default ip nbar protocol-pack, page 117
- description (class-map), page 118
- description (service group), page 120
- df, page 121
- disconnect qdm, page 122
- drop, page 124
- dscp, page 126
- estimate bandwidth, page 129
- exponential-weighting-constant, page 131
- fair-queue (class-default), page 133
- fair-queue (DWFQ), page 136
- fair-queue (policy-map class), page 139
- fair-queue (WFQ), page 141
- air-queue aggregate-limit, page 148
- fair-queue individual-limit, page 150
- fair-queue limit, page 152
- fair-queue qos-group, page 154
- fair-queue tos, page 156
- fair-queue weight, page 158
- feedback, page 160
- frame-relay interface-queue priority, page 162
- frame-relay ip rtp compression-connections, page 165
- frame-relay ip rtp header-compression, page 167
- frame-relay ip rtp priority, page 169

- frame-relay ip tcp compression-connections, page 173
- frame-relay ip tcp header-compression, page 175
- frame-relay map ip compress, page 177
- frame-relay map ip nocompress, page 179
- frame-relay map ip rtp header-compression, page 181
- group (service group), page 184
- hw-module slot (ESP Scheduling), page 186
- hw-module subslot (Channelized SPA Scheduling), page 189

# default ip nbar protocol-pack

To load the base version of the protocol pack that is present in the Cisco IOS image of the Cisco router and to remove all other protocol packs, use the **default ip nbar protocol-pack** command in global configuration mode.

**default ip nbar protocol-pack** [ *protocol-pack* ]

## Syntax Description

| | |
|---|---|
| *protocol-pack* | (Optional) Protocol pack file path and name. |

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.3S | This command was introduced. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T. |

## Usage Guidelines

The protocol pack is a single compressed file that contains multiple Protocol Description Language (PDL) files and a manifest file. Before the protocol pack was introduced, PDLs had to be loaded separately. With network-based application recognition (NBAR) protocol pack, a set of protocols can be loaded, which helps NBAR to recognize additional protocols for classification on your network.

When the **default ip nbar protocol-pack** command is used, all protocol packs are removed from the router, except the base version that is provided with the Cisco IOS image in the router.

## Examples

The following example shows how to load the default protocol pack and remove all other protocol packs:

```
Router# configure terminal
Router(config)# default ip nbar protocol-pack
```

## Related Commands

| Command | Description |
|---|---|
| **ip nbar protocol-pack** | Loads a protocol pack. |
| **show ip nbar protocol-pack** | Displays protocol pack information. |

# description (class-map)

To add a description to the class map or the policy map, use the **description**command in class-map configuration or policy-map configuration mode. To remove the description from the class map or the policy map, use the **no** form of this command.

**description** *character-string*

**no description**

## Syntax Description

| | |
|---|---|
| *character-string* | Comment or a description that is added to the class map or the policy map. The character-string cannot exceed 161 characters. |

## Command Default

If this command is not issued, a description does not exist.

## Command Modes

Class-map configuration (config-cmap)

Policy-map configuration (config-pmap)

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |
| 12.2(18)ZY | This command was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA). |

## Usage Guidelines

The **description** command is meant solely as a comment to be put in the configuration to help you remember information about the class map or policy map, such as which packets are included within the class map.

## Examples

The following example shows how to specify a description within the class map “ip-udp” and the policy map “fpm-policy”:

```
class-map type stack match-all ip-udp
 description “match UDP over IP packets”
 match field ip protocol eq 0x11 next udp
!
policy-map type access-control fpm-policy
 description “drop worms and malicious attacks”
 class ip-udp
 service-policy fpm-udp-policy
!
!
```

```
interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |

# description (service group)

To add a service-group description, use the **description** command in service-group configuration mode. To remove a service-group description, use the **no** form of this command.

**description** *descriptive-text*

**no description**

## Syntax Description

| | |
|---|---|
| *descriptive-text* | Service-group description. Enter up to 240 characters to describe the service group. |

## Command Default

A service-group description is not added.

## Command Modes

Service-group configuration (config-service-group)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRE | This command was introduced. |

## Usage Guidelines

Use the **description** (service group) command to provide additional information about the service group, such as the account number, location, or subscriber name.

## Examples

The following example shows how to create service group 1 and how to add information that identifies the subscriber account number in the description:

```
Router> enable
Router# configure terminal
Router(config)# service-group 1
Router(config-service-group)# description
 subscriber account number 105AB1
Router(config-service-group)# end
```

# df

To change the algorithm for computing the delay factor (DF), use the **df** command in monitor parameters mode. To use the default DF algorithm (rfc4445) use the **no** form of this command.

**df** *algorithm_name*

**no df** *algorithm_name*

## Syntax Description

| | |
|---|---|
| *algorithm_name* | *The algorithm used to compute the delay factor. These algorithms are supported:*<br>• **ipdv**<br>• **rfc4445** |

## Command Default

The rfc4445 algorithm is used.

## Command Modes

Monitor parameter (config-map-c-monitor)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)S | This command was introduced. |

## Usage Guidelines

Use the **df** command to modify the delay factor algorithm. The configured algorithm is used for both IP-CBR and MDI flows in a class. The ipdv-based algorithm is independent of the flow rate and reports only the delay caused by the network. The rfc4445-based algorithm is rate dependent and uses the configured flow rate. The rfc4445 based algorithm reports the sum of inter packet delay and network introduced delay.

## Examples

This example shows how to configure the delay factor to the ipdv-based algorithm:

```
router(config-pmap-c-monitor)# df ipdv
```

## Related Commands

| Command | Description |
|---|---|
| **show policy-map type performance-traffic** | Displays the policy-map information with the DF algorithm used. |

# disconnect qdm

To disconnect a Quality of Service Device Manager (QDM) client, use the **disconnectqdm** command in EXEC or privileged EXEC mode.

**disconnect qdm** [**client** *client-id*]

## Syntax Description

| | |
|---|---|
| **client** | (Optional) Specifies that a specific QDM client will be disconnected. |
| *client-id* | (Optional) Specifies the specific QDM identification number to disconnect. A QDM identification number can be a number from 0 to 2,147,483,647. |

## Command Default

This command has no default settings.

## Command Modes

EXEC Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1(1)E | This command was introduced. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

Use the **disconnectqdm** command to disconnect all QDM clients that are connected to the router.

Use the **disconnectqdm** [**client***client-id*] command to disconnect a specific QDM client connected to a router. For instance, using the **disconnectqdmclient42** command will disconnect the QDM client with the ID 42.

**Note** For the Cisco 7600 series QDM is not supported on Cisco Optical Services Module (OSM) interfaces.

## Examples

The following example shows how to disconnect all connected QDM clients:

```
Router# disconnect qdm
```

The following example shows how to disconnect a specific QDM client with client ID 9:

```
Router# disconnect qdm client 9
```

## Related Commands

| Command | Description |
|---|---|
| **show qdm status** | Displays the status of connected QDM clients. |

# drop

To configure a traffic class to discard packets belonging to a specific class, use the **drop** command in policy-map class configuration mode. To disable the packet discarding action in a traffic class, use the **no** form of this command.

**drop**

**no drop**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |

## Usage Guidelines

Note the following points when configuring the **drop** command to unconditionally discard packets in a traffic class:

- Discarding packets is the only action that can be configured in a traffic class. That is, no other actions can be configured in the traffic class.
- When a traffic class is configured with the **drop** command, a "child" (nested) policy cannot be configured for this specific traffic class through the **servicepolicy** command.
- Discarding packets cannot be configured for the default class known as the class-default class.

## Examples

The following example shows how to create a traffic class called "class1" and configure it for use in a policy map called "policy1". The policy map (service policy) is attached to output serial interface 2/0. All packets that match access-group 101 are placed in class1. Packets that belong to this class are discarded:

```
Router(config)# class-map class1
Router(config-cmap)# match access-group 101
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial2/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **show class-map** | Displays all class maps and their matching criteria. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# dscp

To change the minimum and maximum packet thresholds for the differentiated services code point (DSCP) value, use the **dscp** command in random-detect-group configuration mode. To return the minimum and maximum packet thresholds to the default for the DSCP value, use the **no** form of this command.

**dscp** *dscp-value min-threshold max-threshold* [ *mark-probability-denominator* ]

**no dscp** *dscp-value min-threshold max-threshold* [ *mark-probability-denominator* ]

## Syntax Description

| | |
|---|---|
| *dscp-value* | Specifies the DSCP value. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, or **cs7**. |
| *min-threshold* | Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. When the average queue length reaches the minimum threshold, Weighted Random Early Detection (WRED) randomly drops some packets with the specified DSCP value. |
| *max-threshold* | Maximum threshold in number of packets. The value range of this argument is the value of the *min-threshold* argument to 4096. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified DSCP value. |
| *mark-probability-denominator* | (Optional) Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, one out of every 512 packets is dropped when the average queue is at the maximum threshold. The value range is from 1 to 65536. The default is 10; one out of every ten packets is dropped at the maximum threshold. |

## Command Default

If WRED is using the DSCP value to calculate the drop probability of a packet, all entries of the DSCP table are initialized with the default settings shown in the table in the “Usage Guidelines” section.

## Command Modes

Random-detect-group configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(5)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command must be used in conjunction with the **random-detect-group** command.

Additionally, the **dscp** command is available only if you specified the *dscp-based* argument when using the **random-detect-group** command.

The table below lists the DSCP default settings used by the **dscp** command. The table below lists the DSCP value, and its corresponding minimum threshold, maximum threshold, and mark probability. The last row of the table (the row labeled "default") shows the default settings used for any DSCP value not specifically shown in the table.

***Table 2: dscp Default Settings***

| DSCP (Precedence) | Minimum Threshold | Maximum Threshold | Mark Probability |
|---|---|---|---|
| af11 | 32 | 40 | 1/10 |
| af12 | 28 | 40 | 1/10 |
| af13 | 24 | 40 | 1/10 |
| af21 | 32 | 40 | 1/10 |
| af22 | 28 | 40 | 1/10 |
| af23 | 24 | 40 | 1/10 |
| af31 | 32 | 40 | 1/10 |
| af32 | 28 | 40 | 1/10 |
| af33 | 24 | 40 | 1/10 |
| af41 | 32 | 40 | 1/10 |
| af42 | 28 | 40 | 1/10 |
| af43 | 24 | 40 | 1/10 |

| DSCP (Precedence) | Minimum Threshold | Maximum Threshold | Mark Probability |
|---|---|---|---|
| cs1 | 22 | 40 | 1/10 |
| cs2 | 24 | 40 | 1/10 |
| cs3 | 26 | 40 | 1/10 |
| cs4 | 28 | 40 | 1/10 |
| cs5 | 30 | 40 | 1/10 |
| cs6 | 32 | 40 | 1/10 |
| cs7 | 34 | 40 | 1/10 |
| ef | 36 | 40 | 1/10 |
| rsvp | 36 | 40 | 1/10 |
| default | 20 | 40 | 1/10 |

## Examples

The following example enables WRED to use the DSCP value af22. The minimum threshold for the DSCP value af22 is 28, the maximum threshold is 40, and the mark probability is 10.

```
Router> enable
Router# configure terminal
Router(config)# random-detect-group class1 dscp-based
Router(cfg-red-group)# dscp af22 28 40 10
Router(cfg-red-group)# end
```

## Related Commands

| Command | Description |
|---|---|
| **random-detect-group** | Enables per-VC WRED or per-VC DWRED. |
| **show queueing** | Lists all or selected configured queueing strategies. |
| **show queueing interface** | Displays the queueing statistics of an interface or VC. |

# estimate bandwidth

To estimate the bandwidth needed per traffic class for given quality of service (QoS) targets based on traffic data, use the **estimatebandwidth** command in policy-map class configuration mode. To disable the estimated bandwidth processing, use the **no** form of this command.

**estimate bandwidth** [**drop-one-in** *n*] [**delay-one-in** *n* **milliseconds** *n*]

**no estimate bandwidth**

## Syntax Description

| | |
|---|---|
| **drop-one-in** *n* | (Optional) The packet loss rate; for example, a value of 999 means drop no more than one packet out of 999. The range for*n* is 50 to 1000000 packets. |
| **delay-one-in** *n* **milliseconds** *n* | (Optional) The packet delay time and probability; the range for*n* is 50 to 1000000 packets. The delay threshold; the range for*n* is 8 to 1000 milliseconds. |

## Command Default

Disabled

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.3(14)T | This command was introduced. |

## Usage Guidelines

Use the **estimatebandwidth**command to specify the target drop probability, the delay time and probability, and the timeframe.

If you specify a delay time, you must also specify a delay threshold.

If you issue the **estimatebandwidth** command with no keywords, the default target is drop less than 2 percent, which is the same as entering **estimatebandwidthdrop-one-in500**.

## Examples

In the following example, the QoS targets are drop no more than one packet in 100, and delay no more than one packet in 100 by more than 50 milliseconds:

```
Router(config-pmap-c)# estimate bandwidth drop-one-in 100 delay-one-in 100 milliseconds 50
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth (policy-map class)** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map. |

# exponential-weighting-constant

To configure the exponential weight factor for the average queue size calculation for a Weighted Random Early Detection (WRED) parameter group, use the **exponential-weighting-constant**command in random-detect-group configuration mode. To return the exponential weight factor for the group to the default, use the **no** form of this command.

**exponential-weighting-constant** *exponent*

**no exponential-weighting-constant**

## Syntax Description

| | |
|---|---|
| *exponent* | Exponent from 1 to 16 used in the average queue size calculation. |

## Command Default

The default weight factor is 9.

## Command Modes

Random-detect-group configuration (cfg-red-group)

## Command History

| Release | Modification |
|---|---|
| 11.1(22)CC | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

When used, this command is issued after the **random-detect-group** command is entered.

Use this command to change the exponent used in the average queue size calculation for a WRED parameter group. The average queue size is based on the previous average and the current size of the queue. The formula is:

average = (old_average * (1-1/2^x)) + (current_queue_size * 1/2^x)

where *x* is the exponential weight factor specified in this command. Thus, the higher the factor, the more dependent the average is on the previous average.

**Note** The default WRED parameter values are based on the best available data. We recommend that you do not change the parameters from their default values unless you have determined that your applications would benefit from the changed values.

For high values of *x*, the previous average becomes more important. A large factor smooths out the peaks and lows in queue length. The average queue size is unlikely to change very quickly. The WRED process will be slow to start dropping packets, but it may continue dropping packets for a time after the actual queue size has fallen below the minimum threshold. The resulting slow-moving average will accommodate temporary bursts in traffic.

If the value of *x* gets too high, WRED will not react to congestion. Packets will be sent or dropped as if WRED were not in effect.

For low values of *x*, the average queue size closely tracks the current queue size. The resulting average may fluctuate with changes in the traffic levels. In this case, the WRED process will respond quickly to long queues. Once the queue falls below the minimum threshold, the process will stop dropping packets.

If the value of *x* gets too low, WRED will overreact to temporary traffic bursts and drop traffic unnecessarily.

## Examples

The following example shows how to configure the WRED group called sanjose with a weight factor of 10:

```
random-detect-group sanjose
 exponential-weighting-constant 10
```

## Related Commands

| Command | Description |
|---|---|
| **protect** | Configures a VC or PVC class with protected group or protected VC or PVC status for application to a VC or PVC bundle member. |
| **random-detect exponential-weighting-constant** | Configures the WRED and DWRED exponential weight factor for the average queue size calculation. |
| **random-detect-group** | Defines the WRED or DWRED parameter group. |
| **show queueing** | Lists all or selected configured queueing strategies. |
| **show queueing interface** | Displays the queueing statistics of an interface or VC. |

# fair-queue (class-default)

To specify the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy, use the **fair-queue** command in policy-map class configuration mode. To delete the configured number of dynamic queues from the class-default policy, use the **no** form of this command.

**fair-queue** [ *number-of-dynamic-queues* ]

**no fair-queue** [ *number-of-dynamic-queues* ]

## Syntax Description

| | |
|---|---|
| *number-of-dynamic-queues* | (Optional) A power of 2 that specifies the number of dynamic queues. Range is from 16 to 4096. |

## Command Default

The number of dynamic queues is derived from the interface or ATM permanent virtual circuit (PVC) bandwidth. See the table in the "Usage Guidelines" section for the default number of dynamic queues that weighted fair queueing (WFQ) and class-based WFQ (CBWFQ) use when they are enabled on an interface. See the table in the "Usage Guidelines" section for the default number of dynamic queues used when WFQ or CBWFQ is enabled on an ATM PVC.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command can be used for the default class (commonly known as the class-default class) only. You can use it in conjunction with either the **queue-limit** command or the **random-detect**command.

The class-default class is the default class to which traffic is directed if that traffic does not satisfy the match criteria of other classes whose policy is defined in the policy map.

The table below lists the default number of dynamic queues that weighted fair queueing (WFQ) and class-based WFQ (CBWFQ) use when they are enabled on an interface.

*Table 3: Default Number of Dynamic Queues as a Function of Interface Bandwidth*

| Bandwidth Range | Number of Dynamic Queues |
|---|---|
| Less than or equal to 64 kbps | 16 |
| More than 64 kbps and less than or equal to 128 kbps | 32 |
| More than 128 kbps and less than or equal to 256 kbps | 64 |
| More than 256 kbps and less than or equal to 512 kbps | 128 |
| More than 512 kbps | 256 |

The table below lists the default number of dynamic queues used when WFQ or CBWFQ is enabled on an ATM PVC.

*Table 4: Default Number of Dynamic Queues as a Function of ATM PVC Bandwidth*

| Bandwidth Range | Number of Dynamic Queues |
|---|---|
| Less than or equal to 128 kbps | 16 |
| More than 128 kbps and less than or equal to 512 kbps | 32 |
| More than 512 kbps and less than or equal to 2000 kbps | 64 |
| More than 2000 kbps and less than or equal to 8000 kbps | 128 |
| More than 8000 kbps | 256 |

## Examples

The following example shows how to configure policy for the default class included in the policy map called policy9. Packets that do not satisfy match criteria specified for other classes whose policies are configured in the same service policy are directed to the default class, for which 16 dynamic queues have been reserved. Because the **queue-limit** command is configured, tail drop is used for each dynamic queue when the maximum number of packets are enqueued and additional packets arrive:

```
policy-map policy9
 class class-default
 fair-queue 16
 queue-limit 20
```

The following example shows how to configure policy for the default class included in the policy map called policy8. The **fair-queue** command reserves 20 dynamic queues to be used for the default class. For congestion avoidance, Weighted Random Early Detection (WRED) packet drop is used, not tail drop:

```
policy-map policy8
 class class-default
 fair-queue 64
 random-detect
```

## Related Commands

| Command | Description |
|---|---|
| **queue-limit** | Specifies or modifies the maximum number of packets the queue can hold for a class policy configured in a policy map. |
| **random-detect (interface)** | Enables WRED or DWRED. |

# fair-queue (DWFQ)

To enable Versatile Interface Processor (VIP) distributed weighted fair queueing (DWFQ), use the **fair-queue**command in interface configuration mode. To disable DWFQ, use the **no** form of this command.

**fair-queue**

**no fair-queue**

## Syntax Description

This command has no arguments or keywords.

## Command Default

DWFQ is enabled by default for physical interfaces whose bandwidth is less than or equal to 2.048.

See the table in the "Usage Guidelines" section of this command for a list of the default queue lengths and thresholds.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 11.1 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

The **fair-queue**(DWFQ) command enables DWFQ on an interface using a VIP2-40 or greater interface processor.

With DWFQ, packets are classified by flow. Packets with the same source IP address, destination IP address, source TCP or User Datagram Protocol (UDP) port, destination TCP or UDP port, and protocol belong to the same flow.

DWFQ allocates an equal share of the bandwidth to each flow.

The table below lists the default queue lengths and thresholds.

***Table 5: Default Fair Queue Lengths and Thresholds***

| Queue or Threshold | Default |
|---|---|
| Congestive discard threshold | 64 messages |
| Dynamic queues | 256 queues |

| Queue or Threshold | Default |
|---|---|
| Reservable queues | 0 queues |

DWFQ can be configured on interfaces but not subinterfaces. It is not supported on Fast EtherChannel, tunnel, or other logical or virtual interfaces such as Multilink PPP (MLP).

**Note** The [**no**] **fair-queue** interface configuration command is not a valid configuration for member links of a multilink PPP interface. The command is only valid when configured on the multilink interface itself. Configuring [**no**] **fair-queue** on a member link interface while bidirectional traffic is flowing could result in the output queue becoming stuck on the multilink interface. If this occurs, a **shut**/**noshut** of the interface or a reload of the router may be required to clear the problem. An example configuration is provided in the "Examples" section to demonstrate the cause of this problem.

## Examples

The following example shows how to enable DWFQ on High-Speed Serial Interface (HSSI) interface 0/0/0:

```
interface Hssi0/0/0
 description 45Mbps to R2
 ip address 10.200.14.250 255.255.255.252
 fair-queue
```

The following example shows a basic configuration of two serial interfaces that results in the output queue becoming stuck on the multilink interface because of the **nofair-queue** command:

```
configure terminal
interface serial0/0/0:0
no fair-queue
no max-reserved-bandwidth 90
tx-queue-limit 19
!
interface serial0/0/1:0
no fair-queue
no max-reserved-bandwidth 90
tx-queue-limit 19
```

**Note** This sample configuration is provided for demonstration of a problem. Do not use this configuration.

## Related Commands

| Command | Description |
|---|---|
| **fair-queue (WFQ)** | Enables WFQ for an interface. |
| **fair-queue aggregate-limit** | Sets the maximum number of packets in all queues combined for DWFQ. |
| **fair-queue individual-limit** | Sets the maximum individual queue depth for DWFQ. |
| **fair-queue limit** | Sets the maximum queue depth for a specific DWFQ class. |

| Command | Description |
|---|---|
| **fair-queue qos-group** | Enables DWFQ and classifies packets based on the internal QoS-group number. |
| **fair-queue tos** | Enables DWFQ and classifies packets using the ToS field of packets. |
| **show interfaces** | Displays statistics for all interfaces configured on the router or access server. |
| **show interfaces fair-queue** | Displays information and statistics about WFQ for a VIP-based interface. |

# fair-queue (policy-map class)

To specify the number of queues to be reserved for use by a traffic class, use the **fair-queue** command in policy-map class configuration mode. To delete the configured number of queues from the traffic class, use the **no** form of this command.

**fair-queue** [ *dynamic-queues* ]

**no fair-queue** [ *dynamic-queues* ]

## Syntax Description

| | |
|---|---|
| *dynamic-queues* | (Optional) A number specifying the number of dynamic conversation queues. The number can be in the range of 16 to 4096. |

## Command Default

No queues are reserved.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE and implemented on Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T and was implemented on VIP-enabled Cisco 7500 series routers. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

On a VIP, the **fair-queue** command can be used for any traffic class (as opposed to non-VIP platforms, which can only use the **fair-queue** command in the default traffic class). The **fair-queue**command can be used in conjunction with either the **queue-limit** command or the **random-detectexponential-weighting-constant** command.

## Examples

The following example shows how to configure the default traffic class for the policy map called policy9 to reserve ten queues for packets that do not satisfy match criteria specified for other traffic classes whose policy is configured in the same service policy. Because the **queue-limit** command is configured, tail drop is used for each queue when the maximum number of packets is enqueued and additional packets arrive:

```
policy-map policy9
 class class-default
 fair-queue 10
 queue-limit 20
```

The following example shows how to configure a service policy called policy8 that is associated with a user-defined traffic class called class1. The **fair-queue** command reserves 20 queues to be used for the service policy. For congestion avoidance, Weighted Random Early Detection (WRED) or distributed WRED (DWRED) packet drop is used, not tail drop:

```
policy-map policy8
 class class1
 fair-queue 20
   random-detect exponential-weighting-constant 14
```

## Related Commands

| Command | Description |
|---|---|
| **class class-default** | Specifies the default traffic class for a service policy map. |
| **queue-limit** | Specifies or modifies the maximum number of packets the queue can hold for a class policy configured in a policy map. |
| **random-detect exponential-weighting-constant** | Configures the WRED and DWRED exponential weight factor for the average queue size calculation. |

# fair-queue (WFQ)

**Note** Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **fair-queue**command is hidden in interface configuration mode. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

**Note** Effective with Cisco IOS XE Release 3.2S, the **fair-queue**command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To enable weighted fair queueing (WFQ), use the **fair-queue** command in interface configuration or policy-map class configuration mode. To disable WFQ, use the **no**form of this command.

**fair-queue** [*congestive-discard-threshold* [*dynamic-queues* [ *reservable-queues* ]]]

**no fair-queue**

## Syntax Description

| | |
|---|---|
| *congestive-discard-threshold* | (Optional) Number of messages allowed in each queue. The range is 1 to 4096 and the default is 64 messages. When a conversation reaches this threshold, new message packets are discarded.<br>**Note** If you have hierarchical queueing framework (HQF) configured, then the values are 16 to 4096. |
| *dynamic-queues* | (Optional) Number of dynamic queues used for best-effort conversations (that is, a normal conversation not requiring any special network services). Values are **16**,**32**,**64**,**128**,**256**,**512**,**1024**,**2048**, and **4096**. See the tables in the **fair-queue**(class-default) command for the default number of dynamic queues. |

| | |
|---|---|
| *reservable-queues* | (Optional) Number of reservable queues used for reserved conversations in the range 0 to 1000. The default is 0. Reservable queues are used for interfaces configured for features such as Resource Reservation Protocol (RSVP). |

## Command Default

Fair queueing is enabled by default for physical interfaces whose bandwidth is less than or equal to 2.048 Mbps and that do not use the following:

- X.25 and Synchronous Data Link Control (SDLC) encapsulations
- Link Access Procedure, Balanced (LAPB)
- Tunnels
- Loopbacks
- Dialer
- Bridges
- Virtual interfaces

Fair queueing is not an option for the protocols listed above. However, if you enable custom queueing or priority queueing for a qualifying link, it overrides fair queueing, effectively disabling it. Additionally, fair queueing is automatically disabled if you enable the autonomous or silicon switching engine mechanisms.

**Note** A variety of queueing mechanisms can be configured using multilink; for example, Multichassis Multilink PPP (MMP). However, if only PPP is used on a tunneled interface--for example, virtual private dialup network (VPND), PPP over Ethernet (PPPoE), or PPP over Frame Relay (PPPoFR)--no queueing can be configured on the virtual interface.

The number of dynamic queues is derived from the interface or ATM permanent virtual circuit (PVC) bandwidth. See the table in the **fair-queue**(class-default) command for the default number of dynamic queues that WFQ and class-based WFQ (CBWFQ) use when they are enabled on an interface. See the table in the **fair-queue**(class-default) command for the default number of dynamic queues used when WFQ and CBWFQ are enabled on an ATM PVC.

## Command Modes

Interface configuration (config-if) Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 11.0 | This command was introduced. |
| 12.2(13)T | This command was modified to remove Apollo, VINES, and XNS from the list of protocols and traffic stream discrimination fields. These protocols were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems (XNS) were removed in this release. |

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB. |
| 12.2(33)SB | This command's behavior was modified on the Cisco 10000 series router for the PRE3 and PRE4. |
| 12.4(20)T | Support was added for HQF and user-defined classes using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC). |
| Cisco IOS XE Release 2.6 | This command was modified. This command was hidden. |
| 15.0(1)S | This command was modified. This command was hidden. |
| 15.1(3)T | This command was modified. This command was hidden. |
| Cisco IOS XE Release 3.2S | This command was replaced by an MQC command (or sequence of MQC commands). |

## Usage Guidelines

### High-Level Overview

This command enables WFQ. With WFQ, packets are classified by flow. For example, packets with the same source IP address, destination IP address, source TCP or User Datagram Protocol (UDP) port, destination TCP or UDP port, and protocol belong to the same flow; see the table below for a full list of protocols and traffic stream discrimination fields.

When you enable WFQ on an interface, WFQ provides traffic priority management that automatically sorts among individual traffic streams without requiring that you first define access lists. Enabling WFQ requires use of this command only.

When you enable WFQ on an interface, new messages for high-bandwidth traffic streams are discarded after the configured or default congestive discard threshold has been met. However, low-bandwidth conversations, which include control message conversations, continue to enqueue data. As a result, the fair queue may occasionally contain more messages than its configured threshold number specifies.

WFQ uses a traffic data stream discrimination registry service to determine which traffic stream a message belongs to. For each forwarding protocol, the table below shows the message attributes that are used to classify traffic into data streams.

*Table 6: Weighted Fair Queueing Traffic Stream Discrimination Fields*

| Forwarder | Fields Used |
|---|---|
| AppleTalk | • Source net, node, socket<br>• Destination net, node, socket<br>• Type |
| Connectionless Network Service (CLNS) | • Source network service access point (NSAP)<br>• Destination NSAP |
| DECnet | • Source address<br>• Destination address |
| Frame Relay switching | • Data-link connection identified (DLCI) value |
| IP | • Type of service (ToS)<br>• IP protocol<br>• Source IP address (if message is not fragmented)<br>• Destination IP address (if message is not fragmented)<br>• Source TCP/UDP port<br>• Destination TCP/UDP port |
| Transparent bridging | • Unicast: source MAC, destination MAC<br>• Ethertype Service Advertising Protocol (SAP)/Subnetwork Access Protocol (SNAP) multicast: destination MAC address |
| Source-route bridging | • Unicast: source MAC, destination MAC<br>• SAP/SNAP multicast: destination MAC address |
| Novell NetWare | • Source/destination network/host/socket<br>• Level 2 protocol |

| Forwarder | Fields Used |
|---|---|
| All others (default) | • Control protocols (one queue per protocol) |

**IP Precedence**

IP Precedence, congestion in Frame Relay switching, and discard eligible (DE) flags affect the weights used for queueing.

IP Precedence, which is set by the host or by policy maps, is a number in the range from 0 to 7. Data streams of precedence *number* are weighted so that they are given an effective bit rate of *number*+1 times as fast as a data stream of precedence 0, which is normal.

**FECN and BECN**

In Frame Relay switching, message flags for forward explicit congestion notification (FECN), backward explicit congestion notification (BECN), and DE message flags cause the algorithm to select weights that effectively impose reduced queue priority. The reduced queue priority provides the application with "slow down" feedback and sorts traffic, giving the best service to applications within their committed information rate (CIR).

**Fair Queueing, Custom Queueing, and Priority Queueing**

Fair queueing is supported for all LAN and line (WAN) protocols except X.25, including LAPB and SDLC; see the notes in the section "Command Default." Because tunnels are software interfaces that are themselves routed over physical interfaces, fair queueing is not supported for tunnels. Fair queueing is on by default for interfaces with bandwidth less than or equal to 2 Mbps.

**Note** For Release 10.3 and earlier releases for the Cisco 7000 and 7500 routers with a Route Switch Processor (RSP) card, if you used the **tx-queue-limit** command to set the transmit limit available to an interface on a Multiport Communications Interface (MCI) or serial port communications interface (SCI) card and you configured custom queueing or priority queueing for that interface, the configured transmit limit was automatically overridden and set to 1. With Cisco IOS Release 12.0 and later releases, for WFQ, custom queueing, and priority queueing, the configured transmit limit is derived from the bandwidth value set for the interface using the **bandwidth**(interface)command. Bandwidth value divided by 512 rounded up yields the effective transmit limit. However, the derived value only applies in the absence of a **tx-queue-limit** command; that is, a configured transmit limit overrides this derivation.

**RSVP**

When you configure Resource Reservation Protocol (RSVP) on an interface that supports fair queueing or on an interface that is configured for fair queueing with the reservable queues set to 0 (the default), the reservable queue size is automatically configured using the following method: interface bandwidth divided by 32 kbps. You can override this default by specifying a reservable queue other than 0. For more information on RSVP, refer to the chapter "Configuring RSVP" in the *Cisco IOS Quality of Service Solutions Configuration Guide* .

**Cisco 10000 Series Routers**

In Cisco IOS Release 12.2(33)SB, the router removes the no fair-queue command from serial interfaces.

**HQF**

Beginning with Cisco IOS Release 12.4(20)T, if your image has HQF support, the**fair-queue** command is not enabled automatically under class default. You should enable the fair-queue command and any other supported queueing features before using an HQF-capable image.

## Examples

The following example enables WFQ on serial interface 0, with a congestive threshold of 300. This threshold means that messages are discarded from the queueing system only when 300 or more messages have been queued and the message is in a data stream that has more than one message in the queue. The transmit queue limit is set to 2, based on the 384-kilobit (Kb) line set by the **bandwidth** command:

```
interface serial 0
 bandwidth 384
 fair-queue 300
```

Unspecified parameters take the default values.

The following example requests a fair queue with a congestive discard threshold of 64 messages, 512 dynamic queues, and 18 RSVP queues:

```
interface serial 3/0
 ip unnumbered ethernet 0/0
 fair-queue 64 512 18
```

You can apply the **fair-queue** command to a user-defined class as shown in the following example:

```
policy-map p1
 class c1
  bandwidth 1000
  fair-queue
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth (interface)** | Sets a bandwidth value for an interface. |
| **custom-queue-list** | Assigns a custom queue list to an interface. |
| **fair-queue (class-default)** | Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy. |
| **fair-queue (DWFQ)** | Enables DWFQ. |
| **priority-group** | Assigns the specified priority list to an interface. |
| **priority-list default** | Assigns a priority queue for those packets that do not match any other rule in the priority list. |
| **show interfaces** | Displays statistics for all interfaces configured on the router or access server. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing** | Lists all or selected configured queueing strategies. |

| Command | Description |
|---|---|
| **tx-queue-limit** | Controls the number of transmit buffers available to a specified interface on the MCI and SCI cards. |

# air-queue aggregate-limit

To set the maximum number of packets in all queues combined for Versatile Interface Processor (VIP)-distributed weighted fair queueing (DWFQ), use the **fair-queueaggregate-limit**command in interface configuration mode. To return the value to the default, use the **no** form of this command.

**fair-queue aggregate-limit** *aggregate-packets*

**no fair-queue aggregate-limit**

## Syntax Description

| | |
|---|---|
| *aggregate-packets* | Total number of buffered packets allowed before some packets may be dropped. Below this limit, packets will not be dropped. |

## Command Default

The total number of packets allowed is based on the transmission rate of the interface and the available buffer space on the VIP.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 11.1 CC | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

In general, you should not change the maximum number of packets allows in all queues from the default. Use this command only if you have determined that you would benefit from using a different value, based on your particular situation.

DWFQ keeps track of the number of packets in each queue and the total number of packets in all queues.

When the total number of packets is below the aggregate limit, queues can buffer more packets than the individual queue limit.

When the total number of packets reaches the aggregate limit, the interface starts enforcing the individual queue limits. Any new packets that arrive for a queue that is over its individual queue limit are dropped. Packets that are already in the queue will not be dropped, even if the queue is over the individual limit.

In some cases, the total number of packets in all queues put together may exceed the aggregate limit.

## Examples

The following example shows how to set the aggregate limit to 54 packets:

```
interface Fddi9/0/0
 fair-queue tos
 fair-queue aggregate-limit 54
```

## Related Commands

| Command | Description |
|---|---|
| **fair-queue limit** | Sets the maximum queue depth for a specific DWFQ class. |
| **fair-queue qos-group** | Enables DWFQ and classifies packets based on the internal QoS-group number. |
| **fair-queue tos** | Enables DWFQ and classifies packets using the ToS field of packets. |
| **show interfaces** | Displays statistics for all interfaces configured on the router or access server. |
| **show interfaces fair-queue** | Displays information and statistics about WFQ for a VIP-based interface. |

# fair-queue individual-limit

To set the maximum individual queue depth for Versatile Interface Processor (VIP)-distributed weighted fair queueing (DWFQ), use the **fair-queueindividual-limit**command in interface configuration mode. To return the value to the default, use the **no** form of this command.

**fair-queue individual-limit** *individual-packet*

**no fair-queue individual-limit**

## Syntax Description

| | |
|---|---|
| *individual-packet* | Maximum number of packets allowed in each per-flow or per-class queue during periods of congestion. |

## Command Default

Half of the aggregate queue limit

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 11.1 CC | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

In general, you should not change the maximum individual queue depth from the default. Use this command only if you have determined that you would benefit from using a different value, based on your particular situation.

DWFQ keeps track of the number of packets in each queue and the total number of packets in all queues.

When the total number of packets is below the aggregate limit, queues can buffer more packets than the individual queue limit.

When the total number of packets reaches the aggregate limit, the interface starts enforcing the individual queue limits. Any new packets that arrive for a queue that is over its individual queue limit are dropped. Packets that are already in the queue will not be dropped, even if the queue is over the individual limit.

In some cases, the total number of packets in all queues put together may exceed the aggregate limit.

## Examples

The following example shows how to set the individual queue limit to 27:

```
interface Fddi9/0/0
 mac-address 0000.0c0c.2222
 ip address 10.1.1.1 255.0.0.0
 fair-queue tos
 fair-queue individual-limit 27
```

## Related Commands

| Command | Description |
|---|---|
| **fair-queue (class-default)** | Sets the maximum number of packets in all queues combined for DWFQ. |
| **fair-queue limit** | Sets the maximum queue depth for a specific DWFQ class. |
| **fair-queue qos-group** | Enables DWFQ and classifies packets based on the internal QoS-group number. |
| **fair-queue tos** | Enables DWFQ and classifies packets using the ToS field of packets. |
| **show interfaces** | Displays statistics for all interfaces configured on the router or access server. |
| **show interfaces fair-queue** | Displays information and statistics about WFQ for a VIP-based interface. |

# fair-queue limit

To set the maximum queue depth for a specific Versatile Interface Processor (VIP)-distributed weighted fair queueing (DWFQ) class, use the **fair-queuelimit**command in interface configuration mode. To return the value to the default, use the **no** form of this command.

**fair-queue** {**qos-group** *number*| **tos** *number*} **limit** *class-packet*

**no fair-queue** {**qos-group** *number*| **tos** *number*} **limit** *class-packet*

## Syntax Description

| | |
|---|---|
| **qos-group** *number* | Number of the QoS group, as assigned by a committed access rate (CAR) policy or the Policy Propagation via Border Gateway Protocol (BGP) feature. The value can range from 1 to 99. |
| **tos** *number* | Two low-order IP Precedence bits of the type of service (ToS) field. |
| *class-packet* | Maximum number of packets allowed in the queue for the class during periods of congestion. |

## Command Default

The individual queue depth, as specified by the **fair-queueindividual-limit** command. If the **fair-queueindividual-limit** command is not configured, the default is half of the aggregate queue limit.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 11.1 CC | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use this command to specify the number queue depth for a particular class for class-based DWFQ. This command overrides the global individual limit specified by the **fair-queueindividual-limit** command.

In general, you should not change this value from the default. Use this command only if you have determined that you would benefit from using a different value, based on your particular situation.

## Examples

The following example shows how to set the individual queue limit for ToS group 3 to 20:

```
interface Fddi9/0/0
 mac-address 0000.0c0c.2222
 ip address 10.1.1.1 255.0.0.0
 fair-queue tos
 fair-queue tos 3 limit 20
```

## Related Commands

| Command | Description |
|---|---|
| **fair-queue (class-default)** | Sets the maximum number of packets in all queues combined for DWFQ. |
| **fair-queue qos-group** | Enables DWFQ and classifies packets based on the internal QoS-group number. |
| **fair-queue tos** | Enables DWFQ and classifies packets using the ToS field of packets. |
| **show interfaces** | Displays statistics for all interfaces configured on the router or access server. |
| **show interfaces fair-queue** | Displays information and statistics about WFQ for a VIP-based interface. |

# fair-queue qos-group

To enable Versatile Interface Processor (VIP)-distributed weighted fair queueing (DWFQ) and classify packets based on the internal QoS-group number, use the **fair-queueqos-group**command in interface configuration mode. To disable QoS-group-based DWFQ, use the **no** form of this command.

**fair-queue qos-group**

**no fair-queue qos-group**

## Syntax Description

This command has no arguments or keywords.

## Command Default

QoS-group-based DWFQ is disabled.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 11.1CC | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use this command to enable QoS-group-based DWFQ, a type of class-based DWFQ. Class-based DWFQ overrides flow-based DWFQ. Therefore, this command overrides the **fair-queue** (DWFQ) command.

When this command is enabled, packets are assigned to different queues based on their QoS group. A QoS group is an internal classification of packets used by the router to determine how packets are treated by certain QoS features, such as DWFQ and committed access rate (CAR). Use a CAR policy or the QoS Policy Propagation via Border Gateway Protocol (BGP) feature to assign packets to QoS groups.

Specify a weight for each class. In periods of congestion, each group is allocated a percentage of the output bandwidth equal to the weight of the class. For example, if a class is assigned a weight of 50, packets from this class are allocated at least 50 percent of the outgoing bandwidth during periods of congestion.

## Examples

The following example enables QoS-based DWFQ and allocates bandwidth for nine QoS groups (QoS groups 0 through 8):

```
interface Hssi0/0/0
 description 45Mbps to R2
 ip address 10.200.14.250 255.255.255.252
 fair-queue qos-group
```

```
fair-queue qos-group 1 weight 5
fair-queue qos-group 2 weight 5
fair-queue qos-group 3 weight 10
fair-queue qos-group 4 weight 10
fair-queue qos-group 5 weight 10
fair-queue qos-group 6 weight 15
fair-queue qos-group 7 weight 20
fair-queue qos-group 8 weight 29
```

## Related Commands

| Command | Description |
|---|---|
| **fair-queue (class-default)** | Sets the maximum number of packets in all queues combined for DWFQ. |
| **fair-queue limit** | Sets the maximum queue depth for a specific DWFQ class. |
| **fair-queue tos** | Enables DWFQ and classifies packets using the ToS field of packets. |
| **fair-queue weight** | Assigns a weight to a class for DWFQ. |
| **show interfaces** | Displays statistics for all interfaces configured on the router or access server. |
| **show interfaces fair-queue** | Displays information and statistics about WFQ for a VIP-based interface. |

# fair-queue tos

To enable Versatile Interface Processor (VIP)-distributed weighted fair queueing (DWFQ) and classify packets using the type of service (ToS) field of packets, use the **fair-queuetos**command in interface configuration command. To disable ToS-based DWFQ, use the **no** form of this command.

**fair-queue tos**

**no fair-queue tos**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled

By default, class 0 is assigned a weight of 10; class 1 is assigned a weight of 20; class 2 is assigned a weight of 30; and class 3 is assigned a weight of 40.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 11.1CC | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use this command to enable ToS-based DWFQ, a type of class-based DWFQ. Class-based DWFQ overrides flow-based DWFQ. Therefore, this command overrides the **fair-queue** (DWFQ) command.

When this command is enabled, packets are assigned to different queues based on the two low-order IP Precedence bits in the ToS field of the packet header.

In periods of congestion, each group is allocated a percentage of the output bandwidth equal to the weight of the class. For example, if a class is assigned a weight of 50, packets from this class are allocated at least 50 percent of the outgoing bandwidth during periods of congestion.

If you wish to change the weights, use the **fair-queueweight**command.

## Examples

The following example shows how to enable ToS-based DWFQ on the High-Speed Serial Interface (HSSI) interface 0/0/0:

```
interface Hssi0/0/0
 description 45Mbps to R2
```

```
ip address 10.200.14.250 255.255.255.252
fair-queue
fair-queue tos
```

## Related Commands

| Command | Description |
|---|---|
| **fair-queue (class-default)** | Sets the maximum number of packets in all queues combined for DWFQ. |
| **fair-queue limit** | Sets the maximum queue depth for a specific DWFQ class. |
| **fair-queue qos-group** | Enables DWFQ and classifies packets based on the internal QoS-group number. |
| **fair-queue weight** | Assigns a weight to a class for DWFQ. |
| **show interfaces** | Displays statistics for all interfaces configured on the router or access server. |
| **show interfaces fair-queue** | Displays information and statistics about WFQ for a VIP-based interface. |

# fair-queue weight

To assign a weight to a class for Versatile Interface Processor (VIP)-distributed weighted fair queueing (DWFQ), use the **fair-queueweight**command in interface configuration mode. To remove the bandwidth allocated for the class, use the **no** form of this command.

**fair-queue** {**qos-group** *number*| **tos** *number*} **weight** *weight*

**no fair-queue** {**qos-group** *number*| **tos** *number*} **weight** *weight*

## Syntax Description

| | |
|---|---|
| **qos-group** *number* | Number of the quality of service (QoS) group, as assigned by a committed access rate (CAR) policy or the Policy Propagation via Border Gateway Protocol (BGP) feature. The value range is from 1 to 99. |
| **tos** *number* | Two low-order IP Precedence bits of the type of service (ToS) field. The value range is from 1 to 3. |
| *weight* | Percentage of the output link bandwidth allocated to this class. The sum of weights for all classes cannot exceed 99. |

## Command Default

For QoS DWFQ, unallocated bandwidth is assigned to QoS group 0.

For ToS-based DWFQ, class 0 is assigned a weight of 10; class 1 is assigned a weight of 20; class 2 is assigned a weight of 30; and class 3 is assigned a weight of 40.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 11.1CC | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use this command to allocate percentages of bandwidth for specific DWFQ classes. You must also enable class-based DWFQ on the interface with either the **fair-queueqos-group** or **fair-queuetos**command.

Enter this command once for every class to allocate bandwidth to the class.

For QoS-group-based DWFQ, packets that are not assigned to any QoS groups are assigned to QoS group 0. When assigning weights to QoS group class, remember the following guidelines:

- One percent of the available bandwidth is automatically allocated to QoS group 0.
- The total weight for all the other QoS groups combined cannot exceed 99.
- Any unallocated bandwidth is assigned to QoS group 0.

For ToS-based DWFQ, remember the following guidelines:

- One percent of the available bandwidth is automatically allocated to ToS class 0.
- The total weight for all the other ToS classes combined cannot exceed 99.
- Any unallocated bandwidth is assigned to ToS class 0.

## Examples

The following example allocates bandwidth to different QoS groups. The remaining bandwidth (5 percent) is allocated to QoS group 0.

```
interface Fddi9/0/0
 fair-queue qos-group
 fair-queue qos-group 1 weight 10
 fair-queue qos-group 2 weight 15
 fair-queue qos-group 3 weight 20
 fair-queue qos-group 4 weight 20
 fair-queue qos-group 5 weight 30
```

## Related Commands

| Command | Description |
|---|---|
| **fair-queue qos-group** | Enables DWFQ and classifies packets based on the internal QoS-group number. |
| **fair-queue tos** | Enables DWFQ and classifies packets using the ToS field of packets. |
| **show interfaces** | Displays statistics for all interfaces configured on the router or access server. |
| **show interfaces fair-queue** | Displays information and statistics about WFQ for a VIP-based interface. |

# feedback

To enable the context-status feedback messages from the interface or link, use the **feedback** command in IP Header Compression (IPHC)-profile configuration mode. To disable the context-status feedback messages, use the **no** form of this command.

**feedback**

**no feedback**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Context-status feedback messages are enabled.

## Command Modes

IPHC-profile configuration (config-iphcp)

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

### Intended for Use with IPHC Profiles

The **feedback** command is intended for use as part of an IPHC profile. An IPHC profile is used to enable and configure header compression on your network. For more information about using IPHC profiles to configure header compression, see the "Header Compression" module and the "Configuring Header Compression Using IPHC Profiles" module of the *Cisco IOS Quality of Service Solutions Configuration Guide* , Release 12.4T.

### Restriction

There are two types of IPHC profiles: Internet Engineering Task Force (IETF) profiles and van-jacobson profiles. The **feedback**command is supported for IETF IPHC profiles only. The **feedback** command is not supported for van-jacobson IPHC profiles. For more information about IPHC profile types, see the "Header Compression" section of the *Cisco IOS Quality of Service Solutions Configuration Guide* , Release 12.4T.

### Prerequisite

Before using the **feedback** command, you must enable either TCP header compression or non-TCP header compression. To enable TCP header compression, use the **tcp** command. To enable non-TCP header compression, use the **non-tcp** command.

### Disabling of Context-Status Messages

During header compression, a session context is defined. For each context, the session state is established and shared between the compressor and the decompressor. The context state consists of the full IP/UDP/RTP, IP/UDP, or IP/TCP headers, a few first-order differential values, a link sequence number, a generation number, and a delta encoding table.

When the decompressor loses synchronization with the compressor, the decompressor sends a context status message to the compressor with a list of context IDs to invalidate. The compressor then sends a full-header packet to the decompressor to reestablish a consistent state. Note that all packets for the invalid context IDs are discarded until a full-header packet is received for that context ID.

You can disable the sending of context-status messages either when the time it takes for the packet to traverse the uplink and the downlink portions of the data path is greater than the refresh period (in which case, the sending of the context-status message would not be useful) or when a feedback path does not exist.

## Examples

The following is an example of an IPHC profile called profile2. In this example, context-status feedback messages have been disabled.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp
Router(config-iphcp)# no
 feedback
Router(config-iphcp)# end
```

## Related Commands

| Command | Description |
|---|---|
| **iphc-profile** | Creates an IPHC profile. |
| **non-tcp** | Enables non-TCP header compression within an IPHC profile. |
| **tcp** | Enables TCP header compression within an IPHC profile. |

# frame-relay interface-queue priority

To enable the Frame Relay PVC Interface Priority Queueing (FR PIPQ) feature, use the **frame-relayinterface-queuepriority** command in interface configuration mode. To disable FR PIPQ, use the **no** form of this command.To assign priority to a permanent virtual circuit (PVC) within a Frame Relay map class, use the **frame-relayinterface-queuepriority** command in map-class configuration mode. To remove priority from a PVC within a Frame Relay map class, use the **no** form of this command.

**frame-relay interface-queue priority** [*high-limit medium-limit normal-limit low-limit*]

**no frame-relay interface-queue priority**

**frame-relay interface-queue priority** {**high**| **medium**| **normal**| **low**}

**no frame-relay interface-queue priority**

## Syntax Description

| | |
|---|---|
| *high-limit* | (Optional) Size of the high priority queue specified in maximum number of packets. |
| *medium-limit* | (Optional) Size of the medium priority queue specified in maximum number of packets. |
| *normal-limit* | (Optional) Size of the normal priority queue specified in maximum number of packets. |
| *low-limit* | (Optional) Size of the low priority queue specified in maximum number of packets. |
| **high** | Assigns high priority to a PVC. |
| **medium** | Assigns medium priority to a PVC. |
| **normal** | Assigns normal priority to a PVC. |
| **low** | Assigns low priority to a PVC. |

## Command Default

The default sizes of the high, medium, normal, and low priority queues are 20, 40, 60, and 80 packets, respectively.

When FR PIPQ is enabled on the interface, the default PVC priority is normal priority.

## Command Modes

Interface configuration (config-if) Map-class configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(2)T | This command was introduced. |

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

FR PIPQ must be enabled on the interface in order for the map-class configuration of PVC priority to be effective.

Before you configure FR PIPQ using the **frame-relayinterface-queuepriority**command, the following conditions must be met:

- PVCs should be configured to carry a single type of traffic.
- The network should be configured with adequate call admission control to prevent starvation of any of the priority queues.

You will not be able to configure FR PIPQ if any queueing other than first-in first out (FIFO) queueing is already configured at the interface level. You will be able to configure FR PIPQ when weighted fair queueing (WFQ) is in use, as long as WFQ is the default interface queueing method. Disabling FR PIPQ will restore the interface to dual FIFO queueing if FRF.12 is enabled, FIFO queueing if Frame Relay Traffic Shaping (FRTS) is enabled, or the default queueing method for the interface.

## Examples

The following example shows how to enable FR PIPQ on serial interface 0, and set the limits of the high, medium, normal, and low priority queues to 10, 20, 30, and 40 packets, respectively. PVC 100 is assigned high priority, so all traffic destined for PVC 100 will be sent to the high priority interface queue.

```
interface serial0
 encapsulation frame-relay
 frame-relay interface-queue priority 10 20 30 40
 frame-relay interface-dlci 100
  class high_priority_class
 !
 map-class frame-relay high_priority_class
  frame-relay interface-queue priority high
```

## Related Commands

| Command | Description |
|---|---|
| **debug priority** | Displays priority queueing events. |
| **show frame-relay pvc** | Displays statistics about PVCs for Frame Relay interfaces. |
| **show interfaces** | Displays statistics for all interfaces configured on the router or access server. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |

| Command | Description |
|---|---|
| **show queueing** | Lists all or selected configured queueing strategies. |

# frame-relay ip rtp compression-connections

To specify the maximum number of Real-Time Transport Protocol (RTP) header compression connections that can exist on a Frame Relay interface, use the **frame-relayiprtpcompression-connections** command in interface configuration mode. To restore the default, use the **no** form of this command.

**frame-relay ip rtp compression-connections** *number*

**no frame-relay ip rtp compression-connections**

## Syntax Description

| | |
|---|---|
| *number* | Maximum number of RTP header compression connections. The range is from 3 to 256. |

## Command Default

256 header compression connections

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.1(2)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Before you can configure the maximum number of connections, RTP header compression must be configured on the interface using the **frame-relayiprtpheader-compression** command.

The number of RTP header compression connections must be set to the same value at each end of the connection.

## Examples

The following example shows the configuration of a maximum of 150 RTP header compression connections on serial interface 0:

```
interface serial 0
 encapsulation frame-relay
 frame-relay ip rtp header-compression
 frame-relay ip rtp compression-connections 150
```

## Related Commands

| Command | Description |
|---|---|
| **frame-relay ip rtp header-compression** | Enables RTP header compression for all Frame Relay maps on a physical interface. |
| **frame-relay map ip compress** | Enables both RTP and TCP header compression on a link. |
| **frame-relay map ip rtp header-compression** | Enables RTP header compression per DLCI. |
| **show frame-relay ip rtp header-compression** | Displays RTP header compression statistics for Frame Relay. |

# frame-relay ip rtp header-compression

To enable Real-Time Transport Protocol (RTP) header compression for all Frame Relay maps on a physical interface, use the **frame-relayiprtpheader-compression**command in interface configuration mode. To disable the compression, use the **no** form of this command.

**frame-relay ip rtp header-compression** [**active**| **passive**] **[periodic-refresh]**

**no frame-relay ip rtp header-compression** [**active**| **passive**] **[periodic-refresh]**

## Syntax Description

| | |
|---|---|
| **active** | (Optional) Compresses all outgoing RTP packets. |
| **passive** | (Optional) Compresses the outgoing RTP/User Datagram Protocol (UDP)/IP header only if an incoming packet had a compressed header. |
| **periodic-refresh** | (Optional) Indicates that the compressed IP header will be refreshed periodically. |

## Command Default

Disabled.

By default, whatever type of header compression is configured on the interface will be inherited. If header compression is not configured on the interface, the **active** keyword will be used, but no **header-compression**keyword will appear on the **showrunning-config** command output.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |
| 12.3(2)T | This command was integrated into Cisco IOS Release 12.3(2)T. This command was modified to include the **periodic-refresh** keyword. |
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

When the **frame-relayiprtpheader-compression** command is used on the physical interface, all the interface maps inherit the command; that is, all maps will perform UDP and RTP IP header compression.

## Examples

The following example shows how to enable RTP header compression for all Frame Relay maps on a physical interface:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0.1
Router(config-if)# frame-relay ip rtp header-compression
Router(config-if)# end
```

The following example shows how to enable RTP header compression, and the optional**periodic-refresh** keyword is specified:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0.2
Router(config-if)# frame-relay ip rtp header-compression periodic-refresh
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **frame-relay ip rtp compression-connections** | Specifies maximum number of RTP header compression connections on a Frame Relay interface. |
| **frame-relay map ip nocompress** | Disables both RTP and TCP header compression on a link. |
| **show frame-relay ip rtp header-compression** | Displays RTP header compression statistics for Frame Relay. |

# frame-relay ip rtp priority

**Note** Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **frame-relayiprtppriority**command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

**Note** Effective with Cisco IOS XE Release 3.2S, the **frame-relayiprtppriority**command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* .

To reserve a strict priority queue on a Frame Relay permanent virtual circuit (PVC) for a set of Real-Time Transport Protocol (RTP) packet flows belonging to a range of User Datagram Protocol (UDP) destination ports, use the **frame-relayiprtppriority** command in map-class configuration mode. To disable the strict priority queue, use the **no** form of this command.

**frame-relay ip rtp priority** *starting-rtp-port-number port-number-range bandwidth*

**no frame-relay ip rtp priority**

## Syntax Description

| | |
|---|---|
| *starting-rtp-port-number* | The starting UDP port number. The lowest port number to which the packets are sent. A port number can be a number from 2000 to 65535. |
| *port-number-range* | The range of UDP destination ports. Number, which added to the *starting-rtp-port-number* argument, yields the highest UDP port number. The range can be from 0 to 16383. |
| *bandwidth* | Maximum allowed bandwidth, in kbps. The bandwidth can range from 0 to 2000 kbps. |

## Command Default

No default behavior or values

## Command Modes

Map-class configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(7)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.6 | This command was modified. This command was hidden. |
| 15.0(1)S | This command was modified. This command was hidden. |
| 15.1(3)T | This command was modified. This command was hidden. |
| Cisco IOS XE Release 3.2S | This command was replaced by an MQC command (or sequence of MQC commands). |

## Usage Guidelines

This command is most useful for voice applications, or other applications that are delay-sensitive. To use this command, you must first enter the **map-classframe-relay** command. After the Frame Relay map class has been configured, it must then be applied to a PVC.

This command extends the functionality offered by the **iprtppriority** command by supporting Frame Relay PVCs. The command allows you to specify a range of UDP ports whose voice traffic is guaranteed strict priority service over any other queues or classes using the same output interface. Strict priority means that if packets exist in the priority queue, they are dequeued and sent first--that is, before packets in other queues are dequeued.

Frame Relay Traffic Shaping (FRTS) and Frame Relay Fragmentation (FRF.12) must be configured before the **frame-relayiprtppriority** command is used.

Compressed RTP (CRTP) can be used to reduce the bandwidth required per voice call. When using CRTP with Frame Relay, you must use the **encapsulationframe-relaycisco** command instead of the **encapsulationframe-relayietf**command.

Remember the following guidelines when configuring the *bandwidth* parameter:

- It is always safest to allocate to the priority queue slightly more than the known required amount of bandwidth, to allow room for network bursts.
- The IP RTP Priority admission control policy takes RTP header compression into account. Therefore, while configuring the *bandwidth* parameter of the **iprtppriority** command you need to configure only for the bandwidth of the compressed call. Because the *bandwidth* parameter is the maximum total bandwidth, you need to allocate enough bandwidth for all calls if there will be more than one call.
- Configure a bandwidth that allows room for Layer 2 headers. The bandwidth allocation takes into account the payload plus the IP, UDP, and RTP headers but does not account for Layer 2 headers. Allowing 25 percent bandwidth for other overhead is conservative and safe.

- The sum of all bandwidth allocation for voice and data flows on an interface cannot exceed 75 percent of the total available bandwidth, unless you change the default maximum reservable bandwidth. To change the maximum reservable bandwidth, use the **max-reserved-bandwidth** command on the interface.

For more information on IP RTP Priority bandwidth allocation, refer to the section "IP RTP Priority" in the chapter "Congestion Management Overview" in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

## Examples

The following example first configures the Frame Relay map class called voip and then applies the map class to PVC 100 to provide strict priority service to matching RTP packets:

```
map-class frame-relay voip
 frame-relay cir 256000
 frame-relay bc 2560
 frame-relay be 600
 frame-relay mincir 256000
 no frame-relay adaptive-shaping
 frame-relay fair-queue
 frame-relay fragment 250
 frame-relay ip rtp priority 16384 16380 210
interface Serial5/0
 ip address 10.10.10.10 255.0.0.0
 no ip directed-broadcast
 encapsulation frame-relay
 no ip mroute-cache
 load-interval 30
 clockrate 1007616
 frame-relay traffic-shaping
 frame-relay interface-dlci 100
  class voip
 frame-relay ip rtp header-compression
 frame-relay intf-type dce
```

In this example, RTP packets on PVC 100 with UDP ports in the range from 16384 to 32764 (32764 = 16384 + 16380) will be matched and given strict priority service.

## Related Commands

| Command | Description |
|---|---|
| **encapsulation frame-relay** | Enables Frame Relay encapsulation. |
| **ip rtp priority** | Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports. |
| **map-class frame-relay** | Specifies a map class to define QoS values for an SVC. |
| **max-reserved-bandwidth** | Changes the percent of interface bandwidth allocated for CBWFQ, LLQ, and IP RTP Priority. |
| **priority** | Gives priority to a class of traffic belonging to a policy map. |
| **show frame-relay pvc** | Displays statistics about PVCs for Frame Relay interfaces. |

| Command | Description |
|---|---|
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show traffic-shape queue** | Displays information about the elements queued by traffic shaping at the interface level or the DLCI level. |

# frame-relay ip tcp compression-connections

To specify the maximum number of TCP header compression connections that can exist on a Frame Relay interface, use the **frame-relayiptcpcompression-connections**command in interface configuration mode. To restore the default, use the **no** form of this command.

**frame-relay ip tcp compression-connections** *number*

**no frame-relay ip tcp compression-connections**

## Syntax Description

| | |
|---|---|
| *number* | Maximum number of TCP header compression connections. The range is from 3 to 256. |

## Command Default

256 header compression connections

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.1(2)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Before you can configure the maximum number of connections, TCP header compression must be configured on the interface using the **frame-relayiptcpheader-compression** command.

The number of TCP header compression connections must be set to the same value at each end of the connection.

## Examples

The following example shows the configuration of a maximum of 150 TCP header compression connections on serial interface 0:

```
interface serial 0
 encapsulation frame-relay
 frame-relay ip tcp header-compression
 frame-relay ip tcp compression-connections 150
```

## Related Commands

| Command | Description |
|---|---|
| **frame-relay ip tcp header-compression** | Enables TCP header compression for all Frame Relay maps on a physical interface. |
| **frame-relay map ip compress** | Enables both RTP and TCP header compression on a link. |
| **frame-relay map ip tcp header-compression** | Assigns header compression characteristics to an IP map that differ from the compression characteristics of the interface with which the IP map is associated. |
| **show frame-relay ip tcp header-compression** | Displays statistics and TCP/IP header compression information for the interface. |

# frame-relay ip tcp header-compression

To configure an interface to ensure that the associated permanent virtual circuit (PVC) will always carry outgoing TCP/IP headers in compressed form, use the **frame-relayiptcpheader-compression**command in interface configuration mode. To disable compression of TCP/IP packet headers on the interface, use the **no** form of this command.

**frame-relay ip tcp header-compression [passive]**

**no frame-relay ip tcp header-compression**

## Syntax Description

| | |
|---|---|
| **passive** | (Optional) Compresses the outgoing TCP/IP packet header only if an incoming packet had a compressed header. |

## Command Default

Active TCP/IP header compression; all outgoing TCP/IP packets are subjected to header compression.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command applies to interfaces that support Frame Relay encapsulation, specifically serial ports and High-Speed Serial Interface (HSSI).

Frame Relay must be configured on the interface before this command can be used.

TCP/IP header compression and Internet Engineering Task Force (IETF) encapsulation are mutually exclusive. If an interface is changed to IETF encapsulation, all encapsulation and compression characteristics are lost.

When you use this command to enable TCP/IP header compression, every IP map inherits the compression characteristics of the interface, unless header compression is explicitly rejected or modified by use of the **frame-relaymapiptcpheadercompression**command.

We recommend that you shut down the interface prior to changing encapsulation types. Although this is not required, shutting down the interface ensures the interface is reset for the new type.

## Examples

The following example configures serial interface 1 to use the default encapsulation (cisco) and passive TCP header compression:

```
interface serial 1
 encapsulation frame-relay
 frame-relay ip tcp header-compression passive
```

## Related Commands

| Command | Description |
|---|---|
| **frame-relay map ip tcp header-compression** | Assigns header compression characteristics to an IP map different from the compression characteristics of the interface with which the IP map is associated. |

# frame-relay map ip compress

To enable both Real-Time Transport Protocol (RTP) and TCP header compression on a link, use the **frame-relaymapipcompress**command in interface configuration mode.

**frame-relay map ip** *ip-address dlci* **[broadcast] compress** [**active**| **passive**] [**connections** *number*]

## Syntax Description

| | |
|---|---|
| *ip-address* | IP address of the destination or next hop. |
| *dlci* | Data-link connection identifier (DLCI) number. |
| **broadcast** | (Optional) Forwards broadcasts to the specified IP address. |
| **active** | (Optional) Compresses all outgoing RTP and TCP packets. This is the default. |
| **passive** | (Optional) Compresses the outgoing RTP and TCP header only if an incoming packet had a compressed header. |
| **connections** *number* | (Optional) Specifies the maximum number of RTP and TCP header compression connections. The range is from 3 to 256. |

## Command Default

RTP and TCP header compression are disabled.

The default maximum number of header compression connections is 256.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |
| 12.1(2)T | This command was modified to enable the configuration of the maximum number of header compression connections. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command does not have a “no” form. That is, a command called **noframe-relaymapipcompress** does not exist.

## Examples

The following example enables both RTP and TCP header compression on serial interface 1 and sets the maximum number of RTP and TCP header connections at 16:

```
interface serial 1
 encapsulation frame-relay
 ip address 10.108.175.110 255.255.255.0
 frame-relay map ip 10.108.175.220 180 compress connections 16
```

## Related Commands

| Command | Description |
|---|---|
| **frame-relay ip rtp compression-connections** | Specifies the maximum number of RTP header compression connections on a Frame Relay interface. |
| **frame-relay ip tcp header-compression** | Enables TCP header compression for all Frame Relay maps on a physical interface. |
| **frame-relay map ip nocompress** | Disables both RTP and TCP header compression on a link. |
| **frame-relay map ip rtp header-compression** | Enables RTP header compression for all Frame Relay maps on a physical interface. |
| **show frame-relay ip rtp header-compression** | Displays RTP header compression statistics for Frame Relay. |
| **show frame-relay ip tcp header-compression** | Displays statistics and TCP/IP header compression information for the interface. |

# frame-relay map ip nocompress

To disable both Real-Time Transport Protocol (RTP) and TCP header compression on a link, use the **frame-relaymapipnocompress**command in interface configuration mode.

**frame-relay map ip** *ip-address dlci* **[broadcast] nocompress**

## Syntax Description

| | |
|---|---|
| *ip-address* | IP address of the destination or next hop. |
| *dlci* | Data-link connection identifier (DLCI) number. |
| **broadcast** | (Optional) Forwards broadcasts to the specified IP address. |

## Command Default

No default behaviors or values

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command does not have a “no” form. That is, a command called **noframe-relaymapipnocompress**does not exist.

## Examples

The following example disables RTP and TCP header compression on DLCI 180:

```
interface serial 1
 encapsulation frame-relay
 frame-relay map ip 10.108.175.220 180 nocompress
```

## Related Commands

| Command | Description |
|---|---|
| **frame-relay ip rtp header-compression** | Enables RTP header compression for all Frame Relay maps on a physical interface. |
| **frame-relay ip tcp header-compression** | Enables TCP header compression for all Frame Relay maps on a physical interface. |
| **frame-relay map ip compress** | Enables RTP and TCP header compression on a link. |
| **show frame-relay ip rtp header-compression** | Displays RTP header compression statistics for Frame Relay. |
| **show frame-relay ip tcp header-compression** | Displays statistics and TCP/IP header compression information for the interface. |

# frame-relay map ip rtp header-compression

To enable Real-Time Transport Protocol (RTP) header compression per data-link connection identifier (DLCI), use the **frame-relaymapiprtpheader-compression**command in interface configuration mode. To disable RTP header compression per DLCI and delete the DLCI, use the **no** form of this command.

**frame-relay map ip** *ip-address dlci* **[broadcast] rtp header-compression** [**active**| **passive**] **[periodic-refresh]** [**connections** *number*]

**no frame-relay map ip** *ip-address dlci* **[broadcast] rtp header-compression** [**active**| **passive**] **[periodic-refresh]** [**connections** *number*]

## Syntax Description

| | |
|---|---|
| *ip-address* | IP address of the destination or next hop. |
| *dlci* | DLCI number. |
| **broadcast** | (Optional) Forwards broadcasts to the specified IP address. |
| **active** | (Optional) Compresses outgoing RTP packets. |
| **passive** | (Optional) Compresses the outgoing RTP/ User Datagram Protocol (UDP) /IP header only if an incoming packet had a compressed header. |
| **periodic-refresh** | (Optional) Refreshes the compressed IP header periodically. |
| **connections** *number* | (Optional) Specifies the maximum number of RTP header compression connections. The range is from 3 to 256. |

## Command Default

Disabled.

By default, whatever type of header compression is configured on the interface will be inherited. If header compression is not configured on the interface, the **active** keyword will be used, but no **header-compression** keyword will appear on the **showrunning-config** command output.

The default maximum number of header-compression connections is 256.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |

| Release | Modification |
|---|---|
| 12.1(2)T | This command was integrated into Cisco IOS Release 12.1(2)T. This command was modified to enable the configuration of the maximum number of header compression connections. |
| 12.3(2)T | This command was modified to include the **periodic-refresh** keyword. |
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

When this command is configured, the specified maps inherit RTP header compression. You can have multiple Frame Relay maps, with and without RTP header compression. If you do not specify the number of RTP header compression connections, the map will inherit the current value from the interface.

## Examples

The following example shows how to enable RTP header compression on the Serial1/2.1 subinterface and set the maximum number of RTP header compression connections at 64:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/2.1
Router(config-if)# encapsulation frame-relay
Router(config-if)# ip address 10.108.175.110 255.255.255.0
Router(config-if)# frame-relay map ip 10.108.175.220 180 rtp header-compression connections
 64
Router(config-if)# end
```

The following example shows how to enable RTP header compression on the Serial1/1.0 subinterface and how to use the optional **periodic-refresh** keyword in the configuration:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/1.0
Router(config-if)# encapsulation frame-relay
Router(config-if)# ip address 10.108.175.110 255.255.255.0
Router(config-if)# frame-relay map ip 10.108.175.220 180 rtp header-compression
periodic-refresh
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **frame-relay ip rtp compression-connections** | Specifies the maximum number of RTP header compression connections on a Frame Relay interface. |
| **frame-relay ip rtp header-compression** | Enables RTP header compression for all Frame Relay maps on a physical interface. |

| Command | Description |
|---|---|
| **frame-relay map ip compress** | Enables both RTP and TCP header compression on a link. |
| **show frame-relay ip rtp header-compression** | Displays RTP header compression statistics for Frame Relay. |

# group (service group)

To add a member to a service group, use the **group**command in Ethernet service configuration mode. To remove a member from a service group, use the **no** form of this command.

**group** *service-group-identifier*

**no group** *service-group-identifier*

## Syntax Description

| | |
|---|---|
| *service-group-identifier* | Number of an existing service group to which the member will be added or removed. |

## Command Default

A member is not added.

## Command Modes

Ethernet service configuration (config-if-srv)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRE | This command was introduced. |

## Usage Guidelines

Use the **group** (service group) command to add members (for example, service instances) to service groups and to remove members from service groups.

**Cisco 7600 Series Router and Service Instances From Multiple Interfaces Are Not Allowed**

The Cisco 7600 series router does not allow service instances to join the same group from multiple interfaces. On the Cisco 7600 series router, group members must come from the same interface, as shown the sample configuration below:

```
interface GigabitEthernet 2/0/0
service instance 1 ethernet
 group 32
 service-policy output policy3
service instance 2 ethernet
 group 32
   service instance 3 ethernet
 group 37
interface GigabitEthernet 2/0/1
 service instance 1 ethernet
  group 32 |<--Disallowed because this group has members in g2/0/0 already| |
```

## Examples

The following example shows how to add service instance 200 to service group 20:

```
Router> enable
Router# configure terminal
Router# interface GigabitEthernet 1/0/0
```

```
Router(config-if)# service instance 200 ethernet
Router(config-if-srv)# group 20
Router(config-if-srv)# end
```

# hw-module slot (ESP Scheduling)

To handle the oversubscription of packets at the ingress side of an Embedded Service Processor, provide either a minimum bandwidth or a specific weight to a SIP based on which the excess bandwidth is divided among the low priority packets of the SIPs. Execute the **hw-moduleslot** command in global configuration mode. Use the **no** form of this command to either remove the minimum bandwidth assigned to a SIP or remove the excess weight configured for a SIP.

**hw-module slot** *slot-number* **qos input link** {**A**| **B**} [**bandwidth** *bandwidth_value*] [**weight** *weightage_value*]

## Syntax Description

| | |
|---|---|
| *slot-number* | The slot number of the SIP for which the minimum bandwidth or excess weight needs to be configured. |
| **qos** | Enables configuration of the quality of service (QoS) policy to solve the oversubscription problem on the ingress side. |
| input | Enables the scheduling of packets on the ingress side. |
| **link** | Enables the configuration of each ESI link between the SIP and the ESP. |
| **A** | Specifies the A input QoS link for configuration of parameters. |
| **B** | Specifies the B input QoS link for configuration of parameters. |
| **bandwidth** | Provisions the configuration of a committted minimum bandwidth for the specified SIP. |
| *bandwidth_value* | The minimum bandwidth value in Kbps to be assigned to the SIP. |
| **weight** | Assigns the excess weight available for sharing to the SIP. Based on the excess weight assigned to the SIP, the available bandwidth that is left after processing the high priority packets is divided among the SIPs of low priority packets. |
| *weightage_value* | The weightage value to be assigned to the SIP for dividing the free bandwidth among the SPAs. The valid range for weightage value is 5 to 100. |

## Command Default

By default, the high priority packets are processed first.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release XE 2.1 | This command was introduced as the **hw-moduleslot**(QoS) command. |
| Cisco IOS Release XE 3.1S | The command was modified. The command was changed to the **hw-moduleslot** (ESP Scheduling) command and the **link** keyword was added. |
| Cisco IOS Release XE 3.1.0 | This command was modified. The **linkA**or**linkB**keyword sequences were added to provide specific bay information for configuring parameters on QoS input links. |

## Usage Guidelines

Oversubscription occurs at the SIP and ESP levels. To handle the oversubscription problem at the ESP level, use the **hw-module** slot command. A minimum bandwidth is assigned to a SIP that is connected through the ESI links, and a weight is assigned to the SIPs to divide the available excess bandwidth among the low priority packets. To configure the minimum bandwidth service for a SIP, execute the **hw-moduleslot***slot-number***qosinputlink***link-index***bandwidth***value_in_kbps**command.

To assign a specific weight value to an ESI link connecting a SIP and an ESP, execute the **hw-moduleslot***slot-number***qosinputlink***link-index***weight***weight-value**command.

## Examples

The following example shows how to assign a minimum bandwidth to ESI Link A:

```
Router# config
Router(config)# hw-module slot 1 qos input link A bandwidth 512
```

The following example shows how to assign an excess weight of 150 to a SIP at slot 1 and connected through ESI Link A:

```
Router# config
Router(config)# hw-module slot 1 qos input link A weight 150
```

The following example shows how to display the available link options for ESP40 and SIP40 cards when there are two links configured:

```
Router(config)# hw-module slot 0 qos input link ?
 A  ESI Link A (Bay 0,2)
 B  ESI Link B (Bay 1,3)
```

The following example shows how to display the available link options for ESP40 and SIP10 cards when there is one link configured:

```
Router(config)# hw-module slot 1 qos input link ?
 A  ESI Link A (All Bays)
```

## Related Commands

| Command | Description |
|---|---|
| **show platform hardware slot {f0 \| f1} serdes qos** | Displays the excess weight and committed bandwidth settings for ESPs. |

# hw-module subslot (Channelized SPA Scheduling)

To handle the oversubscription of packets at the ingress side of a SIP for a channelized SPA, assign the excess weight to the entire channelized SPA using the **hw-modulesubslot** command in global configuration mode. Use the **no** form of this command to remove the excess weight configured for the SIP.

**hw-module subslot** *slot/subslot* **qos** [**weight** *weightage_value*]

**no hw-module subslot** *slot/subslot* **qos** [**weight** *weightage_value*]

## Syntax Description

| | |
|---|---|
| *slot-subslot* | The slot number of the SIP, and the subslot number of the channelized SPA for which the excess weight needs to be configured. |
| **qos** | Enables the configuration of the excess weight for low priority packets on a channelized SPA to solve the oversubscription problem on the ingress side. |
| **weight** | Assigns the excess weight to the channelized SPA. Based on the excess weight assigned to the channelized SPA, the available bandwidth that is left after processing the high priority packets is divided among the SPAs. |
| *weightage_value* | The weightage value to be assigned to the channelized SPA for dividing the excess bandwidth among the channelized SPAs. The valid range for weightage value is 5 to 100. |

## Command Default

By default, the high priority packets are processed first.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| 3.1S | This command was introduced to assign weight during the distribution of available bandwidth for channelized SPAs. |

## Usage Guidelines

A SIP contains different types of SPAs in each of its slots. To assign the excess weight to a channelized SPA for low priority packets, the **hw-modulesubslot***slot-subslot***qosweight***weight-value*command has been introduced.

**Note** The option to configure minimum bandwidth for 'strict-priority' queue at port-level (interface-level) is deprecated as it is not applicable to the current mode of operation. Existing configuration will be rejected with an error.

## Examples

The following example shows how to assign an excess weight of 200 to a channelized SPA located at slot 1 and subslot 0:

```
Router# config
Router(config)# hw-module subslot 1/0 qos weight 200
```

## Related Commands

| Command | Description |
|---|---|
| **show platform hardware {slot** *slotno* **\| subslot** *slot/subslot* **} plim qos input bandwidth** | Displays excess weight and committed bandwidth settings configured on a SIP or SPA respectively. |

# identity policy policy-map through ip rsvp pq-profile


- identity policy (policy-map), page 194
- ingress-class-map, page 196
- ip header-compression disable-feedback, page 198
- ip header-compression max-header, page 200
- ip header-compression max-period, page 202
- ip header-compression max-time, page 204
- ip header-compression recoverable-loss, page 206
- ip header-compression old-iphc-comp, page 208
- ip header-compression old-iphc-decomp, page 209
- ip nbar attribute-map, page 210
- ip nbar attribute-set, page 212
- ip nbar classification tunneled-traffic, page 214
- ip nbar custom, page 215
- ip nbar pdlm, page 219
- ip nbar port-map, page 221
- ip nbar protocol-discovery, page 223
- ip nbar protocol-pack, page 225
- ip nbar resources, page 227
- ip nbar resources protocol, page 228
- ip nbar resources system, page 230
- ip options, page 232
- ip rsvp admission-control compression predict, page 234
- ip rsvp aggregation ip, page 236

- ip rsvp aggregation ip map, page 238
- ip rsvp aggregation ip reservation dscp, page 241
- ip rsvp aggregation ip role interior, page 244
- ip rsvp atm-peak-rate-limit, page 246
- ip rsvp authentication, page 248
- ip rsvp authentication challenge, page 250
- ip rsvp authentication key, page 252
- ip rsvp authentication key-chain, page 254
- ip rsvp authentication lifetime, page 256
- ip rsvp authentication neighbor, page 258
- ip rsvp authentication type, page 262
- ip rsvp authentication window-size, page 264
- ip rsvp bandwidth, page 266
- ip rsvp bandwidth ignore, page 271
- ip rsvp bandwidth percent, page 272
- ip rsvp burst policing, page 275
- ip rsvp data-packet classification none, page 276
- ip rsvp dsbm candidate, page 278
- ip rsvp dsbm non-resv-send-limit, page 280
- ip rsvp flow-assist, page 282
- ip rsvp layer2 overhead, page 284
- ip rsvp listener, page 287
- ip rsvp listener outbound, page 290
- ip rsvp msg-pacing, page 293
- ip rsvp neighbor, page 295
- ip rsvp policy cops minimal, page 297
- ip rsvp policy cops report-all, page 298
- ip rsvp policy cops servers, page 300
- ip rsvp policy cops timeout, page 302
- ip rsvp policy default-reject, page 303
- ip rsvp policy identity, page 305
- ip rsvp policy local, page 308
- ip rsvp policy preempt, page 316

- ip rsvp policy vrf, page 317
- ip rsvp pq-profile, page 320

# identity policy (policy-map)

To create an identity policy, use the **identitypolicy** command in policy-map class configuration mode. To remove the policy, use the **no** form of this command.

**identity policy** *policy-name*

**no identity policy** *policy-name*

## Syntax Description

| | |
|---|---|
| *policy-name* | Name of the policy. |

## Command Default

An identity policy is not created.

## Command Modes

Policy-map class configuration (config-pmap-class)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

This command refers to the global identity policy that is configured on the device that contains the access policies that are to be applied. Only a single identity policy can be configured under the policy class configuration submode. If the identity policy is not defined on the device, an error is generated during the application of the policy.

## Examples

The following example shows how create an identity policy called healthy_identity:

```
Router(config)# policy-map type control tag healthy_pmap
Router(config-pmap)# class healthy_class
Router(config-pmap-class)# identity policy healthy_identity
Router(config-pmap-class)# end
```

The following example shows how to add an access group called healthy_acl to the identity policy named healthy_identity:

```
Router(config)# identity policy healthy_identity
Router(config-identity-policy)# access-group healthy_acl
Router(config-identity-policy)# end
```

## Related Commands

| Command | Description |
|---|---|
| **class type tag** | Associates a class map with a policy map. |

| Command | Description |
|---|---|
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |

# ingress-class-map

T o classify the IPv4, IPv6, and MPLS packets for POS, channelized, and clear-channel SPAs, use the **ingress-class-map**commandin global configuration mode to first define the ingress classification template. The ingress classification template is identified by the index-id that will be applied to an interface later. Use the **no** form of this command to remove the template.

**ingress-class-map** *class-map index*

**no ingress-class-map**

## Syntax Description

| | |
|---|---|
| *class-map index* | Class-map index-id to identify the ingress classification template that is a combination of IPv4, IPv6, and MPLS classifications. The valid range for the maximum number of index class maps per carrier card (CC) is 1 to 62 multiplied-by maximum number of carrier card slots. |

## Command Default

No ingress-class-map index-ids are configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.1S | This command was introduced. |

## Usage Guidelines

To classify high priority packets such as IPv4, IPv6, or MPLS in a SIP or SPA, the classification template is defined using the **ingress-classmap***class-mapindex*command. The classification template-specific details are defined in the template, and the template is attached to an interface using the **plimqosinputclass-map**command. The classification template can be deleted using the **no** command form. Each SIP supports 62 ingress classification templates. The total number of ingress classification templates that can be applied on Cisco ASR 1000 Series Router = number of carrier cards multiplied-by 62.

**Note** The classification template cannot be deleted if the template is being used by an interface.

## Examples

The following example shows how to define a classification template using the **ingress-class-map** command:

```
Router# config
```

```
Router(config)# ingress-class-map 1
Router(config-ing-class-map)#
```

## Related Commands

| Command | Description |
|---|---|
| **plim qos input class-map** | Attaches the classification template to an interface. |

# ip header-compression disable-feedback

To disable the context-status feedback messages from the interface or link, use the **ipheader-compressiondisable-feedback** command in interface configuration mode. To enable context-status feedback messages from the interface or link, use the **no** form of this command.

**ip header-compression disable-feedback**

**no ip header-compression disable-feedback**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Context-status feedback messages are enabled by default.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.3(2)T | This command was introduced. |
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S. |

## Usage Guidelines

The **ipheader-compressiondisable-feedback** command is designed for use with satellite links where the path for the upward link is different from the path for the downward link. When the paths are different, context-status messages are not useful.

The **ipheader-compressiondisable-feedback** command can be used with either Real-Time Transport Protocol (RTP) or TCP header compression.

## Examples

The following example disables the context-status messages on serial interface 2/0:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0
Router(config-if)# ip header-compression disable-feedback
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **ip header-compression max-header** | Specifies the maximum size of the compressed IP header. |

| Command | Description |
|---|---|
| **ip header-compression max-period** | Specifies the maximum number of compressed packets between full headers. |
| **ip header-compression max-time** | Specifies the maximum amount of time to wait before the compressed IP header is refreshed. |

# ip header-compression max-header

To specify the maximum amount of time to wait before the compressed IP header is refreshed, use the **ipheader-compressionmax-header** command in interface configuration mode. To return the amount of time to wait before the compressed IP header is refreshed to the default value, use the **no** form of this command.

**ip header-compression max-header** *max-header-size*

**no ip header-compression max-header** *max-header-size*

## Syntax Description

| | |
|---|---|
| *max-header-size* | Size of the IP header, in bytes. The size of the IP header can be in the range of 20 to 168. |

## Command Default

168 bytes

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.3(2)T | This command was introduced. |
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S. |

## Usage Guidelines

The *max-header-size* argument of the **ipheader-compressionmax-header** command can be used to restrict the size of the header to be compressed.

## Examples

The following example shows how to use the **ipheader-compressionmax-header**command to specify the maximum IP header size of the packet to 100 bytes:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0
Router(config-if)# ip header-compression max-header 100
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **ip header-compression disable-feedback** | Disables context-status feedback messages from the interface or link. |

| Command | Description |
|---|---|
| **ip header-compression max-period** | Specifies the maximum number of compressed packets between full headers. |
| **ip header-compression max-time** | Specifies the maximum amount of time to wait before the compressed IP header is refreshed. |

# ip header-compression max-period

To specify the maximum number of compressed packets between full headers, use the **ipheader-compressionmax-period** command in interface configuration mode. To return the number of compressed packets to the default value, use the **no** form of this command.

**ip header-compression max-period** *number-of-packets*

**no ip header-compression max-period** *number-of-packets*

## Syntax Description

| | |
|---|---|
| *number-of-packets* | Specifies a number of packets between full headers. The number can be in the range of 0 to 65535. |

## Command Default

256 packets

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(2)T | This command was introduced. |
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S. |

## Usage Guidelines

With the **ipheader-compressionmax-period**command, full IP packet headers are sent in an exponentially increasing period after there has been a change in the context status. This exponential increase in the time period avoids the necessity of exchanging messages between the mechanism compressing the header and the mechanism decompressing the header.

By default, the **ipheader-compressionmax-period**command operates on User Datagram Protocol (UDP) traffic only. However, if the **periodicrefresh** keyword of either the **frame-relayiprtpheader-compression**command or the **frame-relaymapiprtpheader-compression** command is configured, the **ipheader-compressionmax-period** command operates on both UDP and Real-Time Transport Protocol (RTP) traffic.

## Examples

In the following example, the **ipheader-compressionmax-period**command is configured to specify the number of packets between full header packets. In this configuration, the packet number specified is 160.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0
Router(config-if)# ip header-compression max-period 160
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **frame-relay ip rtp header-compression** | Enables RTP header compression for all Frame Relay maps on a physical interface. |
| **frame-relay map ip rtp header-compression** | Enables RTP header compression per DLCI. |
| **ip header-compression disable-feedback** | Disables context-status feedback messages from the interface or link. |
| **ip header-compression max-header** | Specifies the maximum size of the compressed IP header. |
| **ip header-compression max-time** | Specifies the maximum amount of time to wait before the compressed IP header is refreshed. |

# ip header-compression max-time

To specify the maximum amount of time to wait before the compressed IP header is refreshed, use the **ipheader-compressionmax-time** command in interface configuration mode. To return to the default value, use the **no** form of this command.

**ip header-compression max-time** *length-of-time*

**no ip header-compression max-time** *length-of-time*

## Syntax Description

| | |
|---|---|
| *length-of-time* | Specifies a different amount of time (other than the default) in seconds to wait before the IP header is refreshed. The range is 0 to 65535. |

## Command Default

If not length of time is configured, the default value is 5 seconds.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.3(2)T | This command was introduced. |
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S. |

## Usage Guidelines

The **ipheader-compressionmax-time** command is designed to avoid losing too many packets if the context status of the receiver has been lost.

If a packet is to be sent and the maximum amount of time has elapsed since the last time the IP header was refreshed, a full header is sent.

By default, the **ipheader-compressionmax-time**command operates on User Datagram Protocol (UDP) traffic only. However, if the **periodicrefresh** keyword of either the **frame-relayiprtpheader-compression**command or the **frame-relaymapiprtpheader-compression** command is configured, the **ipheader-compressionmax-time**command operates on UDP and Real-Time Transport Protocol (RTP) traffic.

## Examples

In the following example, the **ipheader-compressionmax-time**command is configured to specify the maximum amount of time to wait before refreshing the compressed IP header. In this configuration the amount of time to wait is 30 seconds.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0
```

```
Router(config-if)# ip header-compression max-time 30
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **frame-relay ip rtp header-compression** | Enables RTP header compression for all Frame Relay maps on a physical interface. |
| **frame-relay map ip rtp header-compression** | Enables RTP header compression per DLCI. |
| **ip header-compression disable-feedback** | Disables context-status feedback messages from the interface or link. |
| **ip header-compression max-header** | Specifies the maximum size of the compressed IP header. |
| **ip header-compression max-period** | Specifies the maximum number of compressed packets between full headers. |

# ip header-compression recoverable-loss

To enable Enhanced Compressed Real-Time Transport Protocol (ECRTP) on an interface, use the **ipheader-compressionrecoverable-loss** command in interface configuration mode. To disable ECRTP on an interface, use the **no** form of this command.

**ip header-compression recoverable-loss** {**dynamic**| *packet-drops*}

**no ip header-compression recoverable-loss**

## Syntax Description

| | |
|---|---|
| **dynamic** | Dynamic recoverable loss calculation. |
| *packet-drops* | Maximum number of consecutive packet drops. Ranges from 1 to 8. |

## Command Default

When using the **dynamic**keyword, the default value is 4.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.3(11)T | This command was introduced. |

## Usage Guidelines

Enhanced CRTP reduces corruption by changing the way the compressor updates the context at the decompressor. The compressor sends changes multiple times to keep the compressor and decompressor synchronized. This method is characterized by the number of *packet-drops* that represent the quality of the link between the hosts. By repeating the updates, the probability of context corruption due to packet loss is minimized.

The value for the *packet-drops* argument is maintained independently for each context and is not required to be the same for all contexts.

## Examples

The following example shows how to configure a serial interface with Point-to-Point Protocol (PPP) encapsulation and to enable ECRTP with dynamic loss recovery:

```
Router(config)# interface serial 2/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression ietf-format
Router(config-if)# ip header-compression recoverable-loss dynamic
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **debug ip rtp error** | Displays RTP header compression errors. |
| **debug ip rtp header-compression** | Displays events specific to RTP header compression. |
| **ip rtp header-compression** | Enables RTP header compression. |
| **show ip rtp header-compression** | Displays RTP header compression statistics. |

# ip header-compression old-iphc-comp

To revert the IP Header Compression (IPHC) format of compression to the non-RFC-compliant format, use the **ipheader-compressionold-iphc-comp**command in interface configuration mode. To disable the IPHC format of compression, use the **no** form of this command.

**ip header-compression old-iphc-comp**

**no ip header-compression old-iphc-comp**

## Syntax Description

This command has no arguments or keywords.

## Command Default

IPHC format compression is not configured.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 15.1(3)T | This command was introduced. |

## Usage Guidelines

The **ipheader-compressionold-iphc-comp** command must be configured only when the IPHC format of compression or service-policy-based compression is configured.

## Examples

The following example shows how to revert the IPHC format of compression to the non-RFC-compliant format:

```
Router> enable

Router# configure terminal
Router(config)# interface serial 0/0
Router(config-if)# ip header-compression old-iphc-comp
```

## Related Commands

| Command | Description |
|---|---|
| **ip header-compression old-iphc-decomp** | Reverts the IPHC format of decompression to the non-RFC-compliant format. |

# ip header-compression old-iphc-decomp

To revert the IP Header Compression (IPHC) format of decompression to the non-RFC-compliant format, use the **ipheader-compressionold-iphc-decomp**command in interface configuration mode. To retain the normal form of the IPHC format decompression, use the **no** form of this command.

**ip header-compression old-iphc-decomp**

**no ip header-compression old-iphc-decomp**

## Syntax Description

This command has no arguments or keywords.

## Command Default

IPHC format decompression is not configured.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 15.1(3)T | This command was introduced. |

## Usage Guidelines

The **ipheader-compressionold-iphc-decomp** command must be configured only when the IPHC format of compression or service-policy-based compression is configured.

## Examples

The following example shows how to revert the IPHC format of decompression to the non-RFC-compliant format:

```
Router> enable

Router# configure terminal
Router(config)# interface serial 0/0
Router(config-if)# ip header-compression old-iphc-decomp
```

## Related Commands

| Command | Description |
|---|---|
| **ip header-compression old-iphc-comp** | Reverts the IPHC format of compression to the non-RFC-compliant format. |

# ip nbar attribute-map

To create an Network-Based Application Recognition (NBAR) attribute profile, use the **ip nbar attribute-map** command in global configuration mode. To remove an NBAR attribute profile, use the **no** form of this command.

**ip nbar attribute-map** *profile-name*

**no ip nbar attribute-map** *profile-name*

## Syntax Description

| | |
|---|---|
| *profile-name* | Name of the protocol attribute profile. |

## Command Default

A new attribute profile is not created.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(4)M2 | This command was introduced. |
| Cisco IOS XE Release 3.8S | This command was integrated into Cisco IOS XE Release 3.8S. |

## Usage Guidelines

NBAR supports the use of custom protocols to identify custom applications. Custom protocols support static port-based protocols and applications that NBAR does not support.

NBAR allows you to configure attribute profiles for protocols and to attach the profiles with the protocols.

The **ip nbar attribute-map** command lets you create an NBAR attribute profile. Upon using this command, you enter the attribute-map submode, which lets you assign various attributes to custom protocols. This attribute profile can be attached to a protocol by using the **ip nbar attribute-set** *protocol-name profile-name* command.

## Examples

The following example shows how to create an attribute profile for the Network News Transfer Protocol (NNTP):

```
Device# configure terminal
Device(config)# ip nbar attribute-map nntp-attrib
```

## Related Commands

| Command | Description |
|---|---|
| **attribute** | Adds attributes to your attribute profiles. |
| **ip nbar attribute-set** | Attaches a new attribute profile to a protocol. |

# ip nbar attribute-set

To assign an attribute profile to a specific protocol, use the **ip nbar attribute-set** command in global configuration mode. To remove the mapping of the attribute profile to the protocol, use the **no** form of this command.

**ip nbar attribute-set** *protocol-name profile-name*

**no ip nbar attribute-set** *protocol-name profile-name*

## Syntax Description

| | |
|---|---|
| *protocol-name* | Protocol to which you want to assign the attribute profile. |
| *profile-name* | Name of the attribute profile. |

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(4)M2 | This command was introduced. |
| Cisco IOS XE Release 3.8S | This command was integrated into Cisco IOS XE Release 3.8S. |

## Usage Guidelines

Network-Based Application Recognition (NBAR) supports the use of custom protocols to identify custom applications. Custom protocols support static port-based protocols and applications that NBAR does not support.

NBAR lets you configure attribute profiles for protocols, and attach the profiles with the protocols.

You can attach an attribute profile to a protocol using the **ip nbar attribute-set** command. After a profile is attached to a protocol, you can edit the profile by adding or deleting its parameters. You can also remove an attached attribute profile from a protocol.

## Examples

The following example shows how to map an attribute profile to the Application Communication Protocol (ACP):

```
Device# configure terminal
Device(config)# ip nbar attribute-set acp test-profile
```

## Related Commands

| Command | Description |
|---|---|
| **ip nbar attribute-map** | Creates an attribute profile. |

# ip nbar classification tunneled-traffic

To enable application classification of IPv6 traffic that is carried over IPv4 tunnels (IPv6 in IPv4 and teredo) in Network Based Application Recognition, use the **ip nbar classification tunneled-traffic** command in global configuration mode. To disable application classification, use the **no** form of this command.

**ip nbar classification tunneled-traffic** {**ipv6inip**| **teredo**}

**no ip nbar classification tunneled-traffic** {**ipv6inip**| **teredo**}

## Syntax Description

| | |
|---|---|
| **ipv6inip** | Classifies IPv6 in IPv4 tunneling traffic. |
| **teredo** | Classifies teredo tunneling traffic. |

## Command Default

Application classification for IPv6 traffic that is tunneled over IPv6 in IPv4 or teredo tunnels is not enabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |
| Cisco IOS XE Release 3.5S | This command was integrated into Cisco IOS XE Release 3.5S. |
| 15.2(1)S | This command was integrated into Cisco IOS Release 15.2(1)S. |

## Usage Guidelines

The **ipv6inip** keyword enables application classification of IPv6 traffic that is carried over IPv4 tunnels over protocol 41. Protocol 41 includes the tunnel types such as ISATAP, 6to4, and 6rd.

The **teredo** keyword enables application classification of IPv6 traffic that is carried over teredo tunnel. The teredo tunnel is identified by two common default ports, port 3544 and port 3545 over UDP, which are on IPv4 tunnel endpoints.

## Examples

The following example shows how to enable application classification for IPv6 traffic carried over teredo tunnels:

```
Router(config)# ip nbar classification tunneled-traffic teredo
```

# ip nbar custom

To extend the capability of Network-Based Application Recognition (NBAR) protocol discovery, use the **ip nbar custom** command in global configuration mode. To stop NBAR from classifying and monitoring additional static port application or classifying unsupported static port traffic, use the **no** form of this command.

**ip nbar custom** *custom-name* {[*field-offset* {**ascii** *ascii-value* | **decimal** *decimal-value* | **hex** *hex-value* | **variable** *variable-name*}] [**destination** | **source**] [*protocol*] | **http** {**host** *host-name* [**id** *selector-id*] | **url** *url-name* [**host** *host-name*] [**id** *selector-id*]}}

**no ip nbar custom** *custom-name*

## Syntax Description

| | |
|---|---|
| *custom-name* | Name of the custom protocol.<br>The name must be no longer than 24 characters and can contain only lowercase letters (a-z), digits (0-9), and the underscore (_) character. |
| *field-offset* | (Optional) A digit representing the byte location for payload inspection on the field. |
| **ascii** *ascii-value* | Sets the format of the inspection value as ASCII and defines the length of the value. Up to 16 characters can be searched. Regular expressions are not supported. |
| **decimal** *decimal-value* | Sets the format of the inspection value as decimal and defines the length of the value. Up to 4 bytes are supported. |
| **hex** *hex-value* | Sets the format of the inspection value as hex and defines the length of the value. Up to 4 bytes are supported. |
| **variable** *variable-name* | When you enter the **variable** keyword, a specific portion of the custom protocol can be treated as an NBAR-supported protocol (for example, a specific portion of the custom protocol can be tracked using class-map statistics and can be matched using the **class-map** command). The *variable-name* argument specifies the name for the field to search in the payload. |
| **destination** | (Optional) Specifies the destination direction of the packets. If you do not specify the destination direction, all packets traveling in both directions are monitored by NBAR. |

| | |
|---|---|
| **source** | (Optional) Specifies the source direction of the packets. If you do not specify the source direction, all packets traveling in both directions are monitored by NBAR. |
| *protocol* | (Optional) Specifies whether the protocol that is implemented by the application is TCP or UDP and defines the following values:<br>• *port-number*—The port to be monitored by the custom application monitors. Up to 16 individual ports can be specified.<br>• **id** *selector-id*—(Optional) Specifies the application ID of the custom protocol. Range: 1 to 65535.<br>• **range** *start-value end-value*—Specifies a range of ports for the custom application to monitor. The *start-value* variable represents the first port in the range, and the *end-value* variable represents the last port in the range. A range of up to 1000 ports can be specified for each custom protocol. |
| **http** | Specifies the name of the custom HTTP string. |
| **host** *host-name* | Specifies the hostname in the HTTP header string. |
| **url** *url-name* | Specifies the URL in the HTTP header string. |
| **id** *selector-id* | (Optional) Specifies the application ID of the custom protocol. Range: 1 to 65535. |

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |
| 12.3(11)T | The **variable** *field-name field-length* keyword-argument pair was introduced. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(17a)SX1 | This command was integrated into Cisco IOS Release 12.2(17a)SX1. |

| Release | Modification |
|---|---|
| 15.2(4)M2 | This command was integrated into Cisco IOS Release 15.2(4)M2. The **http** keyword and the **host** *host-name* and the **url** *url-name* keyword-argument pairs were introduced. |
| Cisco IOS XE Release 3.8S | This command was integrated into Cisco IOS XE Release 3.8S. |

## Usage Guidelines

Use the **ip nbar custom** command in global configuration mode to classify and monitor additional static port applications or to allow NBAR to classify unsupported static port traffic.

The first three characters of a custom protocol must be unique from any predefined protocol. Otherwise, you receive an ambiguous command error message.

NBAR can support up to 128 protocols.

If you enter the **variable** keyword when you configure a custom protocol, traffic statistics for the variable appear in some NBAR class map **show** outputs.

The *protocol* argument stands for the protocol that is implemented by the application. You specify the protocol as TCP or UDP before proceeding to the next set of elements given here:

{*port-number* [**id** *selector-id*] | **range** *start-value end-value*}

Up to 24 variable values per custom protocol can be configured in class maps. For instance, in the following configuration, four variables are used:.

```
Device(config)# ip nbar custom ftdd 23 variable scid 1 tcp range 5001 5005
Device(config)# class-map match-any active-craft
Device(config-cmap)# match protocol ftdd scid 0x15
Device(config-cmap)# match protocol ftdd scid 0x21
Device(config-cmap)# exit
Device(config)# class-map match-any passive-craft
Device(config-cmap)# match protocol ftdd scid 0x11
Device(config-cmap)# match protocol ftdd scid 0x22
```

## Examples

The following example shows how to classify HTTP packets based on any URL that contains the string “whatsnew/latest” preceded by zero or more characters:

```
Device(config)# ip nbar custom my_http http url "*whatsnew/latest"
```

The following example shows how to classify packets based on any hostname that contains the strings “sell” or “dell” followed by zero or more characters:

```
Device(config)# ip nbar custom my_http http host "*(s|d)ell"
```

The following example shows how to configure the custom protocol “app_sales1” to identify TCP packets that have a source port of 4567 and that contain the term SALES in the fifth byte of the payload:

```
Device(config)# ip nbar custom app_sales1 5 ascii SALES source tcp 4567
```

The following example shows how to set the custom protocol “virus_home” to identify UDP packets that have a destination port of 3000 and contain “0x56” in the seventh byte of the payload:

```
Device(config)# ip nbar custom virus_home 7 hex 0x56 destination udp 3000
```

The following example shows how to set the custom protocol “media_new” to identify TCP packets that have a destination or source port of 4500 and that have a value of 90 in the sixth byte of the payload:

```
Device(config)# ip nbar custom media_new 6 decimal 90 tcp 4500
```

The following example shows how to set the custom protocol msn1 to look for TCP packets that have a destination or source port of 6700:

```
Device(config)# ip nbar custom msn1 tcp 6700
```

The following example shows how to set the custom protocol mail_x to look for UDP packets that have a destination port of 8202:

```
Device(config)# ip nbar custom mail_x destination udp 8202
```

The following example shows how to configure the custom protocol mail_y to look for UDP packets that have destination ports between 3000 and 4000, inclusive:

```
Device(config)# ip nbar custom mail_y destination udp range 3000 4000
```

The following example shows how to create the custom protocol ftdd by using a variable. A class map matching this custom protocol based on the variable is also created. In this example, class map matchscidinftdd matches all traffic that has the value 804 at byte 23 entering or leaving TCP ports 5001 to 5005. The variable scid is 2 bytes in length.

```
Device(config)# ip nbar custom ftdd 23 variable scid 2 tcp range 5001 5005
Device(config)# class-map matchscidinftdd
Device(config-cmap)# match protocol ftdd scid 804
```

The same example above can also be done by using hexadecimal values in the class map as follows:

```
Router(config)# ip nbar custom ftdd 23 variable scid 2 tcp range 5001 5005
Router(config)# class-map matchscidinftdd
Router(config-cmap)# match protocol ftdd scid 0x324
```

The following example shows how to use the **variable** keyword to create a custom protocol, and how to configure class maps to classify different values within the variable field into different traffic classes. In the example below, variable scid values 0x15, 0x21, and 0x27 are classified into class map active-craft, while scid values 0x11, 0x22, and 0x25 are classified into class map passive-craft:

```
Router(config)# ip nbar custom ftdd 23 variable scid 1 tcp range 5001 5005
Router(config)# class-map match-any active-craft
Router(config-cmap)# match protocol ftdd scid 0x15
Router(config-cmap)# match protocol ftdd scid 0x21
Router(config-cmap)# match protocol ftdd scid 0x27
Device(config-cmap)# exit
Router(config)# class-map match-any passive-craft
Router(config-cmap)# match protocol ftdd scid 0x11
Router(config-cmap)# match protocol ftdd scid 0x22
Router(config-cmap)# match protocol ftdd scid 0x25
```

# ip nbar pdlm

To extend or enhance the list of protocols recognized by network-based application recognition (NBAR) through a Cisco-provided Packet Description Language Module (PDLM), use the **ipnbarpdlmcommandinglobalconfiguration** mode. To unload a PDLM previously loaded, use the **no** form of this command.

**ip nbar pdlm** *pdlm-name*

**no ip nbar pdlm** *pdlm-name*

## Syntax Description

| | |
|---|---|
| *pdlm-name* | URL at which the PDLM can be found on the flash card. |

## Command Default

No default behavior or values

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)XE2 | This command was introduced. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.1(13)E | This command was implemented on Catalyst 6000 family switches without FlexWAN modules. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(17a)SX1 | This command was integrated into Cisco IOS Release 12.2(17a)SX1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

The **ipnbarpdlm** command is used to extend the list of protocols recognized by a given version of NBAR or to enhance an existing protocol recognition capability. NBAR can be given an external PDLM at run time. In most cases, the PDLM enables NBAR to recognize new protocols without requiring a new Cisco IOS image or a router reload. Only Cisco can provide you with a new PDLM.

A list of the available PDLMs can be viewed online at Cisco.com.

## Examples

The following example configures NBAR to load the citrix.pdlm PDLM from flash memory on the router:

```
ip nbar pdlm flash://citrix.pdlm
```

## Related Commands

| Command | Description |
|---|---|
| **show ip nbar pdlm** | Displays the current PDLM in use by NBAR. |

# ip nbar port-map

To configure network-based application recognition (NBAR) to search for a protocol or protocol name using a port number other than the well-known port, use the **ipnbarport-map**command in global configuration mode. To look for the protocol name using only the well-known port number, use the **no** form of this command.

**ip nbar port-map** *protocol-name* [**tcp**| **udp**] *port-number*

**no ip nbar port-map** *protocol-name* [**tcp**| **udp**] *port-number*

## Syntax Description

| | |
|---|---|
| *protocol-name* | Name of protocol known to NBAR. |
| **tcp** | (Optional) Specifies that a TCP port will be searched for the specified *protocol-name* argument. |
| **udp** | (Optional) Specifies that a User Datagram Protocol (UDP) port will be searched for the specified *protocol-name* argument. |
| *port-number* | Assigned port for named protocol. The *port-number* argument is either a UDP or a TCP port number, depending on which protocol is specified in this command line. Up to 16 *port-number* arguments c an be specified in one command line. Port number values can range from 0 to 65535. |

## Command Default

No protocol is configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)XE2 | This command was introduced. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.1(13)E | This command was implemented on Catalyst 6000 family switches without FlexWAN modules. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(17a)SX1 | This command was integrated into Cisco IOS Release 12.2(17a)SX1. |

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

Use the **ipnbarport-map** command to tell NBAR to look for the protocol or protocol name , using a port number or numbers other than the well-known Internet Assigned Numbers Authority (IANA)-assigned) port number. For example, use this command to configure NBAR to look for Telnet on a port other than 23. You can specify up to 16 ports with this command.

Some of the NBAR protocols look at the ports as well as follow the heuristic approach for traffic classification. If you apply different ports to a protocol using the **ipnbarport-map**command, the heuristic nature of the protocol does not change. The advantage to adding a port number is better performance.

You can remove well-known ports from a predefined port map only if you first set the predefined port map to a port not belonging to any existing port map. For example, if you want to define a custom port map X and also associate it with port 20, you get an error saying that it is not possible. However, if you associate port map A with another port first, such as port 100, and then remove its association with port 20, you can associate custom port map X with port 20.

**Note** For best results, do not configure the Citrix or BitTorrent protocols.

## Examples

The following example configures NBAR to look for the protocol Structured Query Language (SQL)*NET on port numbers 63000 and 63001 instead of on the well-known port number:

```
Router(config)# ip nbar port-map sqlnet tcp 63000 63001
```

## Related Commands

| Command | Description |
|---|---|
| **show ip nbar port-map** | Displays the current protocol-to-port mappings in use by NBAR. |

# ip nbar protocol-discovery

To configure Network-Based Application Recognition (NBAR) to discover traffic for all protocols that are known to NBAR on a particular interface, use the **ipnbarprotocol-discovery**command in interface configuration mode or VLAN configuration mode. To disable traffic discovery, use the **no** form of this command.

**ip nbar protocol-discovery** [**ipv4**| **ipv6**]

**no ip nbar protocol-discovery**

## Syntax Description

| | |
|---|---|
| **ipv4** | (Optional) Specifies protocol discovery only for IPv4 packets on the interface. |
| **ipv6** | (Optional) Specifies protocol discovery only for IPv6 packets on the interface. |

## Command Default

Traffic discovery is disabled.

## Command Modes

Interface configuration (config-if) VLAN configuration (config-vlan)--Catalyst switches only

## Command History

| Release | Modification |
|---|---|
| 12.0(5)XE2 | This command was introduced. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.1(13)E | This command was implemented on Catalyst 6000 family switches without FlexWAN modules. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(17a)SX1 | This command was integrated into Cisco IOS Release 12.2(17a)SX1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(18)ZYA | This command was integrated into Cisco IOS Release 12.2(18)ZYA. Support for Layer 2 Etherchannels, Layer 3 Etherchannels, and VLAN configuration mode was provided (Catalyst switches only). |
| Cisco IOS XE Release 3.3S | This command was integrated into Cisco IOS XE Release 3.3S on the Cisco ASR 1000 Series Aggregation Services Routers. The **ipv6** keyword was added. |

## Usage Guidelines

Use the**ipnbarprotocol-discovery**command to configure NBAR to keep traffic statistics for all protocols that are known to NBAR. Protocol discovery provides an easy way to discover application protocols passing through an interface so that QoS policies can be developed and applied. The protocol discovery feature discovers any protocol traffic supported by NBAR. Protocol discovery can be used to monitor both input and output traffic and may be applied with or without a service policy enabled.

In Cisco IOS XE Release 3.3S, L3 and L4 Internet Assigned Numbers Authority (IANA) protocols are supported for IPv4 and IPv6 packets.

Enter the **ipv4** keyword to enable protocol discovery statistics collection for IPv4 packets, or enter the **ipv6** keyword to enable protocol discovery statistics collection for IPv6 packets. Specifying either of these keywords enables the protocol discovery statistics collection for the specified IP version only. If neither keyword is specified, statistics collection is enabled for both IPv4 and IPv6. The **no** form of this command is not required to disable a keyword because the statistics collection is enabled for the specified keyword only.

**Layer 2/3 Etherchannel Support**

With Cisco IOS Release 12.2(18)ZYA, intended for use on the Cisco 6500 series switch that is equipped with a Supervisor 32/PISA, the **ipnbarprotocol-discovery**command is supported on both Layer 2 and Layer 3 Etherchannels.

## Examples

The following example shows how to configure protocol discovery for both IPv4 and IPv6 on an Ethernet interface:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 2/4
Router(config-if)# ip nbar protocol-discovery
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **show ip nbar protocol-discovery** | Displays the statistics gathered by the NBAR Protocol Discovery feature. |

# ip nbar protocol-pack

To load a network based application recognition (NBAR)protocol pack, use the **ip nbar protocol-pack** command in global configuration mode. To remove the loaded protocol pack, use the **no** form of this command.

**ip nbar protocol-pack** *protocol-pack* **[force]**

**no ip nbar protocol-pack** *protocol-pack*

## Syntax Description

| | |
|---|---|
| *protocol-pack* | Protocol pack file path and name. |
| **force** | (Optional) Loads a protocol pack of a lower version than the default protocol pack version. |

## Command Default

The default protocol pack is loaded.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.3S | This command was introduced. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T. |

## Usage Guidelines

The **ip nbar protocol-pack** command provides an easy way to load a protocol pack, which is a single compressed file that contains multiple Protocol Description Language (PDL) files and a manifest file. Before this command was introduced, PDLs had to be loaded separately. You can use this command to load a set of protocols, which helps NBAR to recognize additional protocols for classification on your network.

Use the **force** keyword in the following situations:

- To load a specific protocol pack of a lower version other than the default protocol pack version present in the Cisco IOS image.
- To retain the existing protocol pack version irrespective of upgrading to newer version or reverting to a protocol pack of lower version.
- To override the active protocol checks.

## Examples

The following example shows how to load a protocol pack named defProtoPack from the harddisk:

```
Router# configure terminal
Router(config)# ip nbar protocol-pack harddisk:defProtoPack
```

The following example shows how to load a protocol pack of lower version using the **force** keyword:

```
Router# configure terminal
Router(config)# ip nbar protocol-pack harddisk:olddefProtoPack force
```

## Related Commands

| Command | Description |
|---|---|
| **default ip nbar protocol-pack** | Loads the base version of the protocol pack and removes all other loaded protocol packs. |
| **show ip nbar protocol-pack** | Displays protocol pack information. |

# ip nbar resources

The **ipnbarresources**command is replaced by the **ipnbarresourcesprotocol** and the**ipnbarresourcessystem** commands. See the **ipnbarresourcesprotocol** and the**ipnbarresourcessystem**commands for more information.

# ip nbar resources protocol

To set the expiration time for network-based application recognition (NBAR) flow-link tables on a protocol basis, use the **ip nbar resources protocol** command in global configuration mode. To set the expiration time to its default value, use the **no** form of this command.

**ip nbar resources protocol** *link-age* [ *protocol-name* ]

**no ip nbar resources protocol** *link-age* [ *protocol-name* ]

## Syntax Description

| | |
|---|---|
| *link-age* | Time, in seconds, at which the links for a protocol expire. The range is from 1 to 1000000000. The default is 120.<br>**Note** The value of the *link-age* argument must be greater than or equal to the value of the *system-link-age* argument that is set by using the **ip nbar resources system** command. |
| *protocol-name* | (Optional) Name of the protocol as registered in a loaded Protocol Description Language (PDL) module. |

## Command Default

The link age for all protocols is 120 seconds.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| Cisco IOS XE Release 3.2S | This command was implemented on the Cisco ASR 1000 Series Routers. |

## Usage Guidelines

The value of the *link-age* argument must be greater than or equal to the *system-link-age* value that is set by using the **ip nbar resources system** command.

If you enter an invalid value for the *link-age* argument, the following error message is displayed:

```
%NBAR ERROR: protocol link age entered must be greater than or equal to the system link
age, <system link age>
```

To display a list of supported protocols, enter the **match protocol ?** or the **show ip nbar port-map** command.

The **ip nbar resources protocol** command must include the *protocol-name* argument to set the link age of a specific protocol. If you do not include the *protocol-name* argument, the link age timer of all protocols is set to the specified link age value.

The **no ip nbar resources protocol** command must include the *protocol-name* argument to reset the link age of a specific protocol. If you do not include the *protocol-name* argument, the link age timer of all protocols is set to 120 seconds.

If you enter a protocol name that does not exist, the following error message is displayed:

```
%NBAR ERROR: <entered string> is not a valid protocol
```

In addition to resetting the link age in all state nodes associated with a specified protocol, the protocol name, along with its link age, is saved in NVRAM for potential device resets.

## Examples

The following example shows how to set the link age for all protocols to 360 seconds:

```
Device# configure terminal
Device(config)# ip nbar resources protocol 360
```

The following example shows how to set the link age for kazaa2 protocol to 180 seconds:

```
Device# configure terminal
Device(config)# ip nbar resources protocol 180 kazaa2
```

## Related Commands

| Command | Description |
|---|---|
| **ip nbar resources system** | Sets the expiration time and memory requirements for NBAR flow-link tables on a systemwide basis. |

# ip nbar resources system

To set the expiration time and memory requirements for network-based application recognition (NBAR) flow-link tables on a systemwide basis, use the**ipnbarresourcessystem**command in global configuration mode. To remove the active links, use the **no** form of this command.

**ip nbar resources system** *system-link-age initial-memory exp-memory*

**no ip nbar resources system**

## Syntax Description

| | |
|---|---|
| *system-link-age* | Time, in seconds, at which the links for a system are aged (expire). The range is from 10 to 86400. The default is 30. |
| *initial-memory* | Size of memory, in kilobytes, allocated for the links at initialization. The range is from 1 to 30000. The default is 10 percent of the total amount of free memory at system initialization and varies from platform to platform. |
| *exp-memory* | Size of memory, in kilobytes, that can be expanded if NBAR detects that more space is needed for the links. The range is from 0 to 112. The default is 112.<br>**Note** The default is based on the size of an internal NBAR structure and may change in future releases. |

## Command Default

The default system link age is 30 seconds upon NBAR activation.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

Because the **ipnbarresourcessystem** command affects NBAR on a systemwide basis, you should not change the parameters arbitrarily. Doing so may cause NBAR to perform inefficiently or incorrectly. The default values are effective in most instances.

## Examples

In the following example, the system link age is 30 seconds, the initial memory is 200 kilobytes, and the expanded memory is 112 kilobytes:

```
Router# configure terminal
Router(config)# ip nbar resources system 30 200 112
```

## Related Commands

| Command | Description |
|---|---|
| **ip nbar resources protocol** | Sets the expiration time for NBAR flow-link tables on a protocol basis. |

# ip options

To drop or ignore IP options packets that are sent to the router, use the **ip options**command in global configuration mode. To disable this functionality and allow all IP options packets to be sent to the router, use the **no** form of this command.

**ip options** {**drop**| **ignore**}

**no ip options** {**drop**| **ignore**}

## Syntax Description

| | |
|---|---|
| **drop** | Router drops all IP options packets that it receives. |
| **ignore** | Router ignores all options and treats the packets as though they did not have any IP options. (The options are not removed from the packet--just ignored.)<br>**Note** This option is not available on the Cisco 10000 series router. |

## Command Default

This command is not enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(23)S | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. |
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S. |
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC. |
| 12.3(19) | This command was integrated into Cisco IOS Release 12.3(19). |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2 for the PRE3. |

## Usage Guidelines

The **ip options** command allows you to filter IP options packets, mitigating the effects of IP options on the router, and on downstream routers and hosts.

Drop and ignore modes are mutually exclusive; that is, if the drop mode is configured and you configure the ignore mode, the ignore mode overrides the drop mode.

**Cisco 10720 Internet Router**

The **ip options ignore** command is not supported. Only drop mode (the **ip options drop** command) is supported.

**Cisco 10000 Series Router**

This command is only available on the PRE3. The PRE2 does not support this command.

The **ip options ignore** command is not supported. The router supports only the **ip options drop** command.

## Examples

The following example shows how to configure the router (and downstream routers) to drop all options packets that enter the network:

```
ip options drop
% Warning:RSVP and other protocols that use IP Options packets may not function in drop or
 ignore modes.
end
```

# ip rsvp admission-control compression predict

To configure Resource Reservation Protocol (RSVP) admission control compression prediction, use the **iprsvpadmission-controlcompressionpredict**command in interface configuration mode. To disable compression prediction, use the **no** form of this command.

**ip rsvp admission-control compression predict** [**method** {**rtp**| **udp**} [**bytes-saved** *N*]]

**no ip rsvp admission-control compression predict** [**method** {**rtp**| **udp**} [**bytes-saved** *N*]]

## Syntax Description

| | |
|---|---|
| **method** | (Optional) Type of compression used. |
| **rtp udp** | Real-Time Transport Protocol (RTP) or User Data Protocol (UDP) compression schemes. |
| **bytes-saved** *N* | (Optional) Predicted number of bytes saved per packet when RSVP predicts that compression will occur using the specified method. Values for N for RTP are 1 to 38; for UDP, 1 to 26. |

## Command Default

This command is enabled by default. The default value of bytes saved for RTP is 36; for UDP, 20.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |

## Usage Guidelines

Use the **iprsvpadmission-controlcompressionpredict**command to disable or enable the RSVP prediction of compression for a specified method or all methods if neither **rtp** nor**udp**is selected. You can adjust the default compressibility parameter that RSVP uses to compute the compression factor for each flow.

If you use the **iprsvpadmission-controlcompressionpredict**command to change the compression method or the number of bytes saved per packet, these values affect only new flows, not existing ones.

There are two approaches to compression--conservative and aggressive. When you predict compression conservatively, you assume savings of fewer bytes per packet, but receive a higher likelihood of guaranteed quality of service (QoS). You are allowed more bandwidth per call, but each link accommodates fewer calls. When you predict compression aggressively, you assume savings of more bytes per packet, but receive a lower likelihood of guaranteed QoS. You are allowed less bandwidth per call, but each link accommodates more calls.

## Examples

The following example shows how to set the compressibility parameter for flows using the RTP method to 30 bytes saved per packet:

```
Router(config-if)# ip rsvp admission-control compression predict method rtp bytes-saved 30
```

The following example shows how to set the compressibility parameter for flows using the UDP method to 20 bytes saved per packet:

```
Router(config-if)# ip rsvp admission-control compression predict method udp bytes-saved 20
```

The following example shows how to disable RTP header compression prediction:

```
Router(config-if)# no ip rsvp admission-control compression predict method rtp
```

The following shows how to disable UDP header compression prediction:

```
Router(config-if)# no ip rsvp admission-control compression predict method udp
```

**Note** Disabling the compressibility parameter affects only those flows using the specified method.

## Related Commands

| Command | Description |
|---|---|
| **show ip rtp header-compression** | Displays statistics about RTP header compression. |

# ip rsvp aggregation ip

To enable Resource Reservation Protocol (RSVP) aggregation on a router, use the **iprsvpaggregationip** command in global configuration mode. To disable RSVP aggregation, use the **no** form of this command.

**ip rsvp aggregation ip**

**no ip rsvp aggregation ip**

## Syntax Description

This command has no arguments or keywords.

## Command Default

RSVP aggregation is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRC | This command was introduced. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

When you enable aggregation on a router, the router can act as an aggregator, a deaggregator, or an interior router. To perform aggregator and deaggregator functions, the RSVP process must see messages with the RSVP-E2E-IGNORE protocol type (134) on a router; otherwise, the messages are forwarded as data by the router's data plane. The**iprsvpaggregationip** command enables RSVP to identify messages with the RSVP-E2E-IGNORE protocol. You then configure additional commands to specify the aggregation and deaggregation behavior of end-to-end (E2E) reservations.

The **iprsvpaggregationip** command registers a router to receive RSVP-E2E-IGNORE messages. It is not necessary to issue this command on interior routers because they are only processing RSVP aggregate reservations. If you do so, you may decrease performance because the interior router will then unnecessarily process all the RSVP-E2E-IGNORE messages.

**Note** If you enable RSVP aggregation globally on an interior router, then you should configure all interfaces as interior. Otherwise, interfaces default to exterior and discard RSVP-E2E-IGNORE packets.

## Examples

The following example shows how to enable RSVP aggregation on a router:

```
Router(config)# ip rsvp aggregation ip
```

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp aggregation ip** | Displays RSVP summary aggregation information. |

# ip rsvp aggregation ip map

To configure Resource Reservation Protocol (RSVP) aggregation rules that tell a router how to map end-to-end (E2E) reservations onto aggregate reservations, use the **iprsvpaggregationipmap** command in global configuration mode. To disable RSVP aggregation mapping rules, use the **no** form of this command.

**ip rsvp aggregation ip map** {**access-list** *acl-number*| **any**} **dscp** *value*

**no ip rsvp aggregation ip map** {**access-list** *acl-number*| **any**}

## Syntax Description

| | |
|---|---|
| **access-list** | Specifies an Access Control List (ACL). |
| *acl-number* | Number of the ACL. Values are 1 to 199. |
| **any** | Indicates the match criteria used if all reservations between an aggregator and a deaggregator are to be aggregated onto a single DSCP. |
| **dscp** *value* | Specifies the differentiated services code point (DSCP). Values can be the following:<br>• 0 to 63--Numerical DSCP values. The default value is 0.<br>• af1 to af43--Assured forwarding (AF) DSCP values.<br>• cs1 to cs7--Type of service (ToS) precedence values.<br>• default--Default DSCP value.<br>• ef--Expedited forwarding (EF) DSCP values. |

## Command Default

No aggregation mapping rules are configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRC | This command was introduced. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

Use the **iprsvpaggregationipmap** command to configure a single global rule for mapping E2E reservations onto aggregates.

Before using the **iprsvpaggregationipmap** command, you should configure an ACL to define a group of RSVP endpoints whose reservations are to be aggregated onto a single DSCP. The ACL can be a standard or extended ACL and matches as follows:

**Standard ACLs**

- IP address matches the RSVP PATH message sender template or RSVP RESV message filter spec; this is the IP source address or the RSVP sender.

**Extended ACLs**

The ACLs used within the **iprsvpaggregationipmap** command match the RSVP message objects as follows for an extended ACL:

- Source IP address and port match the RSVP PATH message sender template or RSVP RESV message filter spec; this is the IP source or the RSVP sender.
- Destination IP address and port match the RSVP PATH/RESV message session object IP address; this is the IP destination address or the RSVP receiver.
- Protocol matches the RSVP PATH/RESV message session object protocol; if protocol = IP, then it matches the source or destination address as above.

**Note** In classic (unaggregated) RSVP, a session is identified in the reservation message session object by the destination IP address and protocol information. In RSVP aggregation, a session is identified by the destination IP address and DSCP within the session object of the aggregate RSVP message. E2E reservations are mapped onto a particular aggregate RSVP session identified by the E2E reservation session object alone or a combination of the session object and sender template or filter spec.

## Examples

In the following example, access list 1 is defined for all RSVP messages whose RSVP PATH message session object destination address is in the 10.1.0.0 subnet so that the deaggregator maps those reservations onto an aggregate reservation for the DSCP associated with the AF41 per hop behavior:

```
Router(config)# access-list 1 permit host 10.1.0.0 0.0.255.255
Router(config)# ip rsvp aggregation ip map access-list 1 dscp af41
```

In the following example, all reservations between an aggregator and a deaggregator are to be aggregated onto a single DSCP:

```
Router(config)# ip rsvp aggregation ip map any dscp af41
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp aggregation ip** | Enables RSVP aggregation on a router. |
| **show ip rsvp aggregation ip** | Displays RSVP summary aggregation information. |

# ip rsvp aggregation ip reservation dscp

To configure Resource Reservation Protocol (RSVP) aggregate reservation attributes (also called token bucket parameters) on a per-differentiated services code point (DSCP) basis, use the **iprsvpaggregationipreservationdscp**command in global configuration mode. To remove aggregation reservation attributes, use the **no** form of this command.

**ip rsvp aggregation ip reservation dscp** *value* [**aggregator** *agg-ip-address*] **traffic-params static rate** *data-rate* [**burst** *burst-size*] [**peak** *peak-rate*]

**no ip rsvp aggregation ip reservation dscp** *value* [**aggregator** *agg-ip-address*] **traffic-params static rate** *data-rate* [**burst** *burst-size*] [**peak** *peak-rate*]

## Syntax Description

| | |
|---|---|
| *value* | The DSCP value for aggregate reservations. Values can one of the following:<br>• 0 to 63--Numerical DSCP values. The default value is 0.<br>• af11 to af43--Assured forwarding (AF) DSCP values.<br>• cs1 to cs7--Type of service (ToS) precedence values.<br>• default--Default DSCP value.<br>• ef--Expedited forwarding (EF) DSCP values. |
| **aggregator** *agg-ip-address* | (Optional) Specifies the IP address of the aggregator for which the data-rate, burst-size, and peak-rate traffic parameters apply.<br>**Note** If omitted, all aggregate reservations to a deaggregator use the same token bucket parameters. |
| **traffic-params** | Specifies the traffic parameter attributes. |
| **static** | Specifies the static traffic parameter attributes. |
| **rate** *data-rate* | Specifies the average data rate, in kilobits per second. Range is from 1 to 10000000. |
| **burst** *burst-size* | (Optional) Specifies the maximum data burst size, in kilobytes. Range is from 1 to 8192.<br>**Note** If omitted, this value is equal to the aggregate rate value. |

| | |
|---|---|
| **peak** *peak-rate* | (Optional) Specifies the peak data rate, in kilobits per second. Range is from 1 to 10000000.<br>**Note** If omitted, this value is equal to the aggregate rate value. |

## Command Default

No aggregation reservation attributes (token bucket parameters) are configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRC | This command was introduced. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

You can use the **iprsvpaggregationipreservationdscp**command to configure the token bucket parameters statically.

The *data-rate*, *burst-size*, and *peak-rate*arguments are required on deggregators to help construct the flowspec object for aggregate RESV messages. Existing RSVP procedures specify that the size of a reservation established for a flow is set to the minimum of the PATH sender_tspec and the RESV flowspec. So if the aggregate PATH sender_tspec *data-rate*, *burst-size*, or *peak-rate*arguments are greater than the *data-rate*, *burst-size*, or *peak-rate*arguments configured on the deaggregator, the aggregate RESV flowspec object will contain the minimum of *data-rate*, *burst-size*, and *peak-rate* from the PATH message and the configured values.

When the aggregate reservation size is changed to a value less strict than the total bandwidth of the end-to-end (E2E) reservations mapped to the aggregate, preemption may occur.

When the aggregate bandwidth is lowered, if preemption is required and has not been enabled by issuing the **iprsvppolicypreempt** command, then the change is rejected and the following messages may appear:

```
RSVP:AGG: Command not accepted.
RSVP-AGG: This change requires some E2E reservations to be removed and
RSVP:AGG: preemption is not enabled. Issue 'ip rsvp policy preempt'
RSVP:AGG: in order to make this change.
```

## Examples

The following example shows how to configure an aggregate RESV message for an aggregate reservation established with aggregator 10.10.10.10, for DSCP = AF11, including a flowspec that requests an average rate and peak rate of 10 kbps and a burst size of 8 KB:

```
Router(config)# ip rsvp aggregation ip reservation dscp af11 aggregator 10.10.10.10
traffic-params static rate 10 burst 8 peak 10
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp aggregation ip** | Enables RSVP aggregation on a router. |
| **ip rsvp policy preempt** | Redistributes bandwidth from lower-priority reservations to high-priority reservations. |
| **show ip rsvp aggregation ip** | Displays RSVP summary aggregation information. |

# ip rsvp aggregation ip role interior

To configure Resource Reservation Protocol (RSVP) aggregation on aggregator and deaggregator interior routers facing an aggregation region, use the **iprsvpaggregationiproleinterior** command in interface configuration mode. To disable RSVP aggregation on aggregator and deaggregator routers, use the **no** form of this command.

**ip rsvp aggregation ip role interior**

**no ip rsvp aggregation ip role interior**

## Syntax Description

This command has no arguments or keywords.

## Command Default

RSVP aggregation is not configured on aggregator and deaggregator interior routers.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRC | This command was introduced. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

This command does not have any effect on a router until end-to-end (E2E) messages arrive on an interface.

If a router is an interior node for all E2E flows, you do not have to configure any aggregation commands. RSVP will not get notifications on any of the RSVP-E2E-IGNORE messages that are forwarded as IP datagrams; however, because the router is loaded with an image that supports aggregation, the router will process aggregate signaling messages correctly.

If you enable aggregation on an interior node, all its interfaces must be configured as interior. Otherwise, all the interfaces have the exterior role, and any E2E Path (E2E-IGNORE) messages arriving at the router are discarded.

In summary, there are two options for an interior router:

- No RSVP aggregation configuration commands are entered.
- Aggregation is enabled and all interfaces are configured as interior.

If the interior role of an interface is unconfigured, all aggregate and E2E reservations installed on that interface are brought down.

### Additional Required Configuration Commands

If you enable aggregation on any RSVP interface on an aggregator or deaggregator as well as interfaces of interior routers, you must also configure the following commands:

- **ip rsvp resource-provider none**
- **ip rsvp data-packet classification none**

The reason for configuring these commands is because Cisco IOS Release 12.2(33)SRC and Cisco IOS XE Release 2.6 support control plane aggregation only. The RSVP data packet classifier does not support aggregation. Data plane aggregation must be achieved by using the RSVP Scalability Enhancements feature.

## Examples

The following example shows how to configure the Ethernet 0/0 interface on an aggregator or deaggregator interior router:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ip rsvp aggregation ip role interior
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp aggregation ip** | Enables RSVP aggregation on a router. |
| **ip rsvp data-packet classification none** | Disables RSVP data packet classification. |
| **ip rsvp resource-provider none** | Configures a resource provider for an aggregate flow. |
| **show ip rsvp aggregation ip** | Displays RSVP summary aggregation information. |

# ip rsvp atm-peak-rate-limit

To set a limit on the peak cell rate (PCR) of reservations for all newly created Resource Reservation Protocol (RSVP) switched virtual circuits (SVCs) established on the current interface or any of its subinterfaces, use the **iprsvpatm-peak-rate-limit** command in interface configuration mode. To remove the current peak rate limit, in which case the reservation peak rate is limited by the line rate, use the **no** form of this command.

**ip rsvp atm-peak-rate-limit** *limit*

**no ip rsvp atm-peak-rate-limit**

## Syntax Description

| | |
|---|---|
| *limit* | The peak rate limit of the reservation specified, in KB. The minimum value allowed is 1 KB; the maximum value allowed is 2 GB. |

## Command Default

The peak rate of a reservation defaults to the line rate.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Each RSVP reservation corresponds to an ATM SVC with a certain peak cell rate (PCR), sustainable cell rate (SCR), and maximum burst size. The PCR, also referred to as the peak rate, can be configured by the user or allowed to default to the line rate.

RSVP controlled-load reservations do not define any peak rate for the data. By convention, the allowable peak rate in such reservations is taken to be infinity, which is usually represented by a very large number. Under these circumstances, when a controlled-load reservation is converted to an ATM SVC, the PCR for the SVC becomes correspondingly large and may be out of range for the switch. You can use the **iprsvpatm-peak-rate-limit** command to limit the peak rate.

The following con ditions determine the peak rate limit on the RSVP SVC:

- The peak rate defaults to the line rate.

- If the peak rate is greater than the configured peak rate limiter, the peak rate is lowered to the peak rate limiter.
- The peak rate cannot be less than the reservation bandwidth. If this is the case, the peak rate is raised to the reservation bandwidth.

**Note** Bandwidth conversions applied to the ATM space from the RSVP space are also applied to the peak rate.

The peak rate limit is local to the router; it does not affect the normal messaging of RSVP. Only the SVC setup is affected. Large peak rates are sent to the next host without modification.

For RSVP SVCs established on subinterfaces, the peak rate limit applied to the subinterface takes effect on all SVCs created on that subinterface. If a peak rate limit is applied to the main interface, the rate limit has no effect on SVCs created on a subinterface of the main interface even if the limit value on the main interface is lower than the limit applied to the subinterface.

For a given interface or subinterface, a peak rate limit applied to that interface affects only new SVCs created on the interface, not existing SVCs.

**Note** This command is available only on interfaces that support the **iprsvpsvc-required** command.

Use the **showiprsvpatm-peak-rate-limit** command to determine the peak rate limit set for an interface or subinterface, if one is configured.

## Examples

The following configuration sample sets the peak rate limit for ATM interface 2/0/0.1 to 100 KB:

```
interface atm2/0/0.1
 ip rsvp atm-peak-rate-limit 100
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp svc-required** | Enables creation of an SVC to service any new RSVP reservation made on the interface or subinterface. |
| **show ip rsvp interface** | Displays RSVP-related interface information. |

# ip rsvp authentication

To activate Resource Reservation Protocol (RSVP) cryptographic authentication, use the **iprsvpauthentication**command in interface configuration mode. To deactivate authentication, use the **no** form of this command.

**ip rsvp authentication**

**no ip rsvp authentication**

## Syntax Description

This command has no arguments or keywords.

## Command Default

RSVP cryptographic authentication is deactivated.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

Use the **iprsvpauthentication** command to deactivate and then reactivate RSVP authentication without reentering the other RSVP authentication configuration commands. You should not enable authentication unless you have previously configured a key. If you issue this command before the **iprsvpauthenticationkey** command, you get a warning message indicating that RSVP discards all messages until you specify a key. The **noiprsvpauthentication**command disables RSVP cryptographic authentication. However, the command does not automatically remove any other authentication parameters that you have configured. You must issue a specific **noiprsvpauthentication**command; for example, **noiprsvpauthenticationkey**,**noiprsvpauthenticationtype**, or **noiprsvpauthenticationwindow-size**, if you want to remove them from the configuration.

The**iprsvpauthentication**command is similar to the**iprsvpneighbor** command. However, the **iprsvpauthentication** command provides better authentication and performs system logging.

## Examples

The following command activates authentication on an interface:

```
Router(config-if)# ip rsvp authentication
```

The following command deactivates authentication on an interface:

```
Router(config-if)# no ip rsvp authentication
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp authentication key** | Specifies the key (string) for the RSVP authentication algorithm. |
| **ip rsvp authentication type** | Specifies the algorithm used to generate cryptographic signatures in RSVP messages. |
| **ip rsvp authentication window-size** | Specifies the maximum number of RSVP authenticated messages that can be received out of order. |
| **ip rsvp neighbor** | Enables neighbors to request a reservation. |

# ip rsvp authentication challenge

To make Resource Reservation Protocol (RSVP) perform a challenge-response handshake with any new RSVP neighbors on a network, use the **iprsvpauthenticationchallenge**command in interface configuration mode. To disable the challenge-response handshake, use the **no** form of this command.

**ip rsvp authentication challenge**

**no ip rsvp authentication challenge**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The challenge-response handshake initiated by this command is disabled.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

The i**prsvpauthenticationchallenge** command requires RSVP to perform a challenge-response handshake with any new RSVP neighbors that are discovered on a network. Such a handshake allows the router to thwart RSVP message replay attacks while booting, especially if there is a long period of inactivity from trusted RSVP neighbors following the reboot. If messages from trusted RSVP neighbors arrive very quickly after the router reboots, then challenges may not be required because the router will have reestablished its security associations with the trusted nodes before the untrusted nodes can attempt replay attacks.

If you enable RSVP authentication globally on an interface over which a Multiprotocol Label Switching (MPLS) Traffic Engineering (TE) label switched path (LSP) travels and the router on which authentication is enabled experiences a stateful switchover (SSO), the following occurs:

- If challenges are disabled (you did not specify the **iprsvpauthenticationchallenge** command), the LSP recovers properly.
- If challenges are enabled (you specified the **iprsvpauthenticationchallenge** command), more RSVP signaling messages are required and the LSP takes longer to recover or the forwarding state may time out and the LSP does not recover. If a timeout occurs, data packet forwarding is interrupted while the headend router signals a new LSP.

If you enable RSVP authentication challenges, you should consider enabling RSVP refresh reduction by using the **iprsvpsignallingrefreshreduction** command. While a challenge handshake is in progress, the receiving

router that is initiating the handshake discards all RSVP messages from the node that is being challenged until the handshake-initiating router receives a valid challenge response.

**Note** If a neighbor does not reply to the first challenge message after 1 second, the Cisco IOS software sends another challenge message and waits 2 seconds. If no response is received to the second challenge, the Cisco IOS software sends another and waits 4 seconds. If no response to the third challenge is received, the Cisco IOS software sends a fourth challenge and waits 8 seconds. If there is no response to the fourth challenge, the Cisco IOS software stops the current challenge to that neighbor, logs a system error message, and does not create a security association for that neighbor. This kind of exponential backoff is used to recover from challenges dropped by the network or busy neighbors.

Activating refresh reduction enables the challenged node to resend dropped messages more quickly once the handshake has completed. This causes RSVP to reestablish reservation state faster when the router reboots.

Enable authentication challenges wherever possible to reduce the router's vulnerability to replay attacks.

## Examples

The following example shows how to enable RSVP to perform a challenge-response handshake:

```
Router(config-if)# ip rsvp authentication challenge
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling refresh reduction** | Enables RSVP refresh reduction. |

# ip rsvp authentication key

To specify the key (string) for the Resource Reservation Protocol (RSVP) authentication algorithm, use the **iprsvpauthenticationkey**command in interface configuration mode. To disable the key, use the **no** form of this command.

**ip rsvp authentication key** *pass-phrase*

**no ip rsvp authentication key**

## Syntax Description

| | |
|---|---|
| *pass-phrase* | Phrase that ranges from 8 to 40 characters. See "Usage Guidelines" for additional information. |

## Command Default

No key is specified.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

Use the **iprsvpauthenticationkey** command to select the key for the authentication algorithm. This key is a passphrase of 8 to 40 characters. It can include spaces; quotes are not required if spaces are used. The key can consist of more than one word. We recommend that you make the passphrase as long as possible. This key must be the same for all RSVP neighbors on this interface. As with all passwords, you should choose them carefully so that attackers cannot easily guess them.

Here are some guidelines:

- Use a mixture of upper- and lowercase letters, digits, and punctuation.
- If using just a single word, do not use a word contained in any dictionary of any language, spelling lists, or other lists of words.
- Use something easily remembered so you do not have to write it down.
- Do not let it appear in clear text in any file or script or on a piece of paper attached to a terminal.

By default, RSVP authentication keys are stored in clear text in the router configuration file, but they can optionally be stored as encrypted text in the configuration file. To enable key encryption, use the global

configuration **keyconfig-key1***string*command. After you enter this command, the passphrase parameter of each **iprsvpauthenticationkey** command is encrypted with the Data Encryption Standard (DES) algorithm when you save the configuration file. If you later issue a **nokeyconfig-key** 1 *string*command, the RSVP authentication key is stored in clear text again when you save the configuration.

The *string*argumentis not stored in the configuration file; it is stored only in the router's private NVRAM and will not appear in the output of a **showrunning-config**or **showconfig** command. Therefore, if you copy the configuration file to another router, any encrypted RSVP keys in that file will not be successfully decrypted by RSVP when the router boots and RSVP authentication will not operate correctly. To recover from this, follow these steps on the new router:

1. For each RSVP interface with an authentication key, issue a **noiprsvpauthenticationkey**command to clear the old key.
2. For that same set of RSVP interfaces, issue an **iprsvpauthenticationkey** command to reconfigure the correct clear text keys.
3. Issue a global **keyconfig-key** 1 *string*command to reencrypt the RSVP keys for the new router.
4. Save the configuration.

## Examples

The following command shows how to set the passphrase to 11223344 in clear text:

```
Router(config-if)# ip rsvp authentication key 11223344
```

The following command shows how to encrypt the authentication key:

```
Router# configure terminal
Router(config)# key config-key 1 11223344
Router(config)# end
```

## Related Commands

| Command | Description |
|---|---|
| **key config-key** | Defines a private DEF key for the router. |

# ip rsvp authentication key-chain

To specify a list of keys for the Resource Reservation Protocol (RSVP) neighbors, use the **iprsvpauthenticationkey-chain**command in global configuration mode. To disable the key chain, use the **no** form of this command. To set the key chain to its default, use the **no**form of this command.

**ip rsvp authentication key-chain** *string*

**no ip rsvp authentication key-chain**

## Syntax Description

| | |
|---|---|
| *string* | Name of key chain. The range is from 1 to 2147483647 keys. |

## Command Default

No key chain is specified.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.0(29)S | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 15.0(1)M | This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M. |

## Usage Guidelines

Use the **iprsvpauthenticationkey-chain** command to select the key chain.

**Note** You cannot use the**iprsvpauthenticationkey** and the **iprsvpauthenticationkey-chain** commands on the same router interface. The commands supersede each other; however, no error message is generated.

## Examples

The following example shows how to set the global default key chain to RSVPkey:

```
Router(config)# ip rsvp authentication key-chain RSVPkey
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp authentication key** | Specifies the interface key (string) for the RSVP authentication algorithm. |
| **show key chain** | Displays authentication key information. |

# ip rsvp authentication lifetime

To control how long Resource Reservation Protocol (RSVP) maintains security associations with other trusted RSVP neighbors, use the **iprsvpauthenticationlifetime**command in interface configuration mode. To disable the lifetime setting, use the **no** form of this command.

**ip rsvp authentication lifetime** *hh* **:** *mm* **:** *ss*

**no ip rsvp authentication lifetime** *hh* **:** *mm* **:** *ss*

## Syntax Description

| | |
|---|---|
| *hh* **:** *mm* **:** *ss* | Hours: minutes: seconds that RSVP maintains security associations with other trusted RSVP neighbors. The range is 1 second to 24 hours. The default is 30 minutes. The colons are required in the syntax. |

## Command Default

If you do not specify a security association lifetime setting, 30 minutes is used.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

Use the**iprsvpauthenticationlifetime** command to indicate when to end security associations with RSVP trusted neighbors. If an association's lifetime expires, but at least one valid, RSVP authenticated message was received in that time period, RSVP resets the security association's lifetime to this configured value. When a neighbor stops sending RSVP signaling messages (that is, the last reservation has been torn down), the memory used for the security association is freed as well as when the association's lifetime period ends. The association can be re-created if that RSVP neighbor resumes its signaling. Setting the lifetime to shorter periods allows memory to be recovered faster when the router is handling a lot of short-lived reservations. Setting the lifetime to longer periods reduces the workload on the router when establishing new authenticated reservations.

Use the **cleariprsvpauthentication** command to free security associations before their lifetimes expire.

## Examples

The following command sets the lifetime period for 30 minutes and 5 seconds:

```
Router(config-if)# ip rsvp authentication lifetime 00:30:05
```

## Related Commands

| Command | Description |
|---|---|
| **clear ip rsvp authentication** | Eliminates RSVP security associations before their lifetimes expire. |

# ip rsvp authentication neighbor

To activate Resource Reservation Protocol (RSVP) cryptographic authentication for a neighbor, use the **iprsvpauthenticationneighbor**command in global configuration mode. To deactivate authentication for a neighbor, use the **no** form of this command.

**ip rsvp authentication neighbor** {**access-list** *acl-name-or-number*| **address** *address*} **[challenge]** [**key-chain** *name*] [**type** {**md5**| **sha-1**}] [**window-size** *number-of-messages*]

**no ip rsvp authentication neighbor** {**access-list** *acl-name-or-number*| **address** *address*} **[challenge]** [**key-chain** *name*] [**type** {**md5**| **sha-1**}] [**window-size** *number-of-messages*]

## Syntax Description

| | |
|---|---|
| **access-list** *acl-name-or-number* | Specifies a standard numbered or named IP access list that describes the set of neighbor IP addresses that share this key. |
| **address** *address* | Specifies a single IP address for a specific neighbor; usually one of the neighbor's physical or logical (loopback) interfaces. |
| **challenge** | (Optional) Requires RSVP to perform a challenge-response handshake with an RSVP neighbor for which RSVP does not have an existing security association in memory. |
| **key-chain** *name* | (Optional) Specifies the name of a key chain that contains the set of keys to be used to communicate with the neighbor. |
| **type** | (Optional) Specifies the algorithm to generate cryptographic signatures in RSVP messages. |
| **md5** | (Optional) Specifies the RSA Message Digest 5 (md5) algorithm. |
| **sha-1** | (Optional) Specifies the National Institute of Standards and Technologies (NIST) Secure Hash Algorithm-1; it is newer and more secure than **md5**. |
| **window-size** *number-of-messages* | (Optional) Specifies the maximum number of authenticated messages that can be received out of order. The range is from 1 to 64. The default value is 1. |

## Command Default

Neighbor cryptographic authentication is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.0(29)S | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 15.0(1)M | This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M. |

## Usage Guidelines

If you omit the optional keywords, the **iprsvpauthenticationneighbor** command enables RSVP cryptographic authentication for a neighbor. Using the optional keywords inherits the global defaults.

In order to enable per-neighbor authentication, you must issue the **iprsvpauthenticationneighbor**command(or the **noiprsvpauthenticationneighbor** command to disable authentication ). If you issue the **iprsvpauthentication** command without **neighbor**, then this command enables authentication for all neighbors and interfaces, regardless of whether there are any per-neighbor or per-interface keys defined. If you issue the **iprsvpauthenticationneighbor**command , then authentication is enabled only for that neighbor.

**Access Control Lists**

A single ACL can describe all the physical and logical interfaces that one neighbor can use to receive RSVP messages from a router; this can be useful when multiple routes exist between two neighbors. One ACL could also specify a number of different neighbors who, along with your router, will share the same key(s); however, this is generally not considered to be good network security practice.

If numbered, the ACL must be in the 1 to 99 range or the 1300 to 1999 range, giving a total of 798 numbered ACLs that can be used to configure neighbor keys (assuming some of them are not being used for other purposes). There is no enforced limit on the number of standard named IP ACLs. The IP addresses used in the ACL should contain at least the neighbor's physical interface addresses; router ID addresses can be added if necessary, especially when using Multi-Protocol Label Switching (MPLS) Traffic Engineering (TE).

The existing**ipaccess-liststandard** command must be used for creating named or numbered standard IP ACLs for RSVP neighbors because standard ACLs deal with just source or destination addresses while extended ACLs deal with five tuples and are more complex to configure. The RSVP CLI returns an error message if any type of ACL other than standard is specified:

```
Router(config)# ip rsvp authentication neighbor access-list 10 key-chain wednesday
% Invalid access list name.
RSVP error: unable to find/create ACL
```

Named standard IP ACLs are also recommended because you can include the neighbor router's hostname as part of the ACL name, thereby making it easy to identify the per-neighbor ACLs in your router configuration.

The RSVP CLI displays an error message if a valid named or numbered ACL is specified, but a nonexistent or invalid key chain has not been associated with it, since the lack of a key chain could cause RSVP messages to or from that neighbor to be dropped:

```
Router(config)# ip rsvp authentication neighbor access-list myneighbor key-chain xyz
RSVP error: Invalid argument(s)
```

**Key Chains**

In the key-chain parameter, the keys are used in order of ascending expiration deadlines. The only restriction on the name is that it cannot contain spaces. The key-chain parameter is optional; that is, you could omit it if you were trying to change other optional authentication parameters for the RSVP neighbor. However, when searching for a key, RSVP ignores any **iprsvpauthenticationneighboraccess-list**command that does not include a key-chain parameter that refers to a valid key chain with at least one unexpired key.

**Error and Warning Conditions**

The RSVP CLI returns an error if any of the key IDs in the chain are duplicates of key IDs in any other chains already assigned to RSVP; for example,

```
Router(config)# ip rsvp authentication neighbor access-list myneighbor key-chain abc
RSVP error: key chains abc and xyz contain duplicate key ID 1
RSVP error: Invalid argument(s)
```

The RSVP CLI returns an error if the specified key chain does not exist or does not contain at least one unexpired key.

If a key chain is properly defined and RSVP later tries to send a message to that neighbor, but cannot find a valid, unexpired per-neighbor or per-interface key, RSVP generates the RSVP_AUTH_NO_KEYS_LEFT system message indicating that a key could not be obtained for that neighbor.

If the key chain contains keys with finite expiration times, RSVP generates the RSVP_AUTH_ONE_KEY_EXPIRED message to indicate when each key has expired.

If RSVP receives a message from a neighbor with the wrong digest type, it generates the RSVP_MSG_AUTH_TYPE_MISMATCH system message indicating that there is a digest type mismatch with that neighbor.

If RSVP receives a message that is a duplicate of a message already in the window or is outside the window, RSVP logs the BAD_RSVP_MSG_RCVD_AUTH_DUP or the BAD_RSVP_MSG_RCVD_AUTH_WIN error message indicating that the message sequence number is invalid.

If a challenge of a neighbor fails or times out, RSVP generates the BAD_RSVP_MSG_RCVD_AUTH_COOKIE system message or the RSVP_MSG_AUTH_CHALLENGE_TIMEOUT message, indicating that the specified neighbor failed to respond successfully to a challenge.

## Examples

The following example shows how to create an access list and a key chain for neighbors V, Y, and Z enable authentication globally using inheritance for all other authentication parameters:

```
Router# configure terminal
Router(config)# ip access-list standard neighbor_V
Router(config-std-nacl)# permit 10.0.0.2
Router(config-std-nacl)#
permit 10.1.16.1
Router(config-std-nacl)# exit
Router(config)# ip access-list standard neighbor_Y
Router(config-std-nacl)# permit 10.0.1.2
Router(config-std-nacl)# permit 10.16.0.1
Router(config-std-nacl)# exit
Router(config)# ip access-list standard neighbor_Z
Router(config-std-nacl)# permit 10.16.0.2
Router(config-std-nacl)# permit 10.1.0.2
```

```
Router(config-std-nacl)# permit 10.0.1.2
Router(config-std-nacl)#
exit
Router(config)# ip rsvp authentication neighbor access-list neighbor_V key-chain neighbor_V
Router(config)# ip rsvp authentication neighbor access-list neighbor_Y key-chain neighbor_Y
Router(config)# ip rsvp authentication neighbor access-list neighbor_Z key-chain neighbor_Z
Router(config)# ip rsvp authentication
Router(config)# end
```

The following example shows how to create an access list and a key chain for neighbors V, Y, and Z and and enable the authentication explicitly for each neighbor:

```
Router(config)# ip rsvp authentication neighbor access-list neighbor_V key-chain neighbor_V
Router(config)# ip rsvp authentication neighbor access-list neighbor_V
Router(config)# ip rsvp authentication neighbor access-list neighbor_Y key-chain neighbor_Y
Router(config)# ip rsvp authentication neighbor access-list neighbor_Y
Router(config)# ip rsvp authentication neighbor access-list neighbor_Z key-chain neighbor_Z
Router(config)# ip rsvp authentication neighbor access-list neighbor_Z
Router(config)#
end
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp authentication** | Activates RSVP cryptographic authentication. |

# ip rsvp authentication type

To specify the type of algorithm used to generate cryptographic signatures in Resource Reservation Protocol (RSVP) messages, use the **iprsvpauthenticationtype**command in interface configuration or global configuration mode. To specify that no type of algorithm is used, use the **no** form of this command. To remove the type from your configuration, use the **default** form of this command.

**Note** Before you use the**noiprsvpauthenticationtype** command, see the "Usage Guidelines" section for more information.

### Syntax for T Releases

**ip rsvp authentication type** {**md5**| **sha-1**}

**no ip rsvp authentication type**

**default ip rsvp authentication type**

### Syntax for 12.0S and 12.2S Releases

**ip rsvp authentication type** {**md5**| **sha-1**}

**default ip rsvp authentication type**

## Syntax Description

| | |
|---|---|
| **md5** | RSA Message Digest 5 algorithm. |
| **sha-1** | National Institute of Standards and Technologies (NIST) Secure Hash Algorithm-1; it is newer and more secure than MD5. |

## Command Default

If no algorithm is specifed, **md5** is used.

## Command Modes

Interface configuration (config-if) Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| 12.0(29)S | This command was introduced in global configuration mode for all neighbors. A **default** form of the command was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

Use the **iprsvpauthentiationtype** command to specify the algorithm to generate cryptographic signatures in RSVP messages. If you do not specify an algorithm, **md5** is used.

If you use the **iprsvpauthentiationtype** command rather than the **iprsvpauthentiationneighbortype**command, the global default for type changes.

The

Although the **noiprsvpauthentiationtype** command is supported in Cisco IOS T releases, the **defaultiprsvpauthentiationtype** command is recommended **toremovetheauthentiationtypefromaconfigurationandforcethetypetoitsdefault.**

## Examples

## Examples

The following example shows how to set the type to sha-1 for interf**aceauthentication**:

```
Router(config-if)# ip rsvp authentication type sha-1
```

## Examples

The following examples show how to set the type to sha-1 for nei**ghborauthentication:**

```
Router(config)# ip rsvp authentication neighbor address 10.1.1.1 type sha-1
```

or

```
Router(config)# ip rsvp authentication neighbor access-list 1 type sha-1
```

The following example shows how to set the global default type to **sha-1forauthentication**:

```
Router(config)# ip rsvp authentication type sha-1
```

## Examples

The following example shows how to remove the type from your configuration and forces the type to its default:

```
Router(config)# default ip rsvp authentication type
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp authentication key** | Specifies the key (string) for the RSVP authentication algorithm. |
| **ip rsvp authentication neighbor type** | Sets the type for a specific neighbor. |

# ip rsvp authentication window-size

To specify the maximum number of Resource Reservation Protocol (RSVP) authenticated messages that can be received out of order, use the **iprsvpauthenticationwindow-size**command in interface configuration mode. To disable the window size (or to use the default value of 1), use the **no** form of this command.

**ip rsvp authentication window-size** [ *number-of-messages* ]

**no ip rsvp authentication window-size**

## Syntax Description

| | |
|---|---|
| *number-of-messages* | (Optional) Maximum number of authenticated messages that can be received out of order. The range is 1 to 64; the default value is 1. |

## Command Default

If no window size is specified, a value of 1 is used.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

Use the **iprsvpauthenticationwindow-size**command to specify the maximum number of RSVP authenticated messages that can be received out of order. All RSVP authenticated messages include a sequence number that is used to prevent replays of RSVP messages.

With a default window size of one message, RSVP rejects any duplicate authenticated messages because they are assumed to be replay attacks. However, sometimes bursts of RSVP messages become reordered between RSVP neighbors. If this occurs on a regular basis, and you can verify that the node sending the burst of messages is trusted, you can use the **iprsvpauthenticationwindow-size** command option to allow for the burst size such that RSVP will not discard such reordered bursts. RSVP will still check for duplicate messages within these bursts.

## Examples

The following example shows how to set the window size to 2:

```
Router(config-if)# ip rsvp authentication window-size 2
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp authentication** | Activates RSVP cryptographic authentication. |

# ip rsvp bandwidth

To enable Resource Reservation Protocol (RSVP) for IP on an interface, use the **ip rsvp bandwidth** command in interface configuration mode. To disable RSVP completely, use the **no** form of this command.

### Syntax for Cisco IOS Release 15.1(2)T and Later Releases

**ip rsvp bandwidth** [*interface-bandwidth* [**percent** *percent-bandwidth*| [ *single-flow-bandwidth* ] [**sub-pool** *bandwidth*]] [**ingress** [*ingress-bandwidth*| **percent** *percent-bandwidth* [*maximum-ingress-bandwidth*| **percent** *percent-bandwidth*]]]]

**no ip rsvp bandwidth**

### Syntax for Cisco IOS Releases 12.0S and 12.2S, Cisco IOS XE Release 2.6, and Later Releases

{**ip rsvp bandwidth** [**rdm** [**bc0** *interface-bandwidth*]] [*single-flow-bandwidth* [**bc1** *bandwidth*| **sub-pool** *bandwidth*]] [*interface-bandwidth* [*single-flow-bandwidth* [**bc1** *bandwidth*| **sub-pool** *bandwidth*]]]| **mam max-reservable-bw** [*interface-bandwidth* [ *single-flow-bandwidth* ] [**bc0** *interface-bandwidth* [**bc1** *bandwidth*]]]| **percent** *percent-bandwidth* [ *single-flow-bandwidth* ]}

{**no ip rsvp bandwidth** [**rdm** [**bc0** *interface-bandwidth*]] [*single-flow-bandwidth* [**bc1** *bandwidth*| **sub-pool** *bandwidth*]] [*interface-bandwidth* [*single-flow-bandwidth* [**bc1** *bandwidth*| **sub-pool** *bandwidth*]]]| **mam max-reservable-bw** [*interface-bandwidth* [ *single-flow-bandwidth* ] [**bc0** *bc0-pool* [**bc1** *bandwidth*]]]| **percent** *percent-bandwidth* [ *single-flow-bandwidth* ]}

## Syntax Description

| | |
|---|---|
| *interface-bandwidth* | (Optional) Maximum amount of bandwidth, in kbps, that can be allocated by RSVP flows. The range is from 1 to 10000000. |
| **percent** *percent-bandwidth* | (Optional) Specifies a percentage of interface bandwidth. The range is from 1 to 1000.<br>• When used with the **ingress** keyword, the **percent** keyword specifies the percentage of interface bandwidth to be configured as RSVP ingress bandwidth. |
| *single-flow-bandwidth* | (Optional) Maximum amount of bandwidth, in kbps, that may be allocated to a single flow. The range is from 1 to 10000000.<br>**Note** This value is ignored by the Diffserve-aware Multiprotocol Label Switching (MPLS) traffic engineering feature. |

| | |
|---|---|
| **sub-pool** *bandwidth* | (Optional) Specifies the amount of bandwidth, in kbps, on the interface that is to be reserved to a portion of the total. The range is from 1 to the value of the smaller of the *interface-bandwidth* and **rdm** *bandwidth* arguments. This keyword and argument pair is used in the traditional (pre-IETF)-Standard) implementation of Diffserv-aware traffic engineering (DS-TE). |
| **ingress** | (Optional) Configures the RSVP ingress reservable bandwidth. |
| *ingress-bandwidth* | (Optional) Ingress reservable bandwidth, in kbps. The range is from 1 to 10000000. |
| *maximum-ingress-bandwidth* | (Optional) Maximum amount of ingress bandwidth, in kbps, that can be allocated to a single flow. The range is from 1 to 10000000; however, the amount you can configure depends on how much bandwidth remains in the pool. |
| **rdm** | (Optional) Specifies the Russian Doll Model (RDM) for DS-TE. |
| **bc0** *interface-bandwidth* | (Optional) Specifies the amount of bandwidth, in kbps, on the interface to be reserved to the total (formerly called “global pool”). The range is from 1 to the value of the **max-reservable-bw** *interface-bandwidth* keyword and argument pair. |
| **bc1** *bandwidth* | (Optional) Specifies the same bandwidth portion as **bc0** *interface-bandwidth*; namely, the amount of bandwidth, in kbps, on the interface that is to be reserved to a portion of the total. |
| **mam** | (Optional) Specifies the Maximum Allocation Model (MAM) for DS-TE. |
| **max-reservable-bw** | (Optional) Specifies the maximum reservable bandwidth and sets a limit on the size of the total pool. |
| **bc1** *bandwidth* | (Optional) Specifies the amount of bandwidth, in kbps, on the interface to be reserved to a portion of the total. (Formerly, this portion was called the “subpool”.) The range is from 1 to the value of the **max-reservable-bw** *interface-bandwidth* keyword and argument. |

**Command Default**

RSVP is disabled by default. If you enter the **ip rsvp bandwidth** command without any bandwidth values (for example, **ip rsvp bandwidth** followed by pressing the Enter key), a default bandwidth value (that is, 75 percent of the link bandwidth) is assumed for both the *interface-bandwidth* and *single-flow-bandwidth* arguments.

**Command Modes**

Interface configuration (config-if)

**Command History**

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.0(11)ST | This command was integrated into Cisco IOS Release 12.0(11)ST. The **sub-pool** keyword was added. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(18)SXD | This command was integrated into Cisco IOS Release 12.2(18)SXD. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SRB | This command was modified. The IETF Standard for DS-TE was added through the **rdm** and **mam** keywords, and their subsidiary arguments. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |
| 15.1(2)T | This command was modified. The **percent** *percent-bandwidth* keyword and argument pair was added. |
| 15.(1)3T | This command was modified. The **ingress** keywordthe *ingress-bandwidth* argument, and the *maximum-ingress-bandwidth* argument were added. |
| 15.2(3)T | This command was modified. Support for IPv6 was added. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |

**Usage Guidelines**

RSVP cannot be configured with distributed Cisco Express Forwarding.

RSVP is disabled by default to allow backward compatibility with systems that do not implement RSVP.

Weighted Random Early Detection (WRED) or fair queueing must be enabled first.

When using this command for DS-TE in IETF Standard mode, you must use either **rdm** and its arguments or **mam** and its arguments; you cannot use both. For more details about each alternative, see *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering* by F. Le Faucheur (RFC 4127)

and *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering* by F. Le Faucheur and W. Lai (RFC 4125).

To eliminate only the subpool portion of the bandwidth, use the **no** form of this command with the **sub-pool** keyword.

You can use the **ip rsvp bandwidth ingress** command to enable the ingress Call Admission Control (CAC) functionality. You can use the **no ip rsvp bandwidth** command to disable the ingress CAC functionality on an interface. However, this command also disables RSVP on the interface. To disable only the ingress functionality on the interface, use the **ip rsvp bandwidth** *interface-bandwidth single-flow-bandwidth* command.

All the configurations related to the **ip rsvp bandwidth** command are applicable for both IPv4 and IPv6 sessions. The IPv4 and IPv6 sessions are admitted only if there is enough bandwidth available in the common bandwidth pool. It is not possible to apply a separate bandwidth limit for IPv4 reservations and IPv6 reservations.

## Examples

The following example shows a T1 (1536 kb/s) link configured to permit RSVP reservation of up to 1158 kbps, but no more than 100 kbps for any given flow on serial interface 0. Fair queueing is configured with 15 reservable queues to support those reserved flows, should they be required.

```
Device(config)# interface serial 0
Device(config-if)# fair-queue 64 256 15
Device(config-if)# ip rsvp bandwidth 1158 100
```

## Related Commands

| Command | Description |
|---|---|
| **fair-queue (WFQ)** | Enables WFQ for an interface. |
| **ip rsvp neighbor** | Enables neighbors to request a reservation. |
| **ip rsvp reservation** | Enables a device to behave like it is receiving and forwarding RSVP RESV messages. |
| **ip rsvp sender** | Enables a device to behave like it is receiving and forwarding RSVP PATH messages. |
| **ip rsvp udp-multicasts** | Instructs the device to generate UDP-encapsulated RSVP multicasts whenever it generates an IP-encapsulated multicast packet. |
| **random-detect (interface)** | Enables WRED or DWRED. |
| **show ip rsvp installed** | Displays RSVP-related installed filters and corresponding bandwidth information. |
| **show ip rsvp interface** | Displays RSVP-related interface information. |
| **show ip rsvp neighbor** | Displays current RSVP neighbors. |
| **show ip rsvp reservation** | Displays RSVP-related receiver information currently in the database. |

| Command | Description |
|---|---|
| **show ip rsvp sender** | Displays RSVP PATH-related sender information currently in the database. |

# ip rsvp bandwidth ignore

To ignore the Resource Reservation Protocol (RSVP) tunnel bandwidth configuration, use the **iprsvpbandwidthignore** command in interface configuration mode.

**ip rsvp bandwidth ignore**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The RSVP tunnel bandwidth configuration is used.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 15.1(2)T | This command was introduced. |
| 15.1(1)S | This command was integrated into Cisco IOS Release 15.1(1)S. |

## Usage Guidelines

You can use the **iprsvpbandwidthignore** command to ignore any RSVP bandwidth configuration on the tunnel. If you need to reconfigure the RSVP bandwidth, use the**iprsvpbandwidth** or **iprsvpbandwidthpercent** command.

## Examples

The following example shows how to ignore the RSVP bandwidth configuration on a tunnel interface:

```
Router(config)# interface tunnel 1
Router(config-if)# ip rsvp bandwidth ignore
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp bandwidth** | Enables RSVP for IP on an interface. |
| **ip rsvp bandwidth percent** | Enables RSVP for IP on an interface and specifies a percentage of the total interface bandwidth as available in the RSVP bandwidth pool. |
| **show ip rsvp interface detail** | Displays the hello configuration for all interfaces. |

# ip rsvp bandwidth percent

To enable Resource Reservation Protocol (RSVP) for IP on an interface and to configure percentages of bandwidth available for RSVP and single flow bandwidth pools, use the **iprsvpbandwidthpercent**command in interface configuration mode. To disable RSVP on an interface, use the **no** form of this command.

**ip rsvp bandwidth percent** *interface-bandwidth* [*max-flow-bw*| **percent** *flow-bandwidth*]

**no ip rsvp bandwidth**

## Syntax Description

| | |
|---|---|
| *interface-bandwidth* | Percentage of interface bandwidth configured for RSVP. The range is from 1 to 1000. |
| *max-flow-bw* | (Optional) Maximum amount of bandwidth, in kb/s, configured for a single flow. The range is from 1 to 10000000; however, the amount you can configure depends on how much bandwidth remains in the pool. |
| **percent** *flow-bandwidth* | (Optional) Specifies the percentage of the bandwidth to be used as flow bandwidth. The range is from 1 to 1000. |

## Command Default

RSVP is disabled by default; therefore, no percentage of bandwidth is set.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRB | This command was introduced. |
| 15.1(2)T | This command was modified. The **percent** and *flow-bandwidth*keyword and argument combination was added. |

## Usage Guidelines

RSVP cannot be configured with distributed Cisco Express Forwarding.

RSVP is disabled by default to allow backward compatibility with systems that do not implement RSVP.

Weighted Random Early Detection (WRED) or fair queueing must be enabled first.

Use the **iprsvpbandwidthpercent** command to set the RSVP bandwidth pool to a specified percentage of interface bandwidth. When you issue the **iprsvpbandwidthpercent** command, the RSVP bandwidth pool adjusts dynamically whenever the bandwidth of the interface changes.

You can use the **iprsvpbandwidthpercent***percent-bandwidth***percent***flow-bandwidth*commandtoconfigure a percentage of interface bandwidth as RSVP bandwidth. The RSVP bandwidth is used to perform RSVP Connection Admission Control (CAC). This command allows oversubscription. That is, you can configure more than 100 percent of the interface bandwidth to be used as RSVP bandwidth and per flow bandwidth.

You can choose to configure an absolute value as the amount of bandwidth used for RSVP by using the **iprsvpbandwidth***rsvp-bandwidth* command on the member links of a bundle. If you use the **iprsvpbandwidthpercent***rsvp-bandwidth* command, then the RSVP bandwidth changes in parallel with the change in the interface bandwidth. The RSVP bandwidth of the bundle depends only on the bundle interface's bandwidth, which in turn depends on the interface bandwidth of the member link and not on the RSVP bandwidth of member link.

The **iprsvpbandwidthpercent** command is blocked on interfaces on which dynamic update of RSVP bandwidth is not supported. A debug message appears if an RSVP client attempts to configure the **iprsvpbandwidthpercent** command on an unsupported interface.

In Cisco IOS Release 15.1(2)T, the **iprsvpbandwidthpercent** command is supported on Multilevel Precedence and Preemption (MLPP) and Multilink Frame Relay (MFR) interfaces.

## Examples

The following example shows a serial link configured to permit an RSVP reservation of up to 90 percent of interface bandwidth but no more than 1000 kb/s for any given flow on serial interface 0:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface serial 0
Router(config-if)# ip rsvp bandwidth percent 90 1000
```

The following example shows a multilink configured to permit 50 percent of the interface bandwidth as the RSVP bandwidth and 10 percent of the interface bandwidth as the flow bandwidth for any given multilink interface 2:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface multilink 2
Router(config-if)# ip rsvp bandwidth percent 50 percent 10
Router(config-if)#
exit
```

## Related Commands

| Command | Description |
|---|---|
| **fair-queue (WFQ)** | Enables WFQ for an interface. |
| **ip rsvp bandwidth** | Enables RSVP for IP on an interface. |
| **ip rsvp neighbor** | Enables neighbors to request a reservation. |
| **ip rsvp reservation** | Enables a router to behave as though it were receiving and forwarding RSVP RESV messages. |
| **ip rsvp sender** | Enables a router to behave as though it were receiving and forwarding RSVP PATH messages. |

| Command | Description |
|---|---|
| **ip rsvp udp-multicasts** | Instructs the router to generate UDP-encapsulated RSVP multicasts whenever it generates an IP-encapsulated multicast packet. |
| **random-detect (interface)** | Enables WRED or DWRED. |
| **show ip rsvp installed** | Displays RSVP-related installed filters and corresponding bandwidth information. |
| **show ip rsvp interface** | Displays RSVP-related interface information. |
| **show ip rsvp neighbor** | Displays current RSVP neighbors. |
| **show ip rsvp reservation** | Displays RSVP-related receiver information currently in the database. |
| **show ip rsvp sender** | Displays RSVP PATH-related sender information currently in the database. |

# ip rsvp burst policing

To configure a burst factor within the Resource Reservation Protocol (RSVP) token bucket policer on a per-interface basis, use the **iprsvpburstpolicing** command in interface configuration mode. To return to the default value, enter the **no** form of this command.

**ip rsvp burst policing** [ *factor* ]

**no ip rsvp burst policing**

## Syntax Description

| | |
|---|---|
| *factor* | (Optional) Indicates a burst factor value as a percentage of the requested burst of the receiver. |

## Command Default

The default value is 200; the minimum value is 100, and the maximum value is 700.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(3)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

You configure the burst police factor per interface, not per flow. The burst factor controls how strictly or loosely the traffic of the sender is policed with respect to burst.

The burst factor applies to all RSVP flows installed on a specific interface. You can configure each interface independently for burst policing.

## Examples

The following example shows the**iprsvpburstpolicing** command with a burst factor of 200:

```
ip rsvp burst policing 200
```

# ip rsvp data-packet classification none

To turn off (disable) Resource Reservation Protocol (RSVP) data packet classification, use the **iprsvpdata-packetclassificationnone**command in interface configuration mode. To turn on (enable) data-packet classification, use the **no** form of this command.

**ip rsvp data-packet classification none**

**no ip rsvp data-packet classification none**

## Syntax Description

This command has no arguments or keywords.

## Command Default

RSVP data packet classification is disabled.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(2)T | This command was introduced. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(18)SXF2 | This command was integrated into Cisco IOS Release 12.2(18)SXF2. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

Use the **iprsvpdata-packetclassificationnone**command when you do not want RSVP to process every packet. Configuring RSVP so that not every packet is processed eliminates overhead and improves network performance and scalability.

## Examples

This section contains two examples of the **iprsvpdata-packetclassificationnone** command. The first example shows how to turn off (disable) data packet classification:

```
Router# configure terminal
Router(config)# interface atm 6/0
Router(config-if)# ip rsvp data-packet classification none
```

The following example shows how to turn on (enable) data packet classification:

```
Router# configure terminal
Router(config)# interface atm 6/0
Router(config-if)# no ip rsvp data-packet classification none
```

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp interface** | Displays RSVP-related interface information. |

# ip rsvp dsbm candidate

To configure an interface as a Designated Subnetwork Bandwidth Manager (DSBM) candidate, use the **iprsvpdsbmcandidate**command in interface configuration mode. To disable DSBM on an interface, which exempts the interface as a DSBM candidate, use the **no** form of this command.

**ip rsvp dsbm candidate** [ *priority* ]

**no ip rsvp dsbm candidate**

## Syntax Description

| | |
|---|---|
| *priority* | (Optional) A value in the range from 64 to 128. Among contenders for the DSBM, the interface with the highest priority number wins the DSBM election process. |

## Command Default

An interface is not configured as a DSBM contender by default. If you use this command to enable the interface as a DSBM candidate and you do not specify a priority, the default priority of 64 is assumed.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.1(1)T | This command was integrated into Cisco IOS Release 12.1(1)T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

SBM protocol entities, any one of which can manage resources on a segment, can reside in Layer 2 or Layer 3 devices. Many SBM-capable devices may be attached to a shared Layer 2 segment. When more than one SBM exists on a given segment, one of the SBMs is elected to be the DSBM. The elected DSBM is responsible for exercising admission control over requests for resource reservations on a segment, which, in the process, becomes a managed segment. A managed segment includes those interconnected parts of a shared LAN that are not separated by DSBMs. In all circumstances, only one, if any, DSBM exists for each Layer 2 segment.

You can configure an interface to have a DSBM priority in the range from 64 to 128. You can exempt an interface from participation in the DSBM election on a segment but still allow the system to interact with the DSBM if a DSBM is present on the segment. In other words, you can allow a Resource Reservation Protocol

(RSVP)-enabled interface on a router connected to a managed segment to be managed by the DSBM even if you do not configure that interface to participate as a candidate in the DSBM election process. To exempt an interface from DSBM candidacy, do not issue the **iprsvpdsbmcandidate**command on that interface.

RSVP cannot be configured with Versatile Interface Processor (VIP)-distributed Cisco Express Forwarding (dCEF).

## Examples

The following example shows how to configure Ethernet interface 2 as a DSBM candidate with a priority of 100:

```
interface Ethernet2
 ip rsvp dsbm candidate 100
```

## Related Commands

| Command | Description |
|---|---|
| **debug ip rsvp** | Displays information about SBM message processing, the DSBM election process, and standard RSVP enabled message processing information. |
| **debug ip rsvp detail** | Displays detailed information about RSVP and SBM. |
| **debug ip rsvp detail sbm** | Displays detailed information about SBM messages only, and SBM and DSBM state transitions. |
| **ip rsvp dsbm non-resv-send-limit** | Configures the NonResvSendLimit object parameters. |
| **show ip rsvp sbm** | Displays information about an SBM configured for a specific RSVP-enabled interface or for all RSVP-enabled interfaces on the router. |

# ip rsvp dsbm non-resv-send-limit

To configure the NonResvSendLimit object parameters, use the **iprsvpdsbmnon-resv-send-limit**command in interface configuration mode. To use the default NonResvSendLimit object parameters, use the **no** form of this command.

**ip rsvp dsbm non-resv-send-limit** {**rate** *kbps*| **burst** *kilobytes*| **peak** *kbps*| **min-unit** *bytes*| **max-unit** *bytes*}

**no ip rsvp dsbm non-resv-send-limit** {**rate** *kbps*| **burst** *kilobytes*| **peak** *kbps*| **min-unit** *bytes*| **max-unit** *bytes*}

## Syntax Description

| | |
|---|---|
| **rate** *kbps* | The average rate, in kbps, for the Designated Subnetwork Bandwidth Manager (DSBM) candidate. The average rate is a number from 1 to 2147483. |
| **burst** *kilobytes* | The maximum burst size, in kb, for the DSBM candidate. The maximum burst size is a number from 1 to 2147483. |
| **peak** *kbps* | The peak rate, in kBps, for the DSBM candidate. The peak rate is a number from 1 to 2147483. |
| **min-unit** *bytes* | The minimum policed unit, in bytes, for the DSBM candidate. The minimum policed unit is a number from 1 to 2147483647. |
| **max-unit** *bytes* | The maximum packet size, in bytes, for the DSBM candidate. The maximum packet size is a number from 1 to 2147483647. |

## Command Default

The default for the **rate**, **burst**, **peak**, **min-unit**, and **max-unit** keywords is unlimited; all traffic can be sent without a valid Resource Reservation Protocol (RSVP) reservation.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

To configure the per-flow limit on the amount of traffic that can be sent without a valid RSVP reservation, configure the **rate**, **burst**, **peak**, **min-unit**, and **max-unit** values for finite values greater than 0.

To allow all traffic to be sent without a valid RSVP reservation, configure the **rate**, **burst**, **peak**, **min-unit**, and **max-unit** values for unlimited traffic. To configure the parameters for unlimited traffic, you can either omit the command, or enter the **no** form of the command (for example, **noiprsvpdsbmnon-resv-send-limitrate**). Unlimited is the default value.

The absence of the NonResvSendLimit object allows any amount of traffic to be sent without a valid RSVP reservation.

RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

## Examples

The following example configures Ethernet interface 2 as a DSBM candidate with a priority of 100, an average rate of 500 kBps, a maximum burst size of 1000 KB, a peak rate of 500 kBps, and unlimited minimum and maximum packet sizes:

```
interface Ethernet2
 ip rsvp dsbm candidate 100
 ip rsvp dsbm non-resv-send-limit rate 500
 ip rsvp dsbm non-resv-send-limit burst 1000
 ip rsvp dsbm non-resv-send-limit peak 500
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp dsbm candidate** | Configures an interface as a DSBM candidate. |
| **show ip rsvp sbm** | Displays information about an SBM configured for a specific RSVP-enabled interface or for all RSVP-enabled interfaces on the router. |

# ip rsvp flow-assist

To enable Resource Reservation Protocol (RSVP) to integrate with the Cisco Express Forwarding (CEF) path for flow classification, policing, and marking, use the **iprsvpflow-assist** command in interface configuration mode. To disable integration of RSVP with CEF for this purpose, use the **iprsvpdata-packetclassificationnone** command.

**ip rsvp flow-assist**

## Syntax Description

This command has no arguments or keywords.

## Command Default

This command is on by default; RSVP integrates with CEF for classification, policing, and marking of data packets.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.4 | The behavior of this command was modified. See the "Usage Guidelines" section for additional information. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

To police and mark data packets of a reserved flow, RSVP must interact with the underlying packet forwarding mechanism, which is CEF.

In Cisco IOS Release 12.4, the **no** form of the **iprsvpflow-assist** command is no longer supported since you can use the existing **iprsvpdata-packetclassificationnone** command to disable RSVP from integrating with any mechanism for handling data packets.

## Examples

The following example shows how to enable RSVP on ATM interface 2/0/0:

```
interface atm2/0/0
 ip rsvp flow-assist
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp data-packet classification none** | Avoids integrating RSVP with the data plane. |
| **ip rsvp precedence** | Allows you to set the IP Precedence values to be applied to packets that either conform to or exceed the RSVP flowspec. |
| **ip rsvp svc-required** | Enables creation of an SVC to service any new RSVP reservation made on the interface or subinterface. |
| **ip rsvp tos** | Allows you to set the ToS values to be applied to packets that either conform to or exceed the RSVP flowspec. |
| **show ip rsvp interface** | Displays RSVP-related interface information. |

# ip rsvp layer2 overhead

To control the overhead accounting performed by Resource Reservation Protocol (RSVP)/weighted fair queueing (WFQ) when a flow is admitted onto an ATM permanent virtual circuit (PVC), use the**iprsvplayer2overhead** command in interface configuration mode. To disable the overhead accounting, use the **no** form of this command.

**ip rsvp layer2 overhead** [*h c n*]

**default ip rsvp layer2 overhead**

**no ip rsvp layer2 overhead** [*h c n*]

## Syntax Description

| | |
|---|---|
| *h* | (Optional) Layer 2 encapsulation header plus trailer size applied to each Layer 3 packet in bytes. Valid sizes are numbers from 0 to 65535. |
| *c* | (Optional) Layer 2 cell header size applied to each Layer 2 cell in bytes. Valid sizes are numbers from 0 to 65535. |
| *n* | (Optional) Layer 2 payload size in bytes. Valid sizes are numbers from 0 to 65534. |

## Command Default

This command is enabled by default on ATM interfaces that are running RSVP and WFQ. You can also use this command on non-ATM interfaces.

The default version of the command, **defaultiprsvplayer2overhead**, or by omitting the parameters (*h* , *c* , and *n* ) and entering the **iprsvplayer2overhead**commandcauses RSVP to determine the overhead values automatically, based on the interface/PVC encapsulation. (Currently, RSVP recognizes ATM Adaptation Layer 5 (AAL5) subnetwork access protocol (SNAP) and MUX (multiplexer) encapsulations.)

On non-ATM/PVC interfaces, the configured *h* , *c* , and *n* parameters determine the values that RSVP uses for its overhead.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(2)T | This command was introduced. |

## Usage Guidelines

When an IP flow traverses a link, the overhead of Layer 2 encapsulation can increase the amount of bandwidth that the flow requires to exceed the advertised (Layer 3) rate.

In many cases, the additional bandwidth a flow requires because of Layer 2 overhead is negligible and can be transmitted as part of the 25 percent of the link, which is unreservable and kept for routing updates and Layer 2 overhead. This situation typically occurs when the IP flow uses large packet sizes or when the Layer 2 encapsulation allows for frames of variable size (such as in Ethernet and Frame Relay encapsulations).

However, when a flow's packet sizes are small and the underlying Layer 2 encapsulation uses fixed-size frames, the Layer 2 encapsulation overhead can be significant, as is the case when Voice Over IP (VoIP) flows traverse ATM links.

To avoid oversubscribing ATM PVCs, which use AAL5 SNAP or AAL5 MUX encapsulations, RSVP automatically accounts for the Layer 2 overhead when admitting a flow. For each flow, RSVP determines the total amount of bandwidth required, including Layer 2 overhead, and uses this value for admission control with the WFQ bandwidth manager.

**Note** The **iprsvplayer2overhead**command does not affect bandwidth requirements of RSVP flows on ATM switched virtual circuits (SVCs).

## Examples

In the following example, the total amount of bandwidth reserved with WFQ appears:

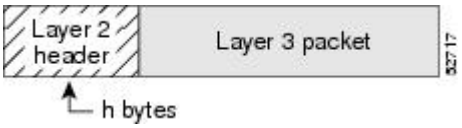
```
Router# show ip rsvp installed detail
RSVP:ATM6/0 has the following installed reservations
RSVP Reservation. Destination is 10.1.1.1, Source is 10.1.1.1,
  Protocol is UDP, Destination port is 1000, Source port is 1000
  Reserved bandwidth:50K bits/sec, Maximum burst:1K bytes, Peak rate:50K bits/sec
  Min Policed Unit:60 bytes, Max Pkt Size:60 bytes
  Resource provider for this flow:
    WFQ on ATM PVC 100/101 on AT6/0: PRIORITY queue 40.  Weight:0, BW 89 kbps
  Conversation supports 1 reservations
  Data given reserved service:0 packets (0M bytes)
  Data given best-effort service:0 packets (0 bytes)
  Reserved traffic classified for 9 seconds
  Long-term average bitrate (bits/sec):0M reserved, 0M best-effort
```

In the preceding example, the flow's advertised Layer 3 rate is 50 kbps. This value is used for admission control with the**iprsvpbandwidth** value. The actual bandwidth required, inclusive of Layer 2 overhead, is 89 kbps. WFQ uses this value for admission control.

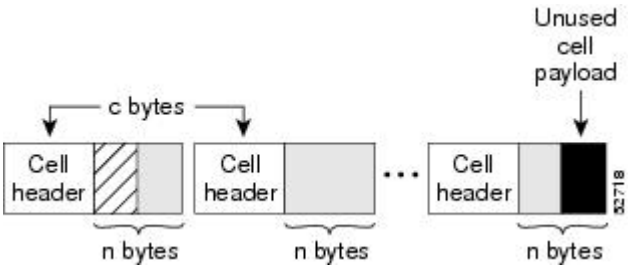
Typically, you should not need to configure or disable the Layer 2 overhead accounting. RSVP uses the advertised Layer 3 flow rate, minimum packet size, and maximum unit size in conjunction with the Layer 2 encapsulation characteristics of the ATM PVC to compute the required bandwidth for admission control. However, you can disable or customize the Layer 2 overhead accounting (for any link type) with the **iprsvplayer2overhead** command. The parameters of this command are based on the following steps that show how a Layer 3 packet is fragmented and encapsulated for Layer 2 transmission.

1 Start with a Layer 3 packet, as shown in Figure 1, which includes an IP header and a payload.

2 Add an encapsulation header or trailer, as shown in Figure 2, of size *h*




3 Segment the resulting packet into fixed-sized cells, as shown in Figure 3, with a cell header of c bytes and a cell payload of n bytes.




4 Transmit the resulting Layer 2 cells.

## Examples

In the following example, Layer 2 overhead accounting is disabled for all reservations on the interface and its PVCs:

```
Router(config-if)# no ip rsvp layer2 overhead
```

In the following example, Layer 2 overhead accounting is configured with ATM AAL5 SNAP encapsulation:

```
Router(config-if)# no ip rsvp layer2 overhead 8 5 48
```

In the following example, Layer 2 overhead accounting is configured with ATM AAL5 MUX encapsulation:

```
Router(config-if)# ip rsvp layer2 overhead 0 5 48
```

In the following example, Layer 2 overhead accounting is configured with Ethernet V2.0 encapsulation (including 8-byte preamble, 6-byte source-active (SA) messages, 6-byte destination-active (DA) messages, 2-byte type, and 4-byte frame check sequence (FCS) trailer):

```
Router(config-if)# ip rsvp layer2 overhead 26 0 1500
```

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp installed** | Displays RSVP-related installed filters and corresponding bandwidth information. |

# ip rsvp listener

To configure a Resource Reservation Protocol (RSVP) router to listen for PATH messages, use the **iprsvplistener** command in global configuration mode. To disable listening, use the **no** form of this command.

**ip rsvp listener** [**vrf** *vrf-name*] *destination-ip* {**udp**| **tcp**| **any**| *number*} {**any**| *destination-port*} {**announce**| **reply**| **reject**}

**no ip rsvp listener** [**vrf** *vrf-name*] *destination-ip* {**udp**| **tcp**| **any**| *number*} {**any**| *destination-port*} {**announce**| **reply**| **reject**}

## Syntax Description

| | |
|---|---|
| **vrf** *vrf-name* | (Optional) Specifies the Virtual routing and forwarding (VRF) instance name. |
| *destination-ip* | IP address of the receiving interface. |
| **udp** | Specifies the UDP for the receiving interface. |
| **tcp** | Specifies the TCP for the receiving interface. |
| **any** | Specifies that any protocol can be used for the receiving interface. |
| *number* | Source port number from 0 to 255; the protocol is IP. |
| **any** | Specifies that any destination port can be used for the receiving interface. |
| *destination-port* | Port number for the receiving interface. Range is from 0 to 65535. |
| **announce** | Receiver announces the arrival of the flow at its destination, but does not send a RESV message in response. |
| **reply** | Sender requests a reply when the flow is received and sends a RESV message when a matching PATH message arrives. |
| **reject** | Router sends a PATHERROR (reject) message in response to an incoming PATH message that matches specified listener parameters. |

## Command Default

This command is disabled by default; therefore, no listeners are configured.

**Command Modes** Global configuration (config)

**Command History**

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.4(6)T | This command was modified. Support for the RSVP application identity (ID) was added. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| 15.0(1)M | This command was modified. The optional **vrf***vrf-name* keyword and argument combination was added. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS Release XE 2.6. |

**Usage Guidelin**

**Note** The syntax of the command depends on your platform and release. The **vrf***vrf-name*keyword and argument combination is not supported on ASR 1000 Series Aggregation Services Routers.

Use the **iprsvplistener** command to allow a router to send a matching RESV message when a PATH message arrives with the desired destination address, port, and protocol. This command copies the application ID and preemption priority value, if present, from the PATH message and includes them in the RESV message.

Use the **iprsvplistenervrf***vrf-name*command to create a listener in the context of the routing domain as defined by VRF. You should be aware of the hierarchy of listener configuration. If you configure a listener for the VRF without specifying the IP address and other fields, then subsequent configuration for a more specific listener configuration with a VRF, an IP address, and a port is not accepted.

This command is similar to the **iprsvpreservation** and**iprsvpreservation-host**commands . However, they do not allow you to specify more than one port or protocol per command; so you may have to enter many commands to proxy for a set of ports and protocols. In contrast, the **iprsvplistener** command allows you to use a wildcard for a set of ports and protocols by using just that one command.

You can use the **debugiprsvpapi**command to look for a matching PATH message, but no RESV message will be sent.

**Examples** In the following example, the sender is requesting that the receiver reply with a RESV message for the flow if the PATH message destination is 192.168.2.1:

```
Router# configure terminal
Router(config)# ip rsvp listener 192.168.2.1 any any reply
```

The following example creates a listener in the VRF routing domain:

```
Router# configure terminal
Router(config)# ip rsvp listener vrf vpn1 10.10.10.10 any any reply
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp reservation** | Enables a router to simulate receiving and forwarding RSVP RESV messages. |
| **ip rsvp reservation-host** | Enables a router to simulate a host generating RSVP RESV messages. |
| **show ip rsvp listeners** | Displays configured RSVP listeners. |

# ip rsvp listener outbound

To configure a Resource Reservation Protocol (RSVP) device to listen for PATH messages sent through a specified interface, use the **ip rsvp listener outbound** command in interface configuration mode. To disable listening for PATH messages, use the **no** form of this command.

**ip rsvp listener outbound** {**reply**| **reject**}

**no ip rsvp listener outbound** {**reply**| **reject**}

## Syntax Description

| | |
|---|---|
| **reply** | For a PATH message exiting from a specified interface, the device does the following:<br>• Installs local PATH state for the message.<br>• Terminates the PATH message and does not forward it downstream.<br>• Generates and sends a RESV (reply) message upstream on behalf of the PATH message with the following:<br>  • The objects in the RESV message are the same as those in the PATH message.<br>  • The policy objects, such as preemption and application IDs, are echoed back.<br>  • Shared explicit style is used. |
| **reject** | For a PATH message exiting from a specified interface, the device does the following:<br>• Terminates the PATH message and does not forward it downstream.<br>• Generates and sends a PATHERROR (reject) message upstream.<br>• Does not install local PATH state and discards the PATH message. |

## Command Default

Listeners are not configured.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SFX5 | This command was introduced. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |
| 15.2(3)T | This command was modified. Support for IPv6 was added. |

## Usage Guidelines

Use the **ip rsvp listener outbound** command to match all PATH messages that are being sent from a specified interface.

When you configure an interface-based receiver proxy to reply, RSVP performs Call Admission Control (CAC) on the outbound (or egress) interface for the flow. If CAC fails, the reservation is not generated. This is the same behavior for the global RSVP receiver proxy command.

The outbound interface that a flow uses is determined when the flow is set up, and the interface-based receiver proxy is consulted. The interface-based receiver proxy is not consulted if there is a change in routing for an existing flow.

If the interface-based receiver proxy receives a RESVERR message with an admission control failure error or a policy reject error, the interface-based receiver proxy generates a PATHERR message with the same error to provide explicit notification to the sender of the reservation failure.

The **ip rsvp listener outbound** configuration will be applicable for both IPv4 and IPv6 PATH messages sent through a specified interface.

## Examples

In the following example, PATH messages sent through Ethernet interface 3/0 are rejected and PATHERROR messages are generated:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# interface Ethernet3/0
Device(config-if)# ip rsvp listener outbound reject
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp listener** | Configures an RSVP device to listen for PATH messages. |
| **ipv6 rsvp reservation** | Enables a networking device to simulate receiving and forwarding IPv6 RSVP RESV messages. |

| Command | Description |
|---|---|
| **ip rsvp reservation-host** | Enables a networking device to simulate a host generating IPv6 RSVP RESV messages. |
| **show ipv6 rsvp listeners** | Displays configured IPv6 RSVP listeners. |

# ip rsvp msg-pacing

**Note** Effective with Cisco IOS Release 12.2(13)T, the **ip rsvp msg-pacing** command is replaced by the **ip rsvp signalling rate-limit** command. See the **ip rsvp signalling rate-limit** command for more information.

To configure the transmission rate for Resource Reservation Protocol (RSVP) messages, use the **ip rsvp msg-pacing** command in global configuration mode. To disable this feature, use the **no** form of this command.

**ip rsvp msg-pacing** [**period** *ms* [**burst** *msgs* [**maxsize** *qsize*]]]

**no rsvp msg-pacing**

## Syntax Description

| | |
|---|---|
| **period** *ms* | (Optional) Length of the interval, in milliseconds, during which a router can send the number of RSVP messages specified in the **burst** keyword. The value can be from 1 to 1000 milliseconds. |
| **burst** *msgs* | (Optional) Maximum number of RSVP messages that a router can send to an output interface during each interval specified in the *period* keyword. The value can be from 1 to 2000. |
| **maxsize** *qsize* | (Optional) Size of per-interface output queues in the sending router. Valid values are from 1 to 2000. |

## Command Default

RSVP messages are not paced. If you enter the command without the optional **burst** keyword, the transmission rate for RSVP messages is limited to 200 messages per second per outgoing interface. The default output queue size, specified in the **maxsize** keyword, is 500.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.0(14)ST | This command was introduced. |
| 12.2(11)S | This command was integrated into Cisco IOS Release 12.2(11)S. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

| Release | Modification |
|---|---|
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(13)T | This command was replaced with the **ip rsvp signalling rate-limit** command. |

## Usage Guidelines

You can use this command to prevent a burst of RSVP traffic engineering signaling messages from overflowing the input queue of a receiving router. Overflowing the input queue with signaling messages results in the router dropping some messages. Dropped messages substantially delay the completion of signaling for LSPs for which messages have been dropped.

If you enter the **ip rsvp msg-pacing** command without the optional **burst** keyword, the transmission rate for RSVP messages is limited to 200 messages per second per outgoing interface. The default output queue size, specified in the **maxsize** keyword, is 500.

## Examples

The following example shows how to configure a router to send a maximum of 150 RSVP traffic engineering signaling messages in 1 second to a neighbor, and the size of the output queue is 750:

```
Router(config)# ip rsvp msg-pacing period 1 burst 150 maxsize 750
```

## Related Commands

| Command | Description |
|---|---|
| **clear ip rsvp msg-pacing** | Clears the RSVP message pacing output from the **show ip rsvp neighbor** command. |

# ip rsvp neighbor

To enable neighbors to request a reservation, use the **iprsvpneighbor**command in interface configuration mode. To disable this function, use the **no** form of this command.

**ip rsvp neighbor** *access-list-number*

**no ip rsvp neighbor** *access-list-number*

## Syntax Description

| | |
|---|---|
| *access-list-number* | Number of a standard or extended IP access list. It can be any number in the range from 1 to 199. |

## Command Default

The router accepts messages from any neighbor.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use this command to allow only specific Resource Reservation Protocol (RSVP) neighbors to make a reservation. If no limits are specified, any neighbor can request a reservation. If an access list is specified, only neighbors meeting the specified access list requirements can make a reservation.

RSVP cannot be configured with Versatile Interface Processor (VIP)-distributed Cisco Express Forwarding (dCEF).

## Examples

The following example shows how to allows neighbors meeting access list 1 requirements to request a reservation:

```
interface ethernet 0
 ip rsvp neighbor 1
```

## Related Commands

| Command | Description |
|---|---|
| **fair-queue (WFQ)** | Enables WFQ for an interface. |
| **ip rsvp bandwidth** | Enables RSVP for IP on an interface. |
| **ip rsvp reservation** | Enables a router to simulate receiving and forwarding RSVP RESV messages. |
| **ip rsvp sender** | Enables a router to simulate receiving and forwarding RSVP PATH messages. |
| **ip rsvp udp-multicasts** | Instructs the router to generate UDP-encapsulated RSVP multicasts whenever it generates an IP-encapsulated multicast packet. |
| **random-detect (interface)** | Enables WRED or DWRED. |
| **show ip rsvp installed** | Displays RSVP-related installed filters and corresponding bandwidth information. |
| **show ip rsvp interface** | Displays RSVP-related interface information. |
| **show ip rsvp neighbor** | Displays current RSVP neighbors. |
| **show ip rsvp reservation** | Displays RSVP-related receiver information currently in the database. |
| **show ip rsvp sender** | Displays RSVP PATH-related sender information currently in the database. |

# ip rsvp policy cops minimal

To lower the load of the Common Open Policy Service (COPS) server and to improve latency times for messages on the governed router, use the **iprsvppolicycopsminimal**command in global configuration mode to restrict the COPS RSVP policy to adjudicate only PATH and RESV messages. To turn off the restriction, use the **no**form of this command.

**ip rsvp policy cops minimal**

**no ip rsvp policy cops minimal**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The default state is OFF, causing all adjudicable RSVP messages to be processed by the configured COPS policy.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

When this command is used, COPS does not attempt to adjudicate PATHERROR and RESVERROR messages. Instead, those messages are all accepted and forwarded.

## Examples

The following example shows how COPS authentication is restricted to PATH and RESV messages:

```
ip rsvp policy cops minimal
```

The following example shows how to remove that restriction:

```
no ip rsvp policy cops minimal
```

# ip rsvp policy cops report-all

To enable a router to report on its success and failure with outsourcing decisions, use the**iprsvppolicycopsreport-all**command in global configuration mode. To return the router to its default, use the **no** form of this command.

**ip rsvp policy cops report-all**

**no ip rsvp policy cops report-all**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The default state of this command is to send reports to the Policy Decision Point (PDP) about configuration decisions only.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

In the default state, the router reports to the PDP when the router has succeeded or failed to implement Resource Reservation Protocol (RSVP) configuration decisions.

A configuration decision contains at least one of the following:

- A RESV ALLOC context (with or without additional contexts)
- A stateless or named decision object

A decision that does not contain at least one of those elements is an *outsourcing decision.*

Some brands of policy server might expect reports about RSVP messaging, which the default state of the Cisco Common Open Policy Service (COPS) for RSVP does not issue. In such cases, use the **iprsvppolicycopsreport-all** command to ensure interoperability between the router and the policy server. Doing so does not adversely affect policy processing on the router.

Unicast FF reservation requests always stimulate a report from the router to the PDP, because those requests contain a RESV ALLOC context (combined with an IN CONTEXT and an OUT CONTEXT).

## Examples

In order to show the Policy Enforcement Point (PEP)-to-PDP reporting process, the **debugcops** command in the following example already is enabled when a new PATH message arrives at the router:

```
Router(config)# ip rsvp policy cops report-all
00:02:48:COPS:** SENDING MESSAGE **
Contents of router's request to PDP:
 COPS HEADER:Version 1, Flags 0, Opcode 1 (REQ), Client-type:1, Length:216
 HANDLE (1/1) object. Length:8.    00 00 02 01
 CONTEXT (2/1) object. Length:8.   R-type:5.     M-type:1
 IN_IF (3/1) object. Length:12.   Address:10.1.2.1.    If_index:4
 OUT_IF (4/1) object. Length:12.   Address:10.33.0.1.    If_index:3 CLIENT SI (9/1) object.
 Length:168.   CSI data:
 [A 27-line Path message omitted here]
00:02:48:COPS:Sent 216 bytes on socket,
00:02:48:COPS:Message event!
00:02:48:COPS:State of TCP is 4
00:02:48:In read function
00:02:48:COPS:Read block of 96 bytes, num=104 (len=104)
00:02:48:COPS:** RECEIVED MESSAGE **
Contents of PDP's decision received by router:
 COPS HEADER:Version 1, Flags 1, Opcode 2 (DEC), Client-type:1, Length:104
 HANDLE (1/1) object. Length:8.    00 00 02 01
 CONTEXT (2/1) object. Length:8.   R-type:1.     M-type:1
 DECISION (6/1) object. Length:8.   COMMAND cmd:1, flags:0
 DECISION (6/3) object. Length:56.   REPLACEMENT
 [A 52-byte replacement object omitted here]
 CONTEXT (2/1) object. Length:8.   R-type:4.     M-type:1
 DECISION (6/1) object. Length:8.   COMMAND cmd:1, flags:0
00:02:48:Notifying client (callback code 2)
00:02:48:COPS:** SENDING MESSAGE **
Contents of router's report to PDP:
 COPS HEADER:Version 1, Flags 1, Opcode 3 (RPT), Client-type:1, Length:24
 HANDLE (1/1) object. Length:8.    00 00 02 01
 REPORT (12/1) object. Length:8.   REPORT type COMMIT (1)
00:02:48:COPS:Sent 24 bytes on socket,
```

# ip rsvp policy cops servers

To specify that Resource Reservation Protocol (RSVP) should use Common Open Policy Service (COPS) policy for remote adjudication, use the **iprsvppolicycopsservers** command in global configuration mode. To turn off the use of COPS for RSVP, use the **no**form of this command.

**ip rsvp policy cops** [ *acl* ] **servers** *server-ip* [ *server-ip* ]

**no ip rsvp policy cops** [ *acl* ] **servers**

## Syntax Description

| | |
|---|---|
| *acl* | (Optional) Specifies the access control list (ACL) whose sessions will be governed by the COPS policy. |
| *server-ip* | (Optional) Specifies the IP addresses of the servers governing the COPS policy. As many as eight servers can be specified, with the first being treated as the primary server. |

## Command Default

If no ACL is specified, the default behavior is for all reservations to be governed by the specified policy servers.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

If more than one server is specified, the first server is treated by RSVP as the primary serer, and functions as such for *all* ACLs specified.

All servers in the list must have the same policy configuration.

If the connection of the router to the server breaks, the router tries to reconnect to that same server. If the reconnection attempt fails, the router then obeys the following algorithm:

If the connection to the Policy Decision Point (PDP) is closed (either because the PDP closed the connection, a TCP/IP error occurred, or the keepalives failed), the Policy Enforcement Point (PEP) issues a CLIENT-CLOSE

message and then attempts to reconnect to the same PDP. If the PEP receives a CLIENT-CLOSE message containing a PDP redirect address, the PEP attempts to connect to the redirected PDP.

Note the following points:

- If either attempt fails, the PEP attempts to connect to the PDPs previously specified in the **iprsvppolicycopsservers** configuration command, obeying the sequence of servers given in that command, always starting with the first server in that list.
- If the PEP reaches the end of the list of servers without connecting, it waits a certain time (called the *reconnect delay* ) before trying again to connect to the first server in the list. This reconnect delay is initially 30 seconds, and doubles each time the PEP reaches the end of the list without having connected, until the reconnect delay becomes its maximum of 30 minutes. As soon as a connection is made, the delay is reset to 30 seconds.

The **no** form of this command need not contain any server IP addresses, but it must contain all the previously specified access lists (see the last example in the following section).

## Examples

This first example applies the COPS policy residing on server 172.27.224.117 to all reservations passing through router-9. It also identifies the backup COPS server for this router as the one at address 172.27.229.130:

```
Router(config)# ip rsvp policy cops servers 172.27.224.117 172.27.229.130
```

The next example applies the COPS policy residing on server 172.27.224.117 to reservations passing through router-9 only if they match access lists 40 and 160. Other reservations passing through that router will not be governed by this server. The command statement also identifies the backup COPS server for that router to be the one at address 172.27.229.130:

```
Router(config)# ip rsvp policy cops 40 160 servers 172.27.224.117 172.27.229.130
```

The following example turns off COPS for the previously specified access lists 40 and 160 (you cannot turn off just one of the previously specified lists):

```
Router(config)# no ip rsvp policy cops 40 160 servers
```

# ip rsvp policy cops timeout

To configure the amount of time the Policy Enforcement Point (PEP) router will retain policy information after losing connection with the Common Open Policy Service (COPS) server, use the **iprsvppolicycopstimeout** command in global configuration mode. To restore the router to the default value (5 minutes), use the **no** form of this command.

**ip rsvp policy cops timeout** *policy-timeout*

**no ip rsvp policy cops timeout**

## Syntax Description

| | |
|---|---|
| *policy-timeout* | Duration of timeout, from 1 to 10,000 seconds. |

## Command Default

Timeout default is 300 seconds (5 minutes).

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Examples

The following example shows how to configure the router to time out all policy information relating to a lost server in 10 minutes:

```
ip rsvp policy cops timeout 600
```

The following example shows how to reset the timeout to the default value:

```
no ip rsvp policy cops timeout
```

# ip rsvp policy default-reject

To reject all messages that do not match the policy access control lists (ACLs), use the **iprsvppolicydefault-reject** command in global configuration mode. To restore the default behavior, which passes along all messages that do not match the ACLs, use the **no** form of this command.

**ip rsvp policy default-reject**

**no ip rsvp policy default-reject**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Without this command, the default behavior of Resource Reservation Protocol (RSVP) is to accept, install, or forward all unmatched RSVP messages. Once this command is invoked, all unmatched RSVP messages are rejected.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

If COPS is configured without an ACL, or if any policy ACL is configured to use the **permitipanyany** command, the behavior of that ACL will take precedence, and no session will go unmatched.

**Note** This command makes one exception to its blocking of unmatched messages. It forwards RESVERROR and PATHERROR messages that were generated by its own rejection of RESV and PATH messages. That is done to ensure that the default-reject operation does not remain totally hidden from network managers.

**Caution** Be extremely careful with this command. It will shut down all RSVP processing on the router if access lists are too narrow or if no Common Open Policy Service (COPS) server has been specified. (Use the **iprsvppolicycopsservers** command to specify a COPS server.)

## Examples

The following example shows how to configure RSVP to reject all unmatched reservations:

```
ip rsvp policy default-reject
```

The following example shows how to configure RSVP to accept all unmatched reservations:

```
no ip rsvp policy default-reject
```

# ip rsvp policy identity

To define Resource Reservation Protocol (RSVP) application identities (IDs), use the **iprsvppolicyidentity** command in global configuration mode. To delete RSVP application IDs, use the **no** form of this command.

**ip rsvp policy identity** *alias* **policy-locator** *locator*

**no ip rsvp policy identity** *alias* [**policy-locator** *locator*]

## Syntax Description

| | |
|---|---|
| *alias* | String used within the router to reference the identity in RSVP configuration commands and **show** displays. The string can have as many as 64 printable characters (in the range 0x20 to 0x7E).<br>**Note** If you use the " " or ? characters as part of the alias or locator string itself, you must type the CTRL-V key sequence before entering the embedded " "or ? characters. The alias is never transmitted to other routers. |
| **policy-locator** *locator* | Specifies string that is signaled in RSVP messages and contains application IDs in X.500 Distinguished Name (DN) format. (See the "**UsageGuidelines**" section for detailed information.) |

## Command Default

This command is disabled by default; therefore, no RSVP application identities are defined.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

You can use RSVP identities as criteria for matching RSVP PATH and RESV messages to local policies. Identities can also be used to configure static senders and receivers. When you use an RSVP identity as the match criterion for a local policy, RSVP treats the *policylocato*r string as a type of pattern-matching string known as a regular expression. Regular expressions allow you to configure a single identity for use with a local policy that can match multiple X.500 DNs. Regular expressions, by default, are not exact matches unless you add appropriate control characters to the expression to force it to be an exact match.

In Cisco IOS and Cisco IOX XE software, the *locator* is the primary piece of information that the router uses to find the correct policy to apply to RSVP messages that contain application IDs. This string assumes the format of an X.500 DN and includes the following attributes as recommended in RFC 2872:

- APP = Application identifier, a required attribute.
- VER = Version number of the application, a required attribute.
- SAPP = Subapplication identifier, an optional attribute. An arbitrary number of subapplication elements can be included.
- GUID = Global unique identifier, an optional attribute.

Here are some examples:

- APP = CCM, VER = 1.1, SAPP = Voice
- GUID = http://www.cisco.com/apps, APP = VideoConference, VER = 1.2.3

You can create a maximum of 100 identities on a router. If you attempt to create more, the command fails and the following error message is generated: “RSVP error: maximum number of identities already created”.

When you use the **iprsvppolicyidentity** command, be aware of the following behavior:

- If you specify *alias* or *locator* strings that are empty or invalid, the command is rejected and an error message is generated.
- Cisco IOS software automatically adds quotes to the *alias* or *locator* strings in the configuration if quotes are required.
- If you specify the optional **policy-locator** keyword in the **no** form of this command, the command is rejected if the *locator* does not match the configured *locator* string for the *alias* being deleted.
- If you specify an *alias* that is missing, empty, or contains invalid characters, the command is rejected and an error message is generated.
- RSVP does not check the *locator* string for a valid X.500 DN; therefore, the *locator* string can be anything that you want.

### Command Restrictions

- User identities are not supported in Cisco IOS Release 12.4(6)T.
- You cannot configure a single router with more than 100 identities at a time.

## Examples

## Examples

The following example shows an application ID for RSVP messages containing a locator string whose contents are the exact string “APP=Voice”:

```
Router# configure terminal
Router(config)# ip rsvp policy identity "rsvp-voice" policy-locator "^APP=Voice$"
Router(config-rsvp-id)# end
```

## Examples

The following example shows an application ID that is a partial match for RSVP messages containing a locator string with the substring “APP=Voice” anywhere in the signaled application ID:

```
Router# configure terminal
Router(config)# ip rsvp policy identity "rsvp-voice" policy-locator ".*APP=Voice.*"
Router(config-rsvp-id)# end
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp policy local** | Creates a local procedure that determines the use of RSVP resources in a network. |
| **show ip rsvp policy identity** | Displays selected RSVP identities in a router configuration. |
| **show ip rsvp policy local** | Displays selected local policies that have been configured. |

# ip rsvp policy local

To determine how to perform authorization on Resource Reservation Protocol (RSVP) requests and enter local policy configuration mode, use the **iprsvppolicylocal**command in global configuration or interface configuration mode. To disable this function, use the **no** form of this command.

**ip rsvp policy local** {**acl** *acl1* [ *acl2...acl8* ]| **dscp-ip** *value1* [ *value2....value8* ]| **default**| **identity** *alias1* [*alias2 ... alias4*]| **origin-as** *as1* [ *as2...as8* ]}

**no ip rsvp policy local** {**acl** *acl1* [ *acl2...acl8* ]| **dscp-ip** *value1* [ *value2...value8* ]| **default**| **identity** *alias1* [ *alias2...alias4* ]| **origin-as** *as1* [ *as2...as8* ]}

## Syntax Description

| | |
|---|---|
| **acl** *acl1* [*acl2...acl8* | Specifies an access control list (ACL). Values for each ACL are 1 to 199.<br>**Note** You must associate at least one ACL with an ACL-based policy. However, you can associate as many as eight ACLs with an ACL-based policy. |
| **dscp-ip** *value1* [*value2...value8* | Specifies the differentiated services code point (DSCP) for matching aggregate reservations. Values can be the following:<br>• 0 to 63--Numerical DSCP values. The default value is 0.<br>• af11 to af43--Assured forwarding (AF) DSCP values.<br>• cs1 to cs7--Type of service (ToS) precedence values.<br>• default--Default DSCP value.<br>• ef--Expedited forwarding (EF) DSCP values.<br>**Note** You must associate at least one DSCP with a DSCP-based policy. However, you can associate as many as eight DSCP values with a DSCP-based policy. |
| **default** | Specifies a default when an RSVP message does not match any ACL, DSCP, identity, or autonomous system. |
| **identity** *alias1* [*alias2...alias4* | Specifies an application ID alias for an application ID previously configured using the **iprsvppolicyidentity** command.<br>**Note** You must associate at least one alias with an application-ID-based policy. However, you can associate as many as four. |

| | |
|---|---|
| **origin-as** *as1* [*as2...as8* | Specifies an autonomous system. Values for each autonomous system are 1 to 65535.<br>**Note** You must associate at least one autonomous system with an autonomous-system-based policy. However, you can associate as many as eight. |

**Command Default**

This command is disabled by default; therefore, no local policies are configured.

**Command Modes**

Global configuration (config) Interface configuration (config-if)

**Command History**

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.0(29)S | This command was modified. The**origin-as***as* keyword and argument combination and new submode commands were added. |
| 12.0(30)S | This command was modified. You can no longer use 0 as the protocol when you configure an ACL. |
| 12.4(4)T | This command was integrated into Cisco IOS Release 12.4(4)T. |
| 12.4(6)T | The command was modified. The following changes were made:<br>• Interface configuration mode was added to support per-interface local policies.<br>• **The identity** *alias* keyword and argument combination was added.<br>• The **maximum**submode command was changed to support RESV messages. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SRC | This command was modified. The **dscp-ip***value*keyword and argument combination was added. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

**Usage Guidelines**

Use the **iprsvppolicylocal**command to determine how to perform authorization on RSVP requests.

**Note** When you enter the **origin-as***as* keyword and argument combination, an RSVP warning message appears stating that the autonomous-system-based policy will be ineffective until BGP is running.

You can use all types of match criteria with non-Traffic-Engineering (TE) reservations. You can use all types of match criteria except application ID with TE reservations because TE PATH and RESV messages sent by Cisco routers do not contain application IDs.

There are five types of local policies--one default local policy, one or more ACL-based policies, one or more autonomous-system-based policies, one or more application-ID-based policies, and one or more DSCP-based policies. The default policy is used when an RSVP message does not match any ACL-, autonomous-system-, application-ID-, or DSCP-based policies.

You can configure a mixture of local policy types including ACL, autonomous system, application ID, DSCP, or default on the same interface or globally. Policies have the following priority (from highest to lowest):

- Nondefault interface policies
- Default interface policy
- Nondefault global policies
- Global default policy

**Note** If you configure an ACL to use with a TE tunnel, do not use 0 as the protocol because RSVP cannot accept any messages since they do not match the ACL.

**Policy-Match Criteria**

**Note** You cannot specify a policy-match criteria more than once using the **iprsvppolicylocal** command.

An ACL-based policy must have at least one ACL associated with it, but it can optionally have up to eight ACLs. The ACLs can be standard or extended IP ACLs. They are matched against source/destination addresses/ports based on RSVP objects inside RSVP signaling messages as described below.

- ACL source address--Matched against the source address in the SENDER_TEMPLATE object in RSVP messages. If this object is not present, the source address in the IP header is used.
- ACL destination address--Matched against the destination address in the SESSION object in RSVP messages. If this object is not present, the destination address in the IP header is used.
- ACL source port--Matched against the source port in the SENDER_TEMPLATE object in RSVP messages. If this object is not present, the source port of 0 is used.
- ACL destination port--Matched against the destination port in the SESSION object in RSVP messages. If this object is not present, the destination port of 0 is used.
- ACL IP protocol--Matched against the IP protocol in the SESSION object in RSVP messages. If this object is not present, the IP protocol of 0 is used. If the IP protocol is for a TE session, then the ACL IP protocol should be UDP.
- ACL differentiated services code point (DSCP) values--Matched against the DSCP value in the IP header of the RSVP message.

**Note** The same policy-match criteria apply when you create ACLs for the **debugiprsvpfilter**command except that the command does not use DSCP and the protocol is ignored for TE sessions.

An autonomous-system-based policy must have at least one autonomous system associated with it, but it can optionally have up to eight autonomous systems. They are matched against the incoming interface/source IP address contained in RSVP objects inside RSVP signaling messages, not on the IP headers of the RSVP messages.

An application-ID-based policy must have at least one application ID associated with it, but it can optionally have up to four application IDs. They are matched against the incoming interface/source IP address contained in RSVP objects inside RSVP signaling messages, not on the IP headers of the RSVP messages.

A DSCP-based policy must have at least one DSCP associated with it, but it can optionally have up to four DSCPs. RSVP extracts the DSCP from the aggregate message SESSION object and applies the local policy that matches the DSCP criteria.

**Command Restrictions**

- You cannot configure more than 300 local policies per router. This limit is independent of policy location (global or per interface) or match criteria such as application IDs, ACLs, or autonomous systems.
- You cannot configure a single local policy with more than four RSVP identities.

**CLI Submodes**

Once you type the **iprsvppolicylocal** command, you enter the local policy CLI submode where you define the properties of the local policy that you are creating.

**Note** The local policy that you create automatically rejects all RSVP messages unless you enter a submode command that instructs RSVP on the types of messages to accept or forward.

The submode commands are as follows:

- **accept** --Accepts, but does not forward RSVP messages.

**accept** {**all** | **path** | **path-error** | **resv** | **resv-error**}

- - **all** --Accepts all incoming RSVP messages.
  - **path** --Accepts incoming PATH messages that meet the match criteria for this policy, which includes ACL(s), autonomous system(s), application ID(s), or default(s). If you omit this command, incoming PATH messages that meet the policy-match criteria are rejected and a PATHERROR message is sent in reply. However, the PATHERROR reply is also subject to local policy.
  - **path-error** --Accepts incoming PATHERROR messages that meet the match criteria for this policy. If you omit this command, incoming, including locally-generated, PATHERROR messages that meet the policy-match criteria are rejected.
  - **resv** --Accepts incoming RESV messages that meet the match criteria for this policy and performs any required admission control. If you omit this command, incoming RESV messages that meet the policy-match criteria are rejected and a RESVERROR message is sent in reply. However, the RESVERROR reply is also subject to local policy.

The default bandwidth for a policy is unlimited. Therefore, if the policy has no configured bandwidth, a RESV message is always accepted by the local policy because any bandwidth request is less than or equal to unlimited. However, the RESV message may subsequently fail admission control if there is insufficient bandwidth in the RSVP pool on the input interface to which the RESV message applies. (See the **iprsvpbandwidth** command for more information.) If the bandwidth requested by the RESV messages is too large, a RESVERROR message that is also subject to local policy is transmitted to the RESV sender.

- • **resv-error** --Accepts incoming RESVERROR messages that meet the policy-match criteria for this policy. If you omit this command, the incoming, including locally-generated, RESVERROR messages that meet the policy-match criteria are rejected.

- **default** --Sets a command to its defaults.
- **exit** --Exits local policy configuration mode.
- **fast-reroute** --Allows TE LSPs that request Fast Reroute service. The default value is accept.
- **forward** --Accepts and forwards RSVP messages.

**forward** {**all**|**path** | **path-error** | **resv** | **resv-error**}

- • **all** --Accepts and forwards all RSVP messages.
  - **path** --Accepts and forwards PATH messages that meet the match criteria for this policy. If you omit this command, PATH messages that meet the policy-match criteria are not forwarded to the next (downstream) hop.
  - **path-error** --Accepts and forwards PATHERROR messages that meet the match criteria for this policy. If you omit this command, the PATHERROR messages that meet the match criteria are not forwarded to the previous (upstream) hop. You may want to reject outbound PATHERROR messages if you are receiving PATH messages from an untrusted node because someone could be trying to port-scan for RSVP. If you reply with a PATHERROR message, the untrusted node knows that you support RSVP and your IP address. Such information could be used to attempt RSVP-based attacks.
  - **resv** --Accepts and forwards RESV messages that meet the match criteria for this policy. If you omit this command, RESV messages that meet the match criteria are not forwarded to the previous (upstream) hop.
  - **resv-error** --Accepts and forwards RESVERROR messages that meet the match criteria for this policy. If you omit this command, the RESVERROR messages that meet the match criteria are not forwarded to the next (downstream) hop. You may want to reject outbound RESVERROR messages if you are receiving RESV messages from an untrusted node because someone could be trying to port-scan for RSVP. If you reply with a RESVERROR message, then the untrusted node knows that you support RSVP and your IP address. Such information could be used to attempt RSVP-based attacks.

- **local-override** --Overrides any other policy sources by enforcing this local policy. Finalizes any decisions by this policy. If local-override is omitted, RSVP holds onto the local policy decision to see if another local or remote policy exists that will make a decision on the RSVP message, and only if there is no other policy decision will the local policy decision be enforced.
- **maximum** [**bandwidth**[**group***x*] [**single***y*] | **senders***n*]--Sets the limits for resources.
  - **bandwidth**[**group***x*] [**single***y*]--Indicates bandwidth limits for RSVP reservations. The **group** keyword specifies the amount of bandwidth that can be requested by all reservations covered by

this policy. The **single** keyword specifies the maximum bandwidth that can be requested by any specific RSVP reservation covered by this policy. The x and y values are in kilobits per second and can range from 1 to 10,000,000 (similar in concept to the existing interface mode **iprsvpbandwidth**command). Absence of a bandwidth command implies that there is no policy limit on bandwidth requests.

Previously, the **maximumbandwidth**command applied only to PATH messages. However, as part of the application ID enhancement, this command now applies only to RESV messages. This change has the following benefits: Allows the local policy bandwidth limit to be used by RSVP's admission control process for both shared and nonshared reservations. Previous releases that performed group bandwidth checks on PATH messages could not account for bandwidth sharing, and, as a result, you had to account for sharing by creating a larger maximum group bandwidth for the policy. Allows a local policy to trigger preemption during the admission control function if there is insufficient policy bandwidth to meet the needs of an incoming RESV message.

- • **senders** *n* -- Limits the number of RSVP senders affected by this policy that can be active at the same time on this router. The value for *n* ranges from 1 to 50,000 with a default of 1000.

**Note** If you do not configure the **iprsvppolicypreempt** command, the **maximum**command may be rejected, resulting in th "**RSVPerror:insufficientpreemptablebandwidth**"**iftherearereservationsadmittedagainstthepolicy,andyoutrytored**

- **no** --Negates a command or sets its defaults.
- **preempt-priority** [**traffic-eng***x*] *setup-priority* [*hold-priority*] --Specifies the RSVP QoS priorities to be inserted into PATH and RESV messages if they were not signaled from an upstream or downstream neighbor or local client application, and the maximum setup or hold priority that RSVP QoS or MPLS/TE sessions can signal. A PATHERROR, RESVERROR, or local application error is returned if these limits are exceeded.

The *x*value indicates the upper limit of the priority for TE reservations. The range of *x*values is 0 to 7 in which the smaller the number, the higher the reservation's priority. For non-TE reservations, the range of *x*values is 0 to 65535 in which the higher the number, the higher the reservation's priority.

The *setup-priority* argument indicates the priority of a reservation when it is initially installed. The optional *hold-priority*argument indicates the priority of a reservation after it has been installed; if omitted, it defaults to the *setup-priority*. Values for the *setup-priority* and *hold-priority* arguments range from 0 to 7 where 0 is considered the highest priority.

If the incoming message has a preemption priority that requests a priority higher than the policy allows, the message is rejected. Use the **tunnelmplstraffic-engpriority** command to configure preemption priority for TE tunnels.

A single policy can contain a **preempt-prioritytraffic-eng** and a **preempt-priority** command, which may be useful if the policy is bound to an ACL that identifies a subnet containing a mix of TE and non-TE endpoints or midpoints.

**Note** If you exit local policy configuration mode without entering any submode commands, the policy that you have created rejects all RSVP messages.

### Per-Interface Local Policies

All the local policy submode commands are also supported on a per-interface basis. You simply enter Cisco IOS interface configuration mode for the selected interface and type in any number and mix of the submode commands.

Per-interface local policies take precedence over global local policies. However, if there is a default local policy configured for an interface, the router does not try to match any RSVP messages arriving on that interface to any of the global local policies. Policies have the following priority (from highest to lowest):

- Nondefault interface policies
- Default interface policy
- Nondefault global policies
- Global default policy

There are some important points to note about per-interface local policies:

- Per-interface local policies do not take the place of the **iprsvpbandwidth** command. The **iprsvpbandwidth** command indicates if RSVP is enabled on an interface as well as the size of the RSVP bandwidth pool. The **iprsvpbandwidth** pool is used by the admission control function of RSVP; per-interface policies are used by the policy control function of RSVP. Policy control is the third phase of RSVP message processing, which consists of validation, authentication, policy control (authorization), and admission control.
- The sum of the group bandwidth of all the local policies assigned to an interface can be greater than the maximum total bandwidth configured in the **iprsvpbandwidth** command. However, the **iprsvpbandwidth** command makes the final decision as to whether there is sufficient bandwidth to admit the reservation.

## Examples

## Examples

In the following example, any RSVP nodes in the 192.168.101.0 subnet can initiate or respond to reservation requests, but all other nodes can respond to reservation requests only. This means that any 192.168.101.x node can send and receive PATH, PATHERROR, RESV, or RESVERROR messages. All other nodes can send only RESV or RESVERROR messages, and all reservations for autonomous system 1 are rejected.

```
Router# configure terminal
Router(config)# access-list 104 permit ip 192.168.101.0 0.0.0.255 any
Router(config)# ip rsvp policy local acl 104
Router(config-rsvp-policy-local)# forward all
Router(config-rsvp-policy-local)# exit
Router(config)# ip rsvp policy local default
Router(config-rsvp-policy-local)# forward resv
Router(config-rsvp-policy-local)# forward resverror
Router(config-rsvp-policy-local)# exit
Router(config)# ip rsvp policy local origin-as 1
Router(config-rsvp-policy-local)# end
```

## Examples

RSVP matches incoming RSVP messages with IDs to configured IDs and policies. The following example configures a global RSVP local policy that limits voice calls to 200 kbps for the whole router regardless of which interface the RSVP signaling occurs on:

```
Router# configure terminal
Router(config)# ip rsvp policy local identity rsvp-voice policy-locator "GUID=www.cisco.com,
```

```
 APP=Voice"
Router(config)# ip rsvp policy local identity rsvp-voice
Router(config-rsvp-local-policy)# forward all
Router(config-rsvp-local-policy)# maximum bandwidth group 200
Router(config-rsvp-local-policy)# end
```

## Examples

The following example configures a local policy that limits all RSVP voice calls on serial interface 2/0/0 to a total of 200 kbps:

```
Router# configure terminal
Router(config)# ip rsvp policy local identity rsvp-voice policy-locator APP=Voice
Router(config)# interface serial2/0/0
Router(config-if)# ip rsvp policy local identity rsvp-voice
Router(config-rsvp-local-policy)# forward all
Router(config-rsvp-local-policy)# maximum bandwidth group 200
Router(config-rsvp-local-policy)# exit
Router(config-if)# ip rsvp policy local default
Router(config-rsvp-local-policy)# forward all
Router(config-rsvp-local-policy)# maximum bandwidth group 50
Router(config-rsvp-local-policy)# end
```

## Examples

The following example configures a local policy to match RSVP aggregation reservations with an RSVP session object DSCP value of 46 and sets the preempt-priority with a setup and hold priority equal to 5.

```
Router# configure terminal
Router(config)# ip rsvp policy local dscp-ip 46
Router(config-rsvp-local-policy)# forward all
Router(config-rsvp-local-policy)# preempt-priority 5 5
Router(config-rsvp-local-policy)# end
```

## Related Commands

| Command | Description |
|---|---|
| **debug ip rsvp filter** | Displays debug messages for RSVP debug message filter. |
| **ip rsvp policy preempt** | Enables RSVP to redistribute bandwidth from lower-priority reservations to new, higher-priority reservations. |
| **show ip rsvp policy** | Displays the configured local policies. |
| show ip rsvp policy cops | Displays the policy server addresses, ACL IDs, and current state of the router's TCP connections to COPS servers. |
| **show ip rsvp policy local** | Displays selected local policies that have been configured. |
| **tunnel mpls traffic-eng priority** | Configures the setup and reservation priority for an MPLS traffic engineering tunnel. |

# ip rsvp policy preempt

To enable Resource Reservation Protocol (RSVP) to take bandwidth from lower-priority reservations and give it to new, higher-priority reservations, use the **iprsvppolicypreempt**command in global configuration mode. To disable this function, use the **no** form of this command.

**ip rsvp policy preempt**

**no ip rsvp policy preempt**

## Syntax Description

This command has no arguments or keywords.

## Command Default

RSVP does not reassign bandwidth from lower-priority reservations to higher-priority reservations.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |

## Usage Guidelines

Use the **iprsvppolicypreempt** command to enable or disable the preemption parameter for all configured local and remote policies without setting the preemption parameter for each policy individually. This command allows you to give preferential quality of service (QoS) treatment to one group of RSVP hosts or applications over another.

## Examples

The following example shows how to enable preemption:

```
Router(config)# ip rsvp policy preempt
```

The following example shows how to disable preemption:

```
Router(config)# no ip rsvp policy preempt
```

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp policy** | Displays the configured local policies. |

# ip rsvp policy vrf

To configure a Resource Reservation Protocol (RSVP) policy for a virtual routing and forwarding (VRF) instance, use the **iprsvppolicyvrf** command in global configuration mode. To remove a VRF-specific policy, use the**no** form of this command.

**ip rsvp policy vrf** *vrf-name* {**identity** *alias* **policy-locator** *regular-expression*| **local** {**acl acl1 [acl2...acl8]**| **default**| **identity** *alias1* [ *alias2...alias4* ]| **origin-as** *as1* [ *as2...as8* ]}}

**no ip rsvp policy vrf** *vrf-name* {**identity** *alias* **policy-locator** *regular-expression*| **local** {**acl acl1 [acl2...acl8]**| **default**| **identity** *alias1* [ *alias2...alias4* ]| **origin-as** *as1* [ *as2...as8* ]}}

## Syntax Description

| | |
|---|---|
| *vrf-name* | Name of a specified VRF. |
| **identity** | Unique information that is conveyed in the POLICY-DATA object for RSVP messages. |
| *alias* | A string used within the router to reference the identity in RSVP configuration commands and show displays. The string can have as many as 64 printable characters (in the range 0x20 to 0x7E).<br>**Note** If you use the " " or ? characters as part of the alias or locator string itself, you must type the CTRL/V key sequence before entering the embedded " " or ? characters. The alias is never transmitted to other routers. |
| **policy-locator** | A string that is signaled in RSVP messages and contains application IDs in X.500 Distinguished Name (DN) format. |
| *regular-expression* | A type of pattern-matching string that allows you to configure a single identity for use with a local policy that can match multiple X.500 DNs. |
| **local** | A local policy. |
| **acl** | Access control list (ACL) for the local policy. |
| *acl1 acl2...acl8* | An ACL. Values for each ACL are 1 to 199.<br>**Note** You must associate at least one ACL with an ACL-based policy. However, you can associate as many as eight. |
| **default** | The policy used when an RSVP message does not match any ACL, identity, or autonomous system. |

| | |
|---|---|
| **identity** | An application ID. |
| *alias1* [*alias2...alias4*] | An application ID alias for an application ID previously configured using the **iprsvppolicyidentity** command.<br>**Note** You must associate at least one alias with an application-ID-based policy. However, you can associate as many as four. |
| origin-as | An autonomous system (AS). |
| *as1* [*as2...as8*] | An AS. Values for each autonomous system are 1 to 65535.<br>**Note** You must associate at least one autonomous system with an autonomous-system-based policy. However, you can associate as many as eight. |

## Command Default

No policies for VRFs are configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced. |

## Usage Guidelines

If you enter a VRF that does not exist, the following error message appears:

```
RSVP error: VRF: myvrf doesn't exist.First create this VRF.
```

To delete the error message, create the VRF called myvrf and issue the command again.

If you configure some VRF-specific policies on a router and the VRF has been removed from the router, then all the policies configured for that VRF are also removed from the configurations.

## Examples

The following example shows how to configure a local default policy for the VRF called myvrf after it has been created:

```
Router(config)# ip rsvp policy vrf myvrf local default
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp policy identity** | Defines RSVP application IDs. |

| Command | Description |
|---|---|
| **ip rsvp policy local** | Defines an RSVP local policy. |

# ip rsvp pq-profile

To specify the criteria for Resource Reservation Protocol (RSVP) to use to determine which flows to direct into the priority queue (PQ) within weighted fair queueing (WFQ), use the **iprsvppq-profile** command in global configuration mode. To disable the specified criteria, use the **no** form of this command.

**ip rsvp pq-profile** [*voice-like*| *r'* [*b'* [*p-to-r'*| *ignore-peak-value*]]]

**no ip rsvp pq-profile**

## Syntax Description

| | |
|---|---|
| *voice-like* | (Optional) Indicates pq-profile parameters sufficient for most voice flows. The default values for r', b', and p-to-r' are used. These values should cause all voice flows generated from Cisco IOS applications and most voice flows from other RSVP applications, such as Microsoft NetMeeting, to be directed into the PQ. |
| *r'* | (Optional) Indicates maximum rate of a flow in bytes per second. Valid range is from 1 to 1048576 bytes per second. |
| *b'* | (Optional) Indicates maximum burst of a flow in bytes. Valid range is from 1 to 8192 bytes. |
| *p-to-r'* | (Optional) Indicates maximum ratio of peak rate to average rate as a percentage. Valid range is from 100 to 4000 percent. |
| *ignore-peak-value* | (Optional) Indicates that the peak rate to average rate ratio of the flow is not evaluated when RSVP identifies flows. |

## Command Default

The default value for r' is 12288 bytes per second.

The default value for b' is 592 bytes.

The default value for p-to-r' is 110 percent.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.1(3)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

| Release | Modification |
|---|---|
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use this command to define the profile of RSVP flows to be placed in the PQ within the WFQ system. You can have only one profile in effect at a time. Changes to this configuration affect only new flows, not existing flows.

This command applies only on interfaces that are running RSVP and WFQ.

RSVP recognizes voice flows based upon the r, b, and p values within the flowspec of a receiver. A reserved flow is granted to the PQ as long as the flowspec parameters of a receiver meet the following default criteria:

(r <= r') AND (b <= b') AND (p/r <= p-to-r')

## Examples

The following example shows how to put voice-like flows (with the default criteria for voice) into the PQ:

```
Router(config)# ip rsvp pq-profile
Router(config)# ip rsvp pq-profile voice-like
Router(config)# ip rsvp pq-profile 12288 592 110
Router(config)# default ip rsvp pq-profile
Router# show running-config | include pq-profile
```

The following example shows how to put all flows matching the voice criteria into the PQ:

```
Router(config)# ip rsvp pq-profile 10240 512 100
Router# show running-config | include pq-profile
ip rsvp pq-profile 10240 512 100
```

The following example shows how to define that no flows are put into the PQ:

```
Router(config)# no ip rsvp pq-profile
Router# show running-config | include pq-profile
no ip rsvp pq-profile
```

The following example shows how to put flows with the criteria given for r' and b' and the default value for p-to-r' into the PQ:

```
Router(config)# ip rsvp pq-profile 9000 300
Router# show running-config | include pq-profile
ip rsvp pq-profile 9000 300 110
```

The following example shows how to put flows with the criteria given for r' and b' and ignoring the peak value of the flow into the PQ:

```
Router(config)# ip rsvp pq-profile 9000 300 ignore-peak-value
Router# show running-config | include pq-profile
ip rsvp pq-profile 9000 300 ignore-peak-value
```

The following example shows how to put Microsoft NetMeeting voice flows with G.711 or adaptive differential pulse code modulation (ADPCM) codecs into the PQ:

```
Router(config)# ip rsvp pq-profile 10200 1200
```

# ip rsvp precedence through load protocol


- ip rsvp precedence, page 325
- ip rsvp qos, page 328
- ip rsvp reservation, page 329
- ip rsvp reservation-host, page 333
- ip rsvp resource-provider, page 337
- ip rsvp sender, page 339
- ip rsvp sender-host, page 342
- ip rsvp signalling dscp, page 345
- ip rsvp signalling fast-local-repair notifications, page 347
- ip rsvp signalling fast-local-repair rate, page 349
- ip rsvp signalling fast-local-repair wait-time, page 351
- ip rsvp signalling hello (configuration), page 353
- ip rsvp signalling hello (interface), page 354
- ip rsvp signalling hello dscp, page 356
- ip rsvp signalling hello graceful-restart, page 358
- ip rsvp signalling hello graceful-restart dscp, page 360
- ip rsvp signalling hello graceful-restart mode, page 362
- ip rsvp signalling hello graceful-restart mode help-neighbor, page 364
- ip rsvp signalling hello graceful-restart neighbor, page 366
- ip rsvp signalling hello graceful-restart refresh interval, page 368
- ip rsvp signalling hello graceful-restart refresh misses, page 370
- ip rsvp signalling hello graceful-restart send, page 372
- ip rsvp signalling hello refresh interval, page 374
- ip rsvp signalling hello refresh misses, page 376

- ip rsvp signalling hello reroute dscp, page 378
- ip rsvp signalling hello reroute refresh interval, page 380
- ip rsvp signalling hello reroute refresh misses, page 382
- ip rsvp signalling hello statistics, page 384
- ip rsvp signalling initial-retransmit-delay, page 385
- ip rsvp signalling patherr state-removal, page 386
- ip rsvp signalling rate-limit, page 388
- ip rsvp signalling refresh interval, page 390
- ip rsvp signalling refresh misses, page 392
- ip rsvp signalling refresh reduction, page 394
- ip rsvp signalling refresh reduction ack-delay, page 396
- ip rsvp snooping, page 397
- ip rsvp source, page 399
- ip rsvp svc-required, page 401
- ip rsvp tos, page 403
- ip rsvp transport, page 406
- ip rsvp transport sender-host, page 408
- ip rsvp tunnel overhead-percent, page 410
- ip rsvp udp-multicasts, page 412
- ip rsvp udp neighbor, page 414
- ip rtp compression-connections, page 416
- ip rtp header-compression, page 418
- ip rtp priority, page 422
- ip tcp compression-connections, page 426
- ip tcp header-compression, page 428
- iphc-profile, page 431
- lane client qos, page 435
- lane qos database, page 437
- load protocol, page 439

# ip rsvp precedence

To enable the router to mark the IP Precedence value of the type of service (ToS) byte for packets in a Resource Reservation Protocol (RSVP) reserved path using the specified values for packets that either conform to or exceed the RSVP flowspec, use the **iprsvpprecedence**command in interface configuration mode. To remove existing IP Precedence settings, use the **no** form of this command.

**ip rsvp precedence** {**conform** *precedence-value*| **exceed** *precedence-value*}

**no ip rsvp precedence** [**conform**| **exceed**]

## Syntax Description

| | |
|---|---|
| **conform** *precedence-value* | Specifies an IP Precedence value in the range from 0 to 7 for traffic that conforms to the RSVP flowspec. The IP Precedence value is written to the three high-order bits (bits 5 to 7) of the ToS byte in the IP header of a packet. Either the **conform** or **exceed** keyword is required; both keywords may be specified.<br>When used with the **no** form of the command, the **conform** keyword is optional. |
| **exceed** *precedence-value* | Specifies an IP Precedence value in the range from 0 to 7 for traffic that exceeds the RSVP flowspec. The IP Precedence value is written to the three high-order bits (bits 5 to 7) of the ToS byte in the IP header of a packet. Either the **conform** or **exceed** keyword is required; both keywords may be specified.<br>When used with the **no** form of the command, the **exceed** keyword is optional. |

## Command Default

The IP Precedence bits of the ToS byte are left unmodified when this command is not used. The default state is equivalent to execution of the **noiprsvpprecedence** command.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Packets in an RSVP reserved path are divided into two classes: those that conform to the reservation flowspec and those that correspond to a reservation but that exceed, or are outside, the reservation flowspec.

The **iprsvpprecedence** command allows you to set the IP Precedence values to be applied to packets belonging to these two classes. You must specify the IP Precedence value for at least one class of traffic when you use this command. You can use a single instance of the command to specify values for both classes, in which case you can specify the **conform** and **exceed** keywords in either order.

As part of its input processing, RSVP uses the **iprsvpprecedence** command to set the IP Precedence bits on conforming and nonconforming packets. If per-VC DWRED is configured, the system uses the IP Precedence and ToS bit settings on the output interface in its packet drop process. The IP Precedence setting of a packet can also be used by interfaces on downstream routers.

Execution of the **iprsvpprecedence** command causes IP Precedence values for all preexisting reservations on the interface to be modified.

**Note** RSVP must be enabled on an interface before you can use this command; that is, use of the **iprsvpbandwidth** command must precede use of the **iprsvpprecedence** command. RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

RSVP receives packets from the underlying forwarding mechanism. Therefore, before you use the **iprsvpprecedence** command to set IP Precedence, one of the following features is required:

- Weighted fair queueing (WFQ) must be enabled on the interface.
- RSVP switched virtual circuits (SVCs) must be used.
- NetFlow must be configured to assist RSVP.

**Note** Use of the **no** form of this command is not equivalent to giving the **iprsvpprecedence0**command, which sets all precedence on the packets to 0, regardless of previous precedence setting.

## Examples

The following example sets the IP Precedence value to 3 for all traffic on the ATM interface 0 that conforms to the RSVP flowspec and to 2 for all traffic that exceeds the flowspec:

```
interface atm0
 ip rsvp precedence conform 3 exceed 2
```

The following example sets the IP Precedence value to 2 for all traffic on ATM interface 1 that conforms to the RSVP flowspec. The IP Precedence values of those packets that exceed the flowspec are not altered in any way.

```
interface ATM1
 ip rsvp precedence conform 2
```

## Related Commands

| Command | Description |
|---|---|
| ip rsvp bandwidth | Enables RSVP for IP on an interface. |
| ip rsvp policy cops minimal | Lowers the COPS server's load and improves latency times for messages on the governed router. |
| **ip rsvp tos** | Allows you to set the ToS values to be applied to packets that either conform to or exceed the RSVP flowspec. |
| **s how ip rsvp** | Displays the IP Precedence and ToS bit values to be applied to packets that either conform to or exceed the RSVP flowspec for a given interface. |

# ip rsvp qos

To enable Resource Reservation Protocol (RSVP) quality of service (QoS) flows on a router running Multiprotocol Label Switching traffic engineering (MPLS TE), use the **iprsvpqos** command in global configuration mode. To disable RSVP QoS flows, use the **no** form of this command.

**ip rsvp qos**

**no ip rsvp qos**

## Syntax Description

This command has no arguments or keywords.

## Command Default

RSVP QoS flows are not enabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRC | This command was introduced. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

If RSVP QoS flows and MPLS TE are enabled, the router processes and installs RSVP label switched path (LSP) and IPv4 messages such as PATH and RESV. If RSVP QoS flows and MPLS TE are then disabled with IPv4 and LSP states installed, all installed IPv4 states are immediately cleared. LSP states remain unmodified. Further refreshes or new IPv4 RSVP messages are forwarded unmodified.

Use the **showiprsvp** command to display the status of the **iprsvpqos** command.

## Examples

The following example configures RSVP QoS flows on a router running MPLS TE:

```
Router> enable
Router# configure terminal
Router(config)# ip rsvp qos
```

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp** | Displays specific information for RSVP categories. |

# ip rsvp reservation

To enable a router to simulate receiving Resource Reservation Protocol (RSVP) RESV messages from a downstream host, use the **iprsvpreservation**command in global configuration mode. To disable this function, use the **no** form of this command.

**ip rsvp reservation** *session-ip-address sender-ip-address* {*ip-protocol*| **tcp**| **udp**} *session-dest-port sender-source-port next-hop-address next-hop-interface* {**ff**| **se**| **wf**} {**load**| **rate**} *bandwidth burst-size* [**identity** *alias*]

**no ip rsvp reservation** *session-ip-address sender-ip-address* {*ip-protocol*| **tcp**| **udp**} *session-dest-port sender-source-port next-hop-address next-hop-interface* {**ff**| **se**| **wf**} {**load**| **rate**} *bandwidth burst-size* [**identity** *alias*]

## Syntax Description

| | |
|---|---|
| *session-ip-address* | For unicast sessions, the address of the intended receiver; for multicast sessions, the IP multicast address of the session. |
| *sender-ip-address* | IP address of the sender. |
| *ip-protocol* \|**tcp** \| **udp** | Specifies the IP protocol in the range of 0 to 255, TCP, or UDP. |
| *session-dest-port sender-source-port* | *The session-dest-port* argument is the destination port. The *sender-source-port* argument is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If the destination is zero, the source must be zero, and the implication is that ports are not checked. If the destination is nonzero, the source must be nonzero (except for Wildcard Filterreservations, for which the source port is always ignored and can therefore be zero). |
| *next-hop-address* | Hostname or IP address of the receiver or the router closest to the receiver. |
| *next-hop-interface* | Next-hop interface or subinterface type and number. Interface type can be **ethernet**, **loopback**, **null**, or **serial**. |
| **ff** \| **se** \| **wf** | Specifies the reservation style:<br>• **ff--** Fixed Filter with single reservation.<br>• **se** --Shared Explicit with shared reservation and limited scope.<br>• **wf** --Wildcard Filter with shared reservation and unlimited scope. |

| | |
|---|---|
| **load** | Specifies the controlled load service. |
| **rate** | Specifies the Quality of Service (QoS) guaranteed bit rate service. |
| *bandwidth* | Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000. |
| *burst-size* | Maximum burst size (kbps of data in queue). The range is from 1 to 65535. |
| **identity** alias | (Optional) Specifies an application ID alias. An alias is a string that can have as many as 64 printable characters (in the range 0x20 to 0x7E).<br>**Note** If you use the " " or ? character as part of the alias or locator string itself, you must type the CTRL-V key sequence before entering the embedded " " or ? character. The alias is never transmitted to other routers. |

## Command Default

The router does not simulate receiving RSVP RESV messages.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.4(6)T | This command was modified. The optional**identity***alias* keyword and argument combination was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

Use the **iprsvpreservation** command to make the router simulate receiving RSVP RESV messages from a downstream host and to proxy RSVP RESV messages for that host. By giving a local (loopback) next-hop address and next-hop interface, you can also use this command to proxy RSVP for the router that you are configuring or you can use the **iprsvpreservation-host** command.

An alias must reference an RSVP identity that you created by using the **iprsvpidentity** command. The policy-locator string associated with this identity is signaled in the RESV message. This identity overrides any application ID that is contained in the matching PATH message.

If the matching PATH message has an application ID, but you have not specified an application ID using the **iprsvpreservation** command, the RESV message will not contain an application ID. However, the RESV message proxied by the **iprsvplistener** command does put the matching PATH message application ID into the proxied RESV message.

## Examples

The following example specifies the use of a Shared Explicit style of reservation and the controlled load service, with token buckets of 100 or 150 kbps and a maximum queue depth of 60 or 65 kbps:

```
Router(config)# ip rsvp reservation 192.168.0.2 172.16.1.1 udp 20 30 172.16.4.1 Ethernet1
se load 100 60
Router(config)# ip rsvp reservation 192.168.0.2 172.16.2.1 tcp 20 30 172.16.4.1 Ethernet1
se load 150 65
```

The following example specifies the use of a Wildcard Filter style of reservation and the guaranteed bit rate service, with token buckets of 300 or 350 kbps, a maximum queue depth of 60 or 65 kbps, and an application ID:

```
Router(config)# ip rsvp reservation 192.168.0.3 0.0.0.0 udp 20 0 172.16.4.1 Ethernet1 wf
rate 300 60 identity xyz
Router(config)# ip rsvp reservation 192.168.1.1 0.0.0.0 udp 20 0 172.16.4.1 Ethernet1 wf
rate 350 65 identity xyz
```

Note that the wildcard filter does not admit the specification of the sender; it accepts all senders. This action is denoted by setting the source address and port to zero. If, in any filter style, the destination port is specified to be zero, RSVP does not permit the source port to be anything else; it understands that such protocols do not use ports or that the specification applies to all ports.

## Related Commands

| Command | Description |
|---|---|
| ip rsvp bandwidth | Enables RSVP for IP on an interface. |
| ip rsvp identity | Defines RSVP application IDs. |
| ip rsvp neighbor | Enables a router to control who its authorized neighbors are. |
| **ip rsvp reservation-host** | Enables a router to simulate a host generating RSVP RESV messages. |
| **ip rsvp sender** | Enables a router to simulate receiving RSVP PATH messages. |
| **ip rsvp sender-host** | Enables a router to simulate a host generating RSVP PATH messages. |
| **show ip rsvp installed** | Displays RSVP-related bandwidth information. |
| **show ip rsvp interface** | Displays RSVP-related interface information. |

| Command | Description |
|---|---|
| **show ip rsvp neighbor** | Displays current RSVP neighbors. |
| show ip rsvp policy identity | Displays selected RSVP identities in a router configuration. |
| **show ip rsvp reservation** | Displays RSVP RESV-related receiver information currently in the database. |
| **show ip rsvp sender** | Displays RSVP PATH-related sender information currently in the database. |

# ip rsvp reservation-host

To enable a router to simulate a host generating Resource Reservation Protocol (RSVP) RESV messages, use the **iprsvpreservation-host**command in global configuration mode. To disable this function, use the **no** form of this command.

**ip rsvp reservation-host** *session-ip-address sender-ip-address* {*ip-protocol*| **tcp**| **udp**} *session-dest-port sender-source-port* {**ff**| **se**| **wf**} {**load**| **rate**} *bandwidth burst-size* [**identity** *alias*] [**vrf** *vrf-name*]

**no ip rsvp reservation-host** *session-ip-address sender-ip-address* {*ip-protocol*| **tcp**| **udp**} *session-dest-port sender-source-port* {**ff**| **se**| **wf**} {**load**| **rate**} *bandwidth burst-size* [**identity** *alias*] [**vrf** *vrf-name*]

## Syntax Description

| | |
|---|---|
| *session-ip-address* | For unicast sessions, this is the address of the intended receiver. IP multicast addresses cannot be used with this argument. It must be a logical address configured on an interface on the router that you are configuring. |
| *sender-ip-address* | IP address of the sender. |
| *ip-protocol* \| **tcp** \| **udp** | Specifies the IP protocol in the range of 0 to 255, TCP or UDP. |
| *session-dest-port sender-source-port* | *The session-dest-port* argument is the destination port. The *sender-source-port* argument is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If the destination is zero, the source must be zero, and the implication is that ports are not checked. If the destination is nonzero, the source must be nonzero (except for Wildcard Filter reservations, for which the source port is always ignored and can therefore be zero). |
| **ff** \| **se** \| **wf** | Specifies the reservation style:<br>• **ff--** Fixed Filter with single reservation.<br>• **se** --Shared Explicit with shared reservation and limited scope.<br>• **wf** --Wildcard Filter with shared reservation and unlimited scope. |
| **load** | Specifies the controlled load service. |
| **rate** | Specifies the Quality of Service (QoS) guaranteed bit rate service. |

| | |
|---|---|
| *bandwidth* | Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000. |
| *burst-size* | Maximum burst size (kbps of data in queue). The range is from 1 to 65535. |
| **identity** alias | (Optional) Specifies an application ID alias. An alias is a string that can have as many as 64 printable characters (in the range 0x20 to 0x7E).<br>**Note** If you use the " " or ? character as part of the alias or locator string itself, you must type the CTRL-V key sequence before entering the embedded " " or ? character. The alias is never transmitted to other routers. |
| **vrf** vrf-name | (Optional) Specifies a virtual routing and forwarding (VRF) instance. |

**Command Default**

The router does not simulate a host generating RSVP RESV messages.

**Command Modes**

Global configuration (config)

**Command History**

| Release | Modification |
|---|---|
| 12.0 | This command was introduced. |
| 12.4(6)T | This command was modified. The optional**identity***alias* keyword and argument combination was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.0(1)M | This command was modified. The optional **vrf***vrf-name* keyword and argument combination was added. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelin

**Note** The syntax of the command depends on your platform and release. The **vrf***vrf-name*keyword and argument combination is not supported on ASR 1000 Series Aggregation Services Routers.

Use the **iprsvpreservation-host**command to make a router simulate a host generating its own RSVP RESV messages. This command is similar to the **iprsvpreservation** command, which can cause a router to generate RESV messages on behalf of another host. The main differences between the **iprsvpreservation-host** and **iprsvpreservation** commands follow:

- When you enter the **iprsvpreservation-host** command, the *session-ip-address* argument must be a local address configured on an interface on the router. Therefore, you cannot proxy a reservation on behalf of a flow that is destined for another host. Also, you cannot use this command to generate reservation messages for multicast sessions.
- Because the message is assumed to originate from the router that you are configuring, you do not specify a next-hop or incoming interface for the RSVP RESV message when entering the **iprsvpreservation-host** command.
- Use the **iprsvpreservation-host** command for debugging and testing purposes because you cannot use it to proxy RSVP for non-RSVP-capable hosts or for multicast sessions.

An alias must reference an RSVP identity that you created by using the **iprsvpidentity** command. The policy-locator string associated with this identity is signaled in the RESV message. This identity overrides any application ID that is contained in the matching PATH message.

If the matching PATH message has an application ID, but you have not specified an application ID using the **iprsvpreservation-host** command, the RESV message does not contain an application ID. However, the RESV message proxied by the **iprsvplistener** command does put the matching PATH message application ID into the proxied RESV message.

## Examples

The following example specifies the use of a Shared Explicit style of reservation and the controlled load service, with token buckets of 100 or 150 kbps, 60 or 65 kbps maximum queue depth, and an application ID:

```
Router(config)# ip rsvp reservation-host 10.1.1.1 10.30.1.4 udp 20 30 se load 100 60 identity
 xyz
Router(config)# ip rsvp reservation-host 10.40.2.2 10.22.1.1 tcp 20 30 se load 150 65
identity xyz
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp bandwidth** | Enables RSVP for IP on an interface. |
| ip rsvp identity | Defines RSVP application IDs. |
| **ip rsvp neighbor** | Enables a router to control who its authorized RSVP neighbors are. |
| **ip rsvp reservation** | Enables a router to simulate receiving RSVP RESV messages. |

| Command | Description |
|---|---|
| ip rsvp sender | Enables a router to simulate receiving RSVP PATH messages. |
| ip rsvp sender-host | Enables a router to simulate a host generating RSVP PATH messages. |
| **show ip rsvp installed** | Displays RSVP-related bandwidth information. |
| **show ip rsvp interface** | Displays RSVP-related interface information. |
| **show ip rsvp neighbor** | Displays current RSVP neighbors. |
| show ip rsvp policy identity | Displays selected RSVP identities in a router configuration. |
| **show ip rsvp reservation** | Displays RSVP RESV-related receiver information currently in the database. |
| **show ip rsvp sender** | Displays RSVP PATH-related sender information currently in the database. |

# ip rsvp resource-provider

To configure a resource provider for an aggregate flow, use the **iprsvpresource-provider** command in interface configuration mode. To disable a resource provider for an aggregate flow, use the **no** form of this command.

**ip rsvp resource-provider** {**none**| **wfq interface**| **wfq pvc**}

**no ip rsvp resource-provider**

## Syntax Description

| | |
|---|---|
| **none** | Specifies no resource provider regardless of whether one is configured on the interface. |
| **wfq interface** | Specifies Weighted fair queueing (WFQ) as the resource provider on the interface. |
| **wfq pvc** | Specifies WFQ as the resource provider on the permanent virtual circuit (PVC) or connection. |

## Command Default

WFQ (the **wfqinterface**keyword) is the default resource provider that Resource Reservation Protocol (RSVP) configures on the interface.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(2)T | This command was introduced. |
| 12.0(24)S | This command was integrated into Cisco IOS Release 12.0(24)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(18)SXF2 | This command was integrated into Cisco IOS Release 12.2(18)SXF2. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelin

**Note** The syntax of the command depends on your platform and image. The **wfqinterface** and **wfqpvc** keywords are not supported on Cisco ASR 1000 series routers.

Use the **iprsvpresource-provider** command to configure the resource provider with which you want RSVP to interact when it installs a reservation.

To ensure that a flow receives quality of service (QoS) guarantees when using WFQ on a per-flow basis, configure **wfqinterface** or **wfqpvc** as the resource provider. To ensure that a flow receives QoS guarantees when using class-based weighted fair queueing (CBWFQ) for data packet processing, configure**none** as the resource provider.

**Note** Resource provider was formerly called QoS provider.

## Examples

In the following example, the **iprsvpresource-provider** command is configured with **wfqpvc** as the resource provider, ensuring that a flow receives QoS guarantees when using WFQ on a per-flow basis:

```
Router# configure terminal
Router(config)# interface atm 6/0
Router(config-if)# ip rsvp resource-provider wfq pvc
```

In the following example, the **iprsvpresource-provider** command is configured with **none**as the resource provider, ensuring that a flow receives QoS guarantees when using CBWFQ for data-packet processing:

```
Router# configure terminal
Router(config)# interface atm 6/0
Router(config-if)# ip rsvp resource-provider none
```

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp interface** | Displays RSVP-related interface information. |

# ip rsvp sender

To enable a router to simulate receiving Resource Reservation Protocol (RSVP) PATH messages, use the **iprsvpsender**command in global configuration mode. To disable this function, use the **no** form of this command.

**ip rsvp sender** *session-ip-address sender-ip-address* {*ip-protocol*| **tcp**| **udp**} *session-dest-port sender-source-port previous-hop-ip-address previous-hop-interface bandwidth burst-size* [**identity** *alias*]

**no ip rsvp sender** *session-ip-address sender-ip-address* {*ip-protocol*| **tcp**| **udp**} *session-dest-port sender-source-port previous-hop-ip-address previous-hop-interface bandwidth burst-size* [**identity** *alias*]

## Syntax Description

| | |
|---|---|
| *session-ip-address* | For unicast sessions, the address of the intended receiver; for multicast sessions, the IP multicast address of the session. |
| *sender-ip-address* | IP address of the sender. |
| *ip-protocol* \| **tcp** \| **udp** | Specifies the IP protocol in the range of 0 to 255, TCP or UDP. |
| *session-dest-port sender-source-port* | *The session-dest-port* argument is the destination port. The *sender-source-port* argument is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If the destination is zero, the source must be zero, and the implication is that ports are not checked. If the destination is nonzero, the source must be nonzero. |
| *previous-hop-ip-address* | Address of the sender or the router closest to the sender. |
| *previous-hop-interface* | Previous-hop interface or subinterface. Interface type can be **ethernet**, **gigabitethernet**, **loopback**, **null**, or **serial**. |
| *bandwidth* | Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000. |
| *burst-size* | Maximum burst size (kbps of data in queue). The range is from 1 to 65535. |

| | |
|---|---|
| **identity** *alias* | (Optional) Specifies an application ID alias. An alias is a string that can have as many as 64 printable character (in the range 0x20 to 0x7E).<br>**Note** If you use the " " or ? character as part of the alias or locator string itself, you must type the CTRL-V key sequence before entering the embedded " " or ? character. The alias is never transmitted to other routers. |

## Command Default

The router does not simulate receiving RSVP PATH messages.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.4(6)T | This command was modified. The optional **identity***alias*keyword and argument combination was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

Use the **iprsvpsender** command to make the router simulate the receiving of RSVP PATH messages from an upstream host and to proxy RSVP PATH messages from that host. By including a local (loopback) previous-hop address and previous-hop interface, you can also use this command to proxy RSVP for the router that you are configuring.

An alias must reference an RSVP identity that you created by using the **iprsvpidentity** command. The policy-locator string associated with this identity is supplied in the PATH message.

## Examples

The following example sets up the router to act as though it is receiving RSVP PATH messages using UDP over loopback interface 1:

```
Router(config)# ip rsvp sender 192.168.0.1 172.16.2.1 udp 20 30 172.16.2.1 loopback1 50 5
identity xyz
Router(config)# ip rsvp sender 192.168.0.2 172.16.2.1 udp 20 30 172.16.2.1 loopback1 50 5
identity xyz
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp bandwidth** | Enables RSVP for IP on an interface. |
| ip rsvp identity | Defines RSVP application IDs. |
| **ip rsvp neighbor** | Enables a router to control who its authorized RSVP neighbors are. |
| **ip rsvp reservation** | Enables a router to simulate receiving RSVP RESV messages. |
| **ip rsvp reservation-host** | Enables a router to simulate a host generating RSVP RESV messages. |
| ip rsvp sender-host | Enables a router to simulate a host generating RSVP PATH messages. |
| **show ip rsvp installed** | Displays RSVP-related bandwidth information. |
| **show ip rsvp interface** | Displays RSVP-related interface information. |
| **show ip rsvp neighbor** | Displays current RSVP neighbors. |
| show ip rsvp policy identity | Displays selected RSVP identities in a router configuration. |
| **show ip rsvp reservation** | Displays RSVP RESV-related receiver information currently in the database. |
| **show ip rsvp sender** | Displays RSVP PATH-related sender information currently in the database. |

# ip rsvp sender-host

To enable a router to simulate a host generating a Resource Reservation Protocol (RSVP) PATH message, use the **iprsvpsender-host**command in global configuration mode. To disable this function, use the **no** form of this command.

**ip rsvp sender-host** *session-ip-address sender-ip-address* {*ip-protocol*| **tcp**| **udp**} *session-dest-port sender-source-port bandwidth burst-size* [**identity** *alias*] [**vrf** *vrf-name*]

**no ip rsvp sender-host** *session-ip-address sender-ip-address* {*ip-protocol*| **tcp**| **udp**} *session-dest-port sender-source-port bandwidth burst-size* [**identity** *alias*] [**vrf** *vrf-name*]

## Syntax Description

| | |
|---|---|
| *session-ip-address* | For unicast sessions, the address of the intended receiver; for multicast sessions, the IP multicast address of the session. |
| *sender-ip-address* | IP address of the sender. It must be a logical address configured on an interface on the router that you are configuring. |
| *ip-protocol* \|**tcp** \| **udp** | Specifies the IP protocol in the range of 0 to 255, TCP or UDP. |
| *session-dest-port sender-source-port* | *The session-dest-port* argument is the destination port. The *sender-source-port* argument is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If the destination is zero, the source must be zero, and the implication is that ports are not checked. If the destination is nonzero, the source must be nonzero. |
| *bandwidth* | Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000. |
| *burst-size* | Maximum burst size (kbps of data in queue). The range is from 1 to 65535. |
| **identity** *alias* | (Optional) Specifies an application ID alias. An alias is a string that can have as many as 64 printable characters (in the range 0x20 to 0x7E).<br>**Note** If you use the " " or ? character as part of the string itself, you must type the CTRL-V key sequence before entering the embedded " " or ? character. The alias is never transmitted to other routers. |

| | |
|---|---|
| **vrf** vrf-name | (Optional) Specifies a virtual routing and forwarding (VRF) instance. |

**Command Default** The router does not simulate RSVP PATH message generation.

**Command Modes** Global configuration (config)

**Command History**

| Release | Modification |
|---|---|
| 12.0 | This command was introduced. |
| 12.4(6)T | This command was modified. The optional **identity***alias*keyword and argument combination was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.0(1)M | This command was modified. The optional **vrf***vrf-name* keyword and argument combination was added. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

**Usage Guidelin**

**Note** The syntax of the command depends on your platform and release. The **vrf***vrf-name*keyword and argument combination is not supported on ASR 1000 Series Aggregation Services Routers.

Use the **iprsvpsender-host**command to make a router simulate a host generating its own RSVP PATH messages. This command is similar to the **iprsvpsender** command, which can cause a router to generate RSVP PATH messages on behalf of another host. The main differences between the **iprsvpsender-host** and **iprsvpsender** commands follow:

- When you enter the **iprsvpsender-host** command, the *sender-ip-address* argument must be a local address configured on an interface of the router.
- Because the message is assumed to originate from the router that you are configuring, you do not specify a previous-hop or incoming interface for the RSVP PATH message when entering the **iprsvpsender-host** command.
- Use the **iprsvpsender-host** command for debugging and testing purposes because you cannot use it to proxy RSVP for non-RSVP-capable hosts.

An alias must reference an RSVP identity that you created by using the **iprsvpidentity** command. The policy-locator string associated with this identity is signaled in the RESV message. This identity overrides any application ID that is contained in the matching PATH message.

## Examples

The following example sets up the router to act like a host that sends traffic to the given address:

```
Router(config)# ip rsvp sender-host 10.0.0.7 10.0.0.1 udp 1 1 10 10 identity xyz
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp bandwidth** | Enables RSVP for IP on an interface. |
| ip rsvp identity | Defines RSVP application IDs. |
| **ip rsvp neighbor** | Enables a router to control who its authorized neighbors are. |
| **ip rsvp reservation** | Enables a router to simulate receiving RSVP RESV messages. |
| **ip rsvp reservation-host** | Enables a router to simulate a host generating RSVP RESV messages. |
| ip rsvp sender | Enables a router to simulate receiving RSVP PATH messages. |
| **show ip rsvp installed** | Displays RSVP-related bandwidth information. |
| **show ip rsvp interface** | Displays RSVP-related interface information. |
| **show ip rsvp neighbor** | Displays current RSVP neighbors. |
| show ip rsvp policy identity | Displays selected RSVP identities in a router configuration. |
| **show ip rsvp reservation** | Displays RSVP RESV-related receiver information currently in the database. |
| **show ip rsvp sender** | Displays RSVP PATH-related sender information currently in the database. |

# ip rsvp signalling dscp

To specify the differentiated services code point (DSCP) value to be used on all Resource Reservation Protocol (RSVP) messages transmitted on an interface, use the **iprsvpsignallingdscp** command in interface configuration mode. To disable this function, use the **no** form of this command.

**ip rsvp signalling dscp** *value*

**no ip rsvp signalling dscp**

## Syntax Description

| | |
|---|---|
| *value* | A number for the DSCP. Range is from 0 to 63. Default is 0. |

## Command Default

The default value is 0.

## Command Modes

Interface configuration.

## Command History

| Release | Modification |
|---|---|
| 12.1 | This command was introduced |
| 12.2(18)SXF2 | This command was integrated into Cisco IOS Release 12.2(18)SXF2. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

You configure the DSCP per interface, not per flow. The DSCP determines the priority that a packet receives from various hops as it travels to its destination.

The DSCP applies to all RSVP flows installed on a specific interface. You can configure each interface independently for DSCP.

## Examples

Here is an example of the **iprsvpsignallingdscp**command with a DSCP value of 6

```
Router(config-if)# ip rsvp signalling dscp 6
Router(config-if)# end
```

To verify the DSCP value, enter the **showiprsvpinterfacedetail** command:

```
Router# show ip rsvp interface serial2/0 detail
Se2/0:
   Bandwidth:
     Curr allocated:10K bits/sec
     Max. allowed (total):1536K bits/sec
     Max. allowed (per flow):1536K bits/sec
   Neighbors:
```

```
  Using IP enacp:1.  Using UDP encaps:0
DSCP value used in Path/Resv msgs:0x6
Burst Police Factor:300%
RSVP:Data Packet Classification provided by: none
```

# ip rsvp signalling fast-local-repair notifications

To configure the number of per flow notifications that Resource Reservation Protocol (RSVP) processes during a fast local repair (FLR) procedure before suspending, use the **iprsvpsignallingfast-local-repairnotifications** command in global configuration mode. To set the number of notifications to its default, use the **no** form of this command.

**ip rsvp signalling fast-local-repair notifications** *number*

**no ip rsvp signalling fast-local-repair notifications**

## Syntax Description

| | |
|---|---|
| *number* | Total number of notifications to be sent. The range is from 10 to 10000. The default value is 1000. |

## Command Default

Notifications are sent by the Routing Information Base (RIB) and processed by RSVP. If the **iprsvpsignallingfast-local-repairnotifications** command is not configured, RSVP processes 1000 notifications, suspends the notifications, and then resumes processing of another 1000 notifications.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRB | This command was introduced. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |
| 15.0(1)M | This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M. |

## Usage Guidelines

Upon a route change, RIB builds a list of notifications, one per affected flow, and notifies RSVP by sending an event including these notifications. Therefore, these events can contain thousands of elements, depending on the number of path state blocks (PSBs) affected.

RSVP processes, by default, 1000 notifications at a time and then suspends if required, to prevent the CPU from being overwhelmed. However, you can configure this number using the **iprsvpsignallingfast-local-repairnotifications** command.

## Examples

The following example shows how to configure the number of flows that are repaired before RSVP suspends to 100:

```
Router(config)# ip rsvp signalling fast-local-repair notifications 100
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling fast-local-repair rate** | Configures the repair rate that RSVP uses for an FLR procedure. |
| **ip rsvp signalling fast-local-repair wait-time** | Configures the delay that RSVP uses to start an FLR procedure. |
| **show ip rsvp signalling fast-local-repair** | Displays FLR-specific information maintained by RSVP. |

# ip rsvp signalling fast-local-repair rate

To configure the repair rate that Resource Reservation Protocol (RSVP) uses for a fast local repair (FLR) procedure, use the **iprsvpsignallingfast-local-repairrate**command in global configuration mode. To set the repair rate to its default, use the **no** form of this command.

**ip rsvp signalling fast-local-repair rate** *messages-per-second*

**no ip rsvp signalling fast-local-repair rate**

## Syntax Description

| | |
|---|---|
| *messages-per-second* | FLR rate for PATH state refresh and repair, in messages per second. The range is 1 to 2500. The default is 400. |

## Command Default

If this command is not configured, the RSVP message pacing rate is used.

**Note** The RSVP message pacing rate is enabled by default in Cisco IOS Release 12.2 and later releases.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRB | This command was introduced. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |
| 15.0(1)M | This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M. |

## Usage Guidelines

The default repair rate is based on the RSVP message pacing rate.

If you configure the FLR rate by using the **iprsvpsignallingfast-local-repairrate** command, and RSVP message pacing is enabled, the lower FLR rate and the RSVP message pacing rate takes effect. If you disable the RSVP rate limit by using the**noiprsvpsignallingrate-limit**command, then the FLR rate is used. However, if you disable the RSVP rate limit and do not configure an FLR rate, then RSVP performs no message pacing and messages are sent back-to-back. This action is not recommended because the point of local repair (PLR) may flood the downstream node with PATH messages causing some of them to be dropped.

The repair rate is determined at notification time, and this same rate is used during the time of the repair even if you change either the RSVP message pacing rate or the FLR rate during this time.

## Examples

The following example shows how to configure a repair rate of 100 messages per second:

```
Router(config)# ip rsvp signalling fast-local-repair rate 100
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling fast-local-repair notifications** | Configures the number of notifications that are processed before RSVP suspends. |
| **ip rsvp signalling fast-local-repair wait-time** | Configures the delay used to start an FLR procedure. |
| **ip rsvp signalling rate-limit** | Controls the transmission rate for RSVP messages sent to a neighboring router during a specified amount of time. |

# ip rsvp signalling fast-local-repair wait-time

To configure the delay that Resource Reservation Protocol (RSVP) uses before starting a fast local repair (FLR) procedure, use the **iprsvpsignallingfast-local-repairwait-time**command in interface configuration mode. To set the delay to its default, use the **no** form of this command.

**ip rsvp signalling fast-local-repair wait-time** *interval*

**no ip rsvp signalling fast-local-repair wait-time**

## Syntax Description

| | |
|---|---|
| *interval* | Amount of time before an FLR procedure begins, in milliseconds (ms). The range is 0 to 5000. The default is 0. |

## Command Default

This command is disabled by default; therefore, no delay is configured.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRB | This command was introduced. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

Use the **iprsvpsignallingfast-local-repairwait-time** command to configure the delay desired in starting an FLR procedure. If you do not configure a delay, then path refreshes are triggered immediately after RSVP receives a route change notification from the Routing Information Base (RIB).

## Examples

The following example configures a delay of 100 ms:

```
Router(config-if)# ip rsvp signalling fast-local-repair wait-time 100
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling fast-local-repair notifications** | Configures the number of notifications that are processed before RSVP suspends. |
| **ip rsvp signalling fast-local-repair rate** | Configures the repair rate that RSVP uses for an FLR procedure. |

# ip rsvp signalling hello (configuration)

To enable Hello globally on the router, use the **iprsvpsignallinghello**command in global configuration mode. To disable Hello globally on the router, use the **no** form of this command.

**ip rsvp signalling hello**

**no ip rsvp signalling hello**

## Syntax Description

This command has no arguments or keywords.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(22)S | This command was introduced. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

To enable Hello globally on the router, you must enter this command. You also must enable Hello on the interface.

## Examples

In the following example, Hello is enabled globally on the router:

```
Router(config)# ip rsvp signalling hello
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello (interface)** | Enables Hello on an interface where you need Fast Reroute protection. |
| **ip rsvp signalling hello statistics** | Enables Hello statistics on the router. |

# ip rsvp signalling hello (interface)

To enable hello on an interface where you need Fast Reroute protection, use the **iprsvpsignallinghello**command in interface configuration mode. To disable hello on an interface where you need Fast Reroute protection, use the **no** form of this command

**ip rsvp signalling hello**

**no ip rsvp signalling hello**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No hellos are enabled.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.0(22)S | This command was introduced. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

You must configure hello globally on a router and on the specific interface.

## Examples

In the following example, hello is enabled on an interface:

```
Router(config-if)# ip rsvp signalling hello
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello (configuration)** | Enables Hello globally on the router. |
| **ip rsvp signalling hello dscp** | Sets the DSCP value that is in the IP header of the Hello messages sent out from the interface. |

| Command | Description |
|---|---|
| **ip rsvp signalling hello refresh misses** | Specifies how many Hello acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down. |
| **ip rsvp signalling hello refresh interval** | Configures the Hello request interval. |

# ip rsvp signalling hello dscp

To set the differentiated services code point (DSCP) value that is in the IP header of a Resource Reservation Protocol (RSVP) traffic engineering (TE) hello message sent from an interface, use the **iprsvpsignallinghellodscp** command in interface configuration mode. To set the DSCP value to its default, use the **no** form of this command.

**ip rsvp signalling hello [fast-reroute] dscp** *num*

**no ip rsvp signalling hello [fast-reroute] dscp**

## Syntax Description

| | |
|---|---|
| **fast-reroute** | (Optional) Initiates Fast Reroute capability. |
| *num* | DSCP value. Valid values are from 0 to 63. |

## Command Default

The default DSCP value is 48.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(22)S | This command was introduced. |
| 12.0(29)S | The optional **fast-reroute** keyword was added. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

If a link is congested, it is recommended that you set the DSCP to a value higher than 0 to reduce the likelihood that hello messages will be dropped.

You configure the DSCP per interface, not per flow.

The DSCP applies to the RSVP hellos created on a specific interface. You can configure each interface independently for DSCP.

If you issue the **iprsvpsignallinghellodscp** command without the optional **fast-reroute**keyword, the command applies to Fast Reroute hellos. This command is provided for backward compatibility; however, we recommend that you use the **iprsvpsignallinghellofast-reroutedscp**command.

## Examples

In the following example, hello messages sent from this interface have a DSCP value of 30 and Fast Reroute capability is enabled by specifying the **fast-reroute** keyword:

```
Router(config-if)# ip rsvp signalling hello fast-reroute dscp 30
```

In the following example, hello messages sent from this interface have a DSCP value of 30 and Fast Reroute capability is enabled by default:

```
Router(config-if)# ip rsvp signalling hello dscp 30
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello (interface)** | Enables hellos on an interface where you need Fast Reroute protection. |
| **ip rsvp signalling hello refresh interval** | Sets the hello refresh interval in hello messages. |
| **ip rsvp signalling hello reroute refresh misses** | Sets the missed refresh limit in hello messages. |

# ip rsvp signalling hello graceful-restart

To enable the Resource Reservation protocol (RSVP) traffic engineering (TE) graceful restart capability on a neighboring router, use the **iprsvpsignallinghellograceful-restart** command in interface configuration mode. To disable the graceful restart capability, use the **no** form of this command.

**ip rsvp signalling hello graceful-restart**

**no ip rsvp signalling hello graceful-restart**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Neighboring routers have only node hello enabled.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRE | This command was introduced. |

## Usage Guidelines

Use the **iprsvpsignallinghellograceful-restart** command to enable support for graceful restart on routers helping their neighbors recover TE tunnels following stateful switchover (SSO).

**Note** This command is optional. Use it when node hello is not supported.

## Examples

The following example configures graceful restart on POS interface 1/0/0 of a neighboring router with the IP address 10.0.0.1:

```
Router# configure terminal

Enter configuration commands, one per line. End with CTTL/Z.
Router(config)# interface POS1/0/0

Router(config-if)# ip rsvp signalling hello graceful-restart
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello graceful-restart mode** | Enables RSVP TE graceful restart support capability on an RP, and enables node hello. |

| Command | Description |
|---|---|
| **show ip rsvp hello graceful-restart** | Displays information about RSVP TE graceful restart hello messages. |

# ip rsvp signalling hello graceful-restart dscp

To set the differentiated services code point (DSCP) value that is in the IP header of a Resource Reservation Protocol (RSVP) traffic engineering (TE) graceful restart hello message, use the **iprsvpsignallinghellograceful-restartdscp** command in global configuration mode. To set the DSCP valueto its default, use the **no** form of this command.

**ip rsvp signalling hello graceful-restart dscp** *num*

**no ip rsvp signalling hello graceful-restart dscp**

## Syntax Description

| | |
|---|---|
| *num* | DSCP value. Valid values are from 0 to 63. |

## Command Default

The default DSCP value is 48.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(29)S | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

If a link is congested, set the DSCP to a value higher than 0 to reduce the likelihood that hello messages get dropped.

The DSCP applies to the RSVP hellos created on a specific router. You can configure each router independently for the DSCP.

## Examples

In the following example, hello messages have a DSCP value of 30:

```
Router(config)# ip rsvp signalling hello graceful-restart dscp 30
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello graceful-restart refresh interval** | Sets the hello request interval in graceful restart hello messages. |
| **ip rsvp signalling hello graceful-restart refresh misses** | Sets the missed refresh limit in graceful restart hello messages. |

# ip rsvp signalling hello graceful-restart mode

To enable Resource Reservation Protocol (RSVP) traffic engineering (TE) graceful restart capability on a Route Processor (RP), use the **iprsvpsignallinghellograceful-restartmode**command in global configuration mode. To disable graceful restart capability, use the **no** form of this command.

### Cisco IOS 12.0(29)S, 12.2(33)SRA, 12.2(33)SXH, and Later Releases

**ip rsvp signalling hello graceful-restart mode** {**help-neighbor**| **full**}

**no ip rsvp signalling hello graceful-restart mode**

### Cisco IOS T and XE Trains

**ip rsvp signalling hello graceful-restart mode help-neighbor**

**no ip rsvp signalling hello graceful-restart mode help-neighbor**

## Syntax Description

| | |
|---|---|
| **help-neighbor** | Enables support for a neighboring router to restart after a failure. |
| **full** | Enables support for a router to perform self-recovery or to help a neighbor restart after a failure. |

## Command Default

Graceful restart is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.0(29)S | This command was introduced as **iprsvpsignallinghellograceful-restartmodehelp-neighbor**. |
| 12.2(33)SRA | This command was modified. The **full** keyword was added.This command replaces the as **iprsvpsignallinghellograceful-restartmodehelp-neighbor**command. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 15.0(1)M | This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 Series Aggregation Services Routers. |

## Usage Guidelines

Use the **iprsvpsignallinghellograceful-restartmodehelp-neighbor**command to enable support capability for a neighboring router to restart after a failure.

Use the **iprsvpsignallinghellograceful-restartmodefull**command to enable support capability for a router to begin self-recovery or help its neighbor to restart on platforms that support stateful switchover (SSO), such as Cisco 7600 series routers, provided that you have installed and configured a standby RP.

## Examples

The following example shows how to configure an RP with support capability to perform self-recovery after a failure:

```
Router(config)# ip rsvp signalling hello graceful-restart mode full
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello graceful-restart dscp** | Sets the DSCP value in the IP header of a RSVP TE graceful restart hello message. |
| **ip rsvp signalling hello graceful-restart neighbor** | Enables RSVP-TE graceful restart support capability on a neighboring router. |
| **ip rsvp signalling hello graceful-restart refresh interval** | Sets the value to control the request interval in graceful restart hello messages. |
| **ip rsvp signalling hello graceful-restart refresh misses** | Sets the value to control the missed refresh limit in graceful restart hello messages. |
| **show ip rsvp hello graceful-restart** | Displays information about RSVP-TE graceful restart hello messages. |

# ip rsvp signalling hello graceful-restart mode help-neighbor

**Note** Effective with Cisco IOS Release 12.2(33)SRA, the **iprsvpsignallinghellograceful-restartmodehelp-neighbor** command is replaced by the **iprsvpsignallinghellograceful-restartmode**command. See the **iprsvpsignallinghellograceful-restartmode**command for more information.

To enable Resource Reservation Protocol (RSVP) traffic engineering (TE) graceful restart capability on a neighboring router, use the **iprsvpsignallinghellograceful-restartmodehelp-neighbor**command in global configuration mode. To disable graceful restart capability, use the **no** form of this command.

**ip rsvp signalling hello graceful-restart mode help-neighbor**

**no ip rsvp signalling hello graceful-restart mode help-neighbor**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Graceful restart is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(29)S | This command was introduced. |
| 12.2(33)SRA | This command was replaced by the **iprsvpsignallinghellograceful-restartmode**command. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

Use the **iprsvpsignallinghellograceful-restartmodehelp-neighbor** command to restart a neighboring router.

## Examples

In the following example, graceful restart is enabled:

```
Router(config)# ip rsvp signalling hello graceful-restart mode help-neighbor
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello graceful-restart dscp** | Sets the DSCP value in the IP header of a RSVP TE graceful restart hello message. |
| **ip rsvp signalling hello graceful-restart refresh interval** | Sets the value to control the request interval in graceful restart hello messages. |
| **ip rsvp signalling hello graceful-restart refresh misses** | Sets the value to control the missed refresh limit in graceful restart hello messages. |

# ip rsvp signalling hello graceful-restart neighbor

To enable Resource Reservation Protocol (RSVP) traffic engineering (TE) graceful restart capability on a neighboring router, use the **iprsvpsignallinghellograceful-restartneighbor**command in interface configuration mode. To disable graceful restart capability, use the **no** form of this command.

**ip rsvp signalling hello graceful-restart neighbor** *ip-address*

**no ip rsvp signalling hello graceful-restart neighbor** *ip-address*

## Syntax Description

| | |
|---|---|
| *ip-address* | IP address of a neighbor on a given interface. |

## Command Default

No neighboring routers have graceful restart capability enabled until you issue this command.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was introduced. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

Use the **iprsvpsignallinghellograceful-restartneighbor** command to enable support for graceful restart on routers helping their neighbors recover TE tunnels following stateful switchover (SSO).

**Note** You must issue this command on every interface of the neighboring router that you want to help restart.

## Examples

The following example configures graceful restart on POS interface 1/0/0 of a neighboring router with the IP address 10.0.0.1:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface POS1/0/0
Router(config-if)# ip rsvp
 signalling hello graceful-restart neighbor 10.0.0.1
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello graceful-restart mode** | Enables RSVP-TE graceful restart support capability on an RP. |
| **show ip rsvp hello graceful-restart** | Displays information about RSVP-TE graceful restart hello messages. |

# ip rsvp signalling hello graceful-restart refresh interval

To configure the Resource Reservation Protocol (RSVP) traffic engineering (TE) refresh interval in graceful restart hello messages, use the **iprsvpsignallinghellograteful-restartrefreshinterval** command in global configuration mode. To set the interval to its default value, use the**no** form of this command.

**ip rsvp signalling hello graceful-restart refresh interval** *interval-value*

**no ip rsvp signalling hello graceful-restart refresh interval**

## Syntax Description

| | |
|---|---|
| *interval-value* | Frequency, in milliseconds (ms), at which a node sends hello messages to a neighbor. Valid values are from 1000 to 30000. |

## Command Default

1000 milliseconds (10 seconds)

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(29)S | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

A node periodically generates a hello message that contains a Hello Request object for all its neighbors. The frequency of those hello messages is determined by the hello interval.

**Note** If you change the default value for this command and you are also using the **iprsvpsignallingrefreshinterval** command, ensure that the value for the **iprsvpsignallinghellograceful-restartrefreshintervalcommandislessthanthevaluefortheiprsvpsignallingrefreshinterval** command. Otherwise, some or all of the label-switched paths (LSPs) may not be recovered after a stateful switchover (SSO) has occurred. We recommend that the value for the**iprsvpsignallingrefreshinterval**command be twice the value for the **iprsvpsignallinghellograceful-restartrefreshintervalcommand.**

## Examples

In the following example, hello requests are sent to a neighbor every 5000 ms:

```
Router(config)# ip rsvp signalling hello graceful-restart refresh interval 5000
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello graceful-restart dscp** | Sets the DSCP value in the IP header of a RSVP TE graceful restart hello message. |
| **ip rsvp signalling hello graceful-restart refresh misses** | Sets the missed refresh limit in graceful restart hello messages. |
| **ip rsvp signalling refresh interval** | Specifies the interval between sending refresh messages for each RSVP state. |

# ip rsvp signalling hello graceful-restart refresh misses

To specify how many sequential Resource Reservation Protocol (RSVP) traffic engineering (TE) graceful restart hello acknowledgments (ACKs) a node can miss before the node considers communication with its neighbor lost, use the **iprsvpsignallinghellograceful-restartrefreshmisses** command in global configuration mode. To return the missed refresh limit to its default value, use the **no** form of this command.

**ip rsvp signalling hello graceful-restart refresh misses** *msg-count*

**no ip rsvp signalling hello graceful-restart refresh misses**

## Syntax Description

| | |
|---|---|
| *msg-count* | The number of sequential hello acknowledgments (ACKs) that a node can miss before RSVP considers the state expired and tears it down. Valid values are from 4 to 10. |

## Command Default

The default number of sequential hello acknowledgments is 4.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(29)S | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T |

## Usage Guidelines

A hello message comprises a hello message, a Hello Request object, and a Hello ACK object. Each request is answered by an acknowledgment. If a link is congested or a router has a heavy load, set this number to a value higher than the default value to ensure that hello does not falsely declare that a neighbor is down.

**Note** If you change the default value for this command and you are also using the **iprsvpsignallinghellorefreshmisses**command, ensure that the value for the **iprsvpsignallinghellograceful-restartrefreshmisses**command is less than the value for the **iprsvpsignallinghellorefreshmisses** command. Otherwise, some or all of the label-switched paths (LSPs) may not be recovered after a stateful switchover (SSO) has occurred. We recommend that the value for the**iprsvpsignallinghellorefreshmisses**command be twice the value for the **iprsvpsignallinghellograceful-restartrefreshmisses**command.

## Examples

In the following example, if the node does not receive five sequential hello acknowledgments, the node declares that its neighbor is down:

```
Router(config)# ip rsvp signalling hello graceful-restart refresh misses 5
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello graceful-restart dscp** | Sets the DSCP value in graceful restart hello messages. |
| **ip rsvp signalling hello graceful-restart refresh interval** | Sets the refresh interval in graceful restart hello messages. |
| **ip rsvp signalling refresh misses** | Specifies the number of successive refresh messages that can be missed before RSVP removes a state from the database. |
| **ip rsvp signalling hello refresh misses** | Specifies how many Hello acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down. |

# ip rsvp signalling hello graceful-restart send

To configure the time for Resource Reservation Protocol (RSVP) label switched paths (LSPs) in a Multiprotocol Label Switching (MPLS) traffic engineering (TE) network to recover or restart after a stateful switchover (SSO) occurs, use the **iprsvpsignallinghellograceful-restartsend** command in global configuration mode. To keep the default recovery and restart times, use the **no** form of this command.

**ip rsvp signalling hello graceful-restart send** {**recovery-time** *ms*| **restart-time** *ms*}

**no ip rsvp signalling hello graceful-restart send** {**recovery-time** *ms*| **restart-time** *ms*}

## Syntax Description

| | |
|---|---|
| **recovery-time** *ms* | Configures the time in milliseconds (ms) in outgoing hello messages to allow LSPs to recover after an SSO occurs. Values are 0 to 3600000. |
| **restart-time** *ms* | Configures the time in ms in outgoing hello messages to allow LSPs to restart after an SSO occurs. Values are 0 to 3600000. |

## Command Default

The default recovery and restart times of 120,000 and 30,000 ms, respecively, are in effect until you change them.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **iprsvpsignallinghellograceful-restartsend**command to give LSPs a longer time to recover or restart after an SSO occurs. Otherwise, the LSPs may not all come back up and your network performance is negatively affected.

## Examples

In the following example, a recovery time of 300,000 ms is configured:

```
Router(config)# ip rsvp signalling hello graceful-restart send recovery-time 300000
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello graceful-restart dscp** | Sets the DSCP value in the IP header of an RSVP TE graceful restart hello message. |
| **ip rsvp signalling hello graceful-restart mode** | Enables RSVP TE graceful restart capability on an RP. |
| **ip rsvp signalling hello graceful-restart neighbor** | Enables RSVP TE graceful restart capability on a neighboring router. |
| **ip rsvp signalling hello graceful-restart refresh interval** | Configures the RSVP TE refresh interval in graceful restart hello messages. |
| **ip rsvp signalling hello graceful-restart refresh misses** | Specifies how many sequential RSVP TE graceful restart hello acknowledgments a node can miss before the node considers communication with its neighbor lost. |

# ip rsvp signalling hello refresh interval

To configure the Resource Reservation Protocol (RSVP) traffic engineering (TE) hello refresh interval, use the **iprsvpsignallinghellorefreshinterval** command in interface configuration mode. To set the refresh interval to its default value, use the**no** form of this command.

**ip rsvp signalling hello [fast-reroute] refresh interval** *interval-value*

**no ip rsvp signalling hello [fast-reroute] refresh interval**

## Syntax Description

| | |
|---|---|
| **fast-reroute** | (Optional) Initiates Fast Reroute capability. |
| *interval-value* | Frequency, in milliseconds (msec), at which a node sends hello messages to a neighbor. Valid values are from 10 to 30000 msec.<br>**Note** Values below the default of 200 msec are not recommended, because they can cause RSVP Hellos to falsely detect a neighbor down event and unecessarily trigger Fast ReRoute. |

## Command Default

The default frequencyat which a node sends hello messages to a neighbor is 200 msec.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(22)S | This command was introduced. |
| 12.0(29)S | The optional **fast-reroute**keyword was added. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

You can configure the hello request interval on a per-interface basis. A node periodically generates a hello message containing a Hello Request object for each neighbor whose status is being tracked. The frequency of those hello messages is determined by the hello interval.

If you issue the **iprsvpsignallinghellorefreshinterval**command without the optional **fast-reroute**keyword, the command applies to Fast Reroute hellos. This command is provided for backward compatibility; however, we recommend that you use the **iprsvpsignallinghellofast-rerouterefreshinterval**command.

## Examples

In the following example, hello requests are sent to a neighbor every 5000 milliseconds and Fast Reroute capability is enabled by specifying the **fast-reroute** keyword:

```
Router(config-if)# ip rsvp signalling hello fast-reroute refresh interval 5000
```

In the following example, hello requests are sent to a neighbor every 5000 milliseconds and Fast Reroute capability is enabled by default:

```
Router(config-if)# ip rsvp signalling hello refresh interval 5000
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello dscp** | Sets the DSCP value in hello messages. |
| **ip rsvp signalling hello graceful-restart fresh interval** | Sets the refresh interval in graceful restart hello messages. |
| **ip rsvp signalling hello reroute refresh misses** | Sets the missed refresh limit in hello messages. |

# ip rsvp signalling hello refresh misses

To specify how many Resource Reservation Protocol (RSVP) traffic engineering (TE) hello acknowledgments a node can miss in a row before the node considers that communication with its neighbor is down, use the **iprsvpsignallinghellorefreshmisses** command in interface configuration mode. To return the missed refresh limit to its default value, use the **no** form of this command.

**ip rsvp signalling hello [fast-reroute] refresh misses** *msg-count*

**no ip rsvp signalling hello [fast-reroute] refresh misses**

## Syntax Description

| | |
|---|---|
| **fast-reroute** | (Optional) Initiates Fast Reroute capability. |
| *msg-count* | Number of sequential hello acknowledgments that a node can miss before RSVP considers the state expired and tears it down. Valid values are from 4 to 10. |

## Command Default

The default number of sequential hello acknowledgments is 4.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(22)S | This command was introduced. |
| 12.0(29)S | The optional **fast-reroute** keyword was added. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T |

## Usage Guidelines

A hello comprises a hello message, a Hello Request object, and a Hello ACK object. Each request is answered by an acknowledgment. If a link is very congested or a router has a very heavy load, set this number to a value higher than the default value to ensure that hello does not falsely declare that a neighbor is down.

If you issue the **iprsvpsignallinghellorefreshmisses**command without the optional **fast-reroute**keyword, the command applies to Fast Reroute hellos and Fast Reroute capability is enabled by default. This command is

provided for backward compatibility; however, we recommend that you use the **iprsvpsignallinghellofast-rerouterefreshmisses**command.

## Examples

In the following example, if the node does not receive five hello acknowledgments in a row, the node declares that its neighbor is down and Fast Reroute is enabled by specifying the **fast-reroute** keyword:

```
Router(config-if)# ip rsvp signalling hello fast-reroute refresh misses 5
```

In the following example, if the node does not receive five hello acknowledgments in a row, the node declares that its neighbor is down and Fast Reroute is enabled by default:

```
Router(config-if)# ip rsvp signalling hello refresh misses 5
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello dscp** | Sets the DSCP value in hello messages. |
| **ip rsvp signalling hello refresh interval** | Sets the refresh interval in hello messages. |

# ip rsvp signalling hello reroute dscp

To set the differentiated services code point (DSCP) value that is in the IP header of a Resource Reservation Protocol (RSVP) traffic engineering (TE) reroute hello (for state timeout) message sent from an interface, use the **iprsvpsignallinghelloreroutedscp** command in interface configuration mode. To set the DSCP value to its default, use the **no** form of this command.

**ip rsvp signalling hello reroute dscp** *num*

**no ip rsvp signalling hello reroute dscp**

## Syntax Description

| | |
|---|---|
| *num* | DSCP value. Valid values are from 0 to 63. |

## Command Default

The default DSCP value is 48.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(29)S | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

If a link is congested, you should set the DSCP to a value higher than 0 to reduce the likelihood that hello messages get dropped.

You configure the DSCP per interface, not per flow.

The DSCP applies to the RSVP hellos created on a specific interface. You can configure each interface independently for DSCP.

## Examples

In the following example, hello messages sent from this interface have a DSCP value of 30:

```
Router(config-if)# ip rsvp signalling hello reroute dscp 30
```

## Related Commands

| Command | Description |
|---|---|
| ip rsvp signalling hello reroute refresh interval | Sets the hello request interval in reroute hello messages. |
| ip rsvp signalling hello reroute refresh misses | Sets the missed refresh limit in reroute hello messages. |

# ip rsvp signalling hello reroute refresh interval

To configure the Resource Reservation Protocol (RSVP) traffic engineering (TE) reroute hello (for state timeout) refresh interval, use the **iprsvpsignallinghellorerouterefreshinterval** command in interface configuration mode. To set the refresh interval to its default value, use the**no** form of this command.

**ip rsvp signalling hello reroute refresh interval** *interval-value*

**no ip rsvp signalling hello reroute refresh interval**

## Syntax Description

| | |
|---|---|
| *interval-value* | Frequency, in milliseconds, at which a node sends hello messages to a neighbor. Valid values are from 1000 to 30000 (1 to 30 seconds). |

## Command Default

The default *frequency*at which a node sends hello messages to a neighbor is 1000 milliseconds (10 seconds).

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.0(29)S | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

You can configure the hello request interval on a per-interface basis. A node periodically generates a hello message containing a Hello Request object for each neighbor whose status is being tracked. The frequency of those hello messages is determined by the hello interval. For some routers, if you set the interval to a value less than the default value, CPU usage may be high.

## Examples

In the following example, hello requests are sent to a neighbor every 5000 milliseconds and Fast Reroute capability is enabled by default:

```
Router(config-if)# ip rsvp signalling hello reroute refresh interval 5000
```

## Related Commands

| Command | Description |
|---|---|
| ip rsvp signalling hello reroute refresh misses | Sets the missed refresh limit in reroute hello messages. |

# ip rsvp signalling hello reroute refresh misses

To specify how many Resource Reservation Protocol (RSVP) traffic engineering (TE) reroute hello (for state timeout) acknowledgments (ACKs) a node can miss in a row before the node considers communication with its neighbor is down, use the **iprsvpsignallinghellorerouterefreshmisses** command in interface configuration mode. To return the missed refresh limit to its default value, use the **no** form of this command.

**ip rsvp signalling hello reroute refresh misses** *msg-count*

**no ip rsvp signalling hello reroute refresh misses**

## Syntax Description

| | |
|---|---|
| *msg-count* | The number of sequential hello acknowledgments (ACKs) that a node can miss before RSVP considers the state expired and tears it down. Valid values are from 4 to 10. |

## Command Default

The default is 4.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(29)S | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

A hello comprises a hello message, a Hello Request object, and a Hello ACK object. Each request is answered by an acknowledgment. If a link is very congested or a router has a very heavy load, set this number to a value higher than the default value to ensure that hello does not falsely declare that a neighbor is down.

## Examples

In the following example, if the node does not receive five hello acknowledgments in a row, the node declares that its neighbor is down:

```
Router(config-if)# ip rsvp signalling hello reroute refresh misses 5
```

## Related Commands

| Command | Description |
|---|---|
| ip rsvp signalling hello reroute dscp | Sets the DSCP value in reroute hello messages. |

| Command | Description |
|---|---|
| ip rsvp signalling hello reroute refresh interval | Sets the refresh interval in reroute hello messages. |

# ip rsvp signalling hello statistics

To enable Hello statistics on the router, use the **iprsvpsignallinghellostatistics** command in global configuration mode. To disable Hello statistics on the router, use the **no** form of this command.

**ip rsvp signalling hello statistics**

**no ip rsvp signalling hello statistics**

## Syntax Description

This command has no arguments or keywords.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(22)S | This command was introduced. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Examples

In the following example, Hello statistics are enabled on the router:

```
Router(config)# ip rsvp signalling hello statistics
```

## Related Commands

| Command | Description |
|---|---|
| **clear ip rsvp hello instance statistics** | Clears Hello statistics for an instance. |
| **ip rsvp signalling hello (configuration)** | Enables Hello globally on the router. |
| **show ip rsvp hello statistics** | Displays how long Hello packets have been in the Hello input queue. |

# ip rsvp signalling initial-retransmit-delay

To configure the minimum amount of time that a Resource Reservation Protocol (RSVP)-configured router waits for an acknowledgment (ACK) message before retransmitting the same message, use the **iprsvpsignallinginitial-retransmit-delay** command in global configuration mode. To reset the delay value to its default, use the**no**form of this command.

**ip rsvp signalling initial-retransmit-delay** *delay-value*

**no ip rsvp signalling initial-retransmit-delay**

## Syntax Description

| | |
|---|---|
| *delay-value* | Minimum amount of time that a router waits for an ACK message before the first retransmission of the same message. The delay value ranges from 500 to 30,000 milliseconds (ms). |

## Command Default

The default value is 1000 ms (1.0 sec).

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |

## Usage Guidelines

Use the ip rsvp signalling initial-retransmit-delaycommand to configure the minimum amount of time that a router waits for an ACK message before retransmitting the same message.

If an ACK is not received for a state, the first retransmit occurs after the initial retransmit interval. If no ACK is received after the first retransmit, a second retransmit occurs. The message continues to be retransmitted, with the gap between successive retransmits being twice the previous interval, until an ACK is received. Then the message drops into normal refresh schedule if it needs to be refreshed (Path and Resv messages), or is processed (Error or Tear messages). If no ACK is received after five retransmits, the message is discarded as required.

## Examples

The following command shows how to set the initial-retransmit-delay to 2 seconds:

```
Router(config)# ip rsvp signalling initial-retransmit-delay 2000
```

The following command shows how to reset the initial-retransmit-delay to the default (1.0 sec):

```
Router(config)# no ip rsvp signalling initial-retransmit-delay
```

# ip rsvp signalling patherr state-removal

To reduce the amount of Resource Reservation Protocol (RSVP) traffic messages in a network, use the **iprsvpsignallingpatherrstate-removal** command in global configuration mode. To disable this function, use the **no** form of this command.

**ip rsvp signalling patherr state-removal** [**neighbor** *acl*]

**no ip rsvp signalling patherr state-removal**

## Syntax Description

| | |
|---|---|
| **neighbor** | (Optional) Adjacent routers that are part of a particular traffic engineering tunnel. |
| *acl* | (Optional) A simple access list with values from 1 to 99. |

## Command Default

Disabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |

## Usage Guidelines

Use the **iprsvpsignallingpatherrstate-removal**command to allow routers to delete Path state automatically when forwarding a PathError message, thereby eliminating the need for a subsequent PathTear message.

This command is most effective when all network nodes support this feature. All nodes need to have the latest version of Cisco IOS software configured.

This command applies only to label-switched path (LSP) flows.

## Examples

The following command shows how to enable **iprsvpsignallingpatherrstate-removal**:

```
Router(config)# ip rsvp signalling patherr state-removal
```

The following command shows how to disable **iprsvpsignallingpatherrstate-removal**:

```
Router(config)# no ip rsvp signalling patherr state-removal
```

The following command shows how to enable **iprsvpsignallingpatherrstate-removal** based on an access control list (ACL):

```
Router(config)# ip rsvp signalling patherr state-removal neighbor 98
```

The following command shows how to disable **iprsvpsignallingpatherrstate-removal** based on an ACL:

```
Router(config)# no ip rsvp signalling patherr state-removal neighbor 98
```

# ip rsvp signalling rate-limit

To control the transmission rate for Resource Reservation Protocol (RSVP) messages that are sent to a neighboring device during a specified amount of time, use the **ip rsvp signalling rate-limit** command in global configuration mode. To disable this function, use the **no** form of this command.

### Releases Before Cisco IOS Release 12.4(20)T

**ip rsvp signalling rate-limit** [**burst** *number*] [**maxsize** *bytes*] [**period** *ms*]

**no ip rsvp signalling rate-limit**

### Cisco IOS 12.0S Releases, 12.2S Releases, XE 2 Releases, Release 12.4(20)T, and Later T Releases

**ip rsvp signalling rate-limit** [**burst** *number*] [**limit** *number*] [**maxsize** *bytes*] [**period** *ms*]

**no ip rsvp signalling rate-limit**

## Syntax Description

| | |
|---|---|
| **burst** *number* | (Optional) Specifies the maximum number of RSVP messages that are sent to a neighboring device during each interval. Range is from 1 to 5000. Default is 8. |
| **maxsize** *bytes* | (Optional) Specifies the maximum size of the message queue, in bytes. Valid range is from 1 to 5000. Default is 2000. |
| **period** *ms* | (Optional) Specifies the length of time, in milliseconds (ms). Valid range is from 10 to 5000. Default is 20. |
| **limit** *number* | (Optional) Specifies the maximum number of messages to send per queue interval when the number of messages sent is less than the number of messages to be sent normally. Valid range is from 1 to 5000. Default is 37. |

## Command Default

If you do not enter this command, the default values are used.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. This command replaces the **ip rsvp msg pacing** command. |

| Release | Modification |
|---|---|
| 12.0(24)S | This command was modified. The **limit** keyword was added. |
| 12.0(29)S | This command was modified. The default argument values for the **burst** and **maxsize** keywords were increased to 8 messages and 2000 bytes, respectively. |
| 12.2(18)SXF5 | This command was integrated into Cisco IOS Release 12.2(18)SXF5. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| Cisco IOS XE Release 2.3 | This command was integrated into Cisco IOS XE Release 2.3. |
| 15.2(3)T | This command was modified. Support for IPv6 was added. |

## Usage Guidelines

Use the **ip rsvp signalling rate-limit** command to prevent a burst of RSVP traffic engineering signaling messages from overflowing the input queue of a receiving device, which would cause the device to drop some messages. Dropped messages substantially delay the completion of signaling.

This command replaces the **ip rsvp msg-pacing** command.

All configurations related to the **ip rsvp signalling rate-limit** command are applicable to both IPv4 and IPv6 sessions.

## Examples

The following command shows how six messages with a message queue of 500 bytes are sent every 10 ms to any neighboring device:

```
Device(config)# ip rsvp signalling rate-limit burst 6 maxsize 500 period 10
```

## Related Commands

| Command | Description |
|---|---|
| **clear ip rsvp signalling rate-limit** | Clears (sets to zero) the number of messages that were dropped because of a full queue. |
| **debug ip rsvp rate-limit** | Displays debug messages for RSVP rate-limiting events. |
| **show ip rsvp signalling rate-limit** | Displays the RSVP rate-limiting parameters. |

# ip rsvp signalling refresh interval

To specify the interval between sending refresh messages for each Resource Reservation Protocol (RSVP) state, use the **iprsvpsignallingrefreshinterval** command in global configuration mode. To set the interval to its default value, use the**no** form of the command.

**ip rsvp signalling refresh interval** *interval-value*

**no ip rsvp signalling refresh interval**

## Syntax Description

| | |
|---|---|
| *interval-value* | Time, in milliseconds, between sending refreshes for each RSVP state. The range is from 5000 to 4294967295 milliseconds; the default value is 30000. |

## Command Default

30000 milliseconds (30 seconds)

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.0(26)S | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(18)SXF5 | This command was integrated into Cisco IOS Release 12.2(18)SXF5. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| 15.0(1)M | This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M. |

## Usage Guidelines

Use the **iprsvpsignallingrefreshinterval** command to specify the interval between sending refresh messages for each RSVP state.

The RSVP protocol relies on a soft-state mechanism to maintain state consistency in the face of network losses. This mechanism is based on continuous refresh messages to keep a state current. Each RSVP router is responsible for sending periodic refresh messages to its neighbors.

**Note** If you change the default value for this command and you are also using the **iprsvpsignallinghellograceful-restartrefreshinterval** command, ensure that the value for the **iprsvpsignallinghellograceful-restartrefreshinterval** command is less than the value for the **iprsvpsignallingrefreshinterval** command. Otherwise, some or all of the label-switched paths (LSPs) may not be recovered after a stateful switchover (SSO) has occurred. We recommend that the value for the **iprsvpsignallingrefreshinterval** command be twice the value for the **iprsvpsignallinghellograceful-restartrefreshinterval** command.

## Examples

The following example shows how to specify a refresh interval of 60000 milliseconds (60 seconds):

```
Router(config)# ip rsvp signalling refresh interval 60000
```

The following example returns the refresh interval to the default value of 30 seconds:

```
Router(config)# no ip rsvp signalling refresh interval
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling refresh misses** | Specifies the number of successive refresh messages that can be missed before RSVP removes a state from the database. |

# ip rsvp signalling refresh misses

To specify the number of successive refresh messages that can be missed before Resource Reservation Protocol (RSVP) removes a state from the database, use the **iprsvpsignallingrefreshmisses** command in global configuration mode. To return the missed refresh limit to its default value, use the **no** form of this command.

**ip rsvp signalling refresh misses** *msg-count*

**no ip rsvp signalling refresh misses**

## Syntax Description

| | |
|---|---|
| *msg-count* | Number of successive refresh messages that can be missed before RSVP considers the state expired and tears it down. The range is 2 to 10. The default is 4. |

## Command Default

4 messages

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.0(26)S | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(18)SXF5 | This command was integrated into Cisco IOS Release 12.2(18)SXF5. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| 15.0(1)M | This command was integrated into a release earlier than Cisco IOS Release 15.0(1)M. |

## Usage Guidelines

Use the**iprsvpsignallingrefreshmisses**command to specify the number of successive refresh messages that can be missed before RSVP regards the router state as expired and removes that state from the database.

**Note** If you change the default value for this command and you are also using the **iprsvpsignallinghellograceful-restartrefreshmisses**command, ensure that the value for the **iprsvpsignallinghellograceful-restartrefreshmisses** command is less than the value for the **iprsvpsignallingrefreshmisses**command. Otherwise, some or all of the label-switched paths (LSPs) may not be recovered after a stateful switchover (SSO) has occurred. We recommend that the value for the **iprsvpsignallingrefreshmisses**command be twice the value for the **iprsvpsignallinghellograceful-restartrefreshmisses**command.

## Examples

The following example shows how to specify a missed refresh limit of 6 messages:

```
Router(config)# ip rsvp signalling refresh misses 6
```

The following example shows how to return the refresh misses limit to the default value of 4:

```
Router(config)# no ip rsvp signalling refresh misses
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling refresh interval** | Specifies the interval between sending refresh messages for each RSVP state. |

# ip rsvp signalling refresh reduction

To enable Resource Reservation Protocol (RSVP) refresh reduction, use the**iprsvpsignallingrefreshreduction** command in global configuration mode. To disable refresh reduction, use the **no** form of this command.

**ip rsvp signalling refresh reduction**

**no ip rsvp signalling refresh reduction**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |

## Usage Guidelines

RSVP refresh reduction is a set of extensions to reduce the messaging load imposed by RSVP and to help it scale to support larger numbers of flows.

The following features of the refresh reduction standard (RFC 2961) are supported and will be turned on with this command:

- Setting the refresh-reduction-capable bit in message headers
- Message-Identifier (ID) usage
- Reliable messaging with rapid retransmit, acknowledgement (ACK) messages, and MESSAGE_ID objects
- Summary refresh extension
- Bundle messages (reception only)

Refresh reduction requires the cooperation of the neighbor to operate; for this purpose, the neighbor must also support the standard. If the router detects that a directly connected neighbor is not supporting the refresh reduction standard (either through observing the refresh-reduction-capable bit in messages received from the next hop, or by sending a MESSAGE_ID object to the next hop and receiving an error), refresh reduction will not be used on this link irrespective of this command.

## Examples

The following command shows how to enable RSVP refresh reduction:

```
Router(config)# ip rsvp signalling refresh reduction
```

The following command shows how to disable RSVP refresh reduction:

```
Router(config)# no ip rsvp signalling refresh reduction
```

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp interface** | Displays RSVP-related interface information. |
| **show ip rsvp signalling refresh reduction** | Displays refresh-reduction parameters for RSVP messages. |

# ip rsvp signalling refresh reduction ack-delay

To configure the maximum amount of time that a Resource Reservation Protocol (RSVP)-configured router holds on to an acknowledgment (ACK) message before sending it, use the**iprsvpsignallingrefreshreductionack-delay**command in global configuration mode. To reset the ack-delay value to its default, use the **no**form of this command.

**ip rsvp signalling refresh reduction ack-delay** *delay-value*

**no ip rsvp signalling refresh reduction ack-delay**

## Syntax Description

| | |
|---|---|
| *delay-value* | Maximum amount of time that a router holds on to an ACK message before sending it. Values range from 100 to 10000 milliseconds (ms). |

## Command Default

The default value is 250 ms (0.25 sec).

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |

## Usage Guidelines

Use the **iprsvpsignallingrefreshreductionack-delay**command to configure the maximum amount of time that an RSVP-configured router keeps an ACK message before sending it.

## Examples

The following command shows how to set the ack-delay value to 1 second:

```
Router(config)# ip rsvp signalling refresh reduction ack-delay 1000
```

The following command shows how to set the ack-delay value to the default value:

```
Router(config)# no ip rsvp signalling refresh reduction ack-delay
```

# ip rsvp snooping

To enable Resource Reservation Protocol (RSVP) snooping in a specific set of VLANs, use the **ip rsvp snooping** command in global configuration mode. To disable RSVP snooping, use the **no** form of this command.

**ip rsvp snooping** [**vlan** *vlan-id* | **vlan-range** *vlan-id-start vlan-id-end*]

**no ip rsvp snooping** [**vlan** *vlan-id* | **vlan-range** *vlan-id-start vlan-id-end*]

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) Specifies the VLAN in which RSVP snooping must be enabled. |
| **vlan-range** *vlan-id-start vlan-id-end* | (Optional) Specifies a range of VLANs in which RSVP snooping must be enabled. |

## Command Default

RSVP snooping is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(44)SE | This command was introduced. |

## Usage Guidelines

Use the **ip rsvp snooping** command to enable or disable RSVP snooping in a specific VLAN or range of VLANs. Specifying VLANs is optional. The keyword argument pairs **vlan** *vlan-id* and **vlan-range** *vlan-id-start vlan-id-end* are visible only on platforms that support per-VLAN snooping. If you do not specify VLAN details, snooping is enabled on all VLANs. Using this command more than once will not disable the previous configurations. In the event of creating a new VLAN, if RSVP snooping is enabled on all VLANs, RSVP snooping will be enabled on the new VLAN too. If you use the **no ip rsvp snooping** command without specifying any VLANs, RSVP snooping will be disabled in all VLANs.

## Examples

The following example shows how to enable RSVP snooping in a specific VLAN:

```
Device> enable
Device# configure terminal
Device(config)# ip rsvp snooping vlan 10
```

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp snooping** | Displays the list of VLANs in which RSVP snooping is enabled. |

# ip rsvp source

To configure a Resource Reservation Protocol (RSVP) router to populate an address other than the native interface address in the previous hop (PHOP) address field of the PHOP object when forwarding a PATH message onto that interface, use the **iprsvpsource** command in interface configuration mode. To keep the native interface address in the PHOP address field, use the **no** form of this command.

**ip rsvp source** {**address** *ip-address*| **interface** *type number*}

**no ip rsvp source**

## Syntax Description

| | |
|---|---|
| **address** *ip-address* | IP address for the PHOP address field. |
| **interface** *type number* | Interface type and number that is used as the source for the PHOP address field. |

## Command Default

The native interface address is written in the PHOP address field.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |
| 12.2(33)SRE | This command was integrated into Cisco IOS Release 12.2(33)SRE. |

## Examples

The following example configures IP address 10.1.3.13 for the PHOP address field:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface ethernet 0/0
Router(config-if)# ip rsvp bandwidth
Router(config-if)# ip rsvp source address 10.1.3.13
Router(config-if)# end
```

The following example configures loopback interface 0 as the interface whose address is used in the PHOP address field:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface ethernet 1/0
Router(config-if)# ip rsvp bandwidth
Router(config-if)# ip rsvp source interface loopback 0
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp interface** | Displays RSVP-related information. |

# ip rsvp svc-required

To enable creation of a switched virtual circuit (SVC) to service any new Resource Reservation Protocol (RSVP) reservation made on the interface or subinterface of an Enhanced ATM port adapter (PA-A3), use the **iprsvpsvc-required** command in interface configuration mode. To disable SVC creation for RSVP reservations, use the **no** form of this command.

**ip rsvp svc-required**

**no ip rsvp svc-required**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command applies exclusively to the RSVP-ATM QoS Interworking feature.

Usually reservations are serviced when RSVP classifies packets and a queueing mechanism schedules them for transmission to manage congestion. Traditionally, RSVP is used with weighted fair queueing (WFQ). When RSVP is coupled with WFQ, all of the packets visible to WFQ are also visible to RSVP, which allows RSVP to identify and take action on packets important to it. In this case, WFQ provides bandwidth guarantees.

However, when the **iprsvpsvc-required** command is used to configure an interface or subinterface, a new SVC is established and used to service each new reservation on the interface. ATM SVCs are used to provide bandwidth guarantees and NetFlow is used on input interfaces to make data packets visible to RSVP.

**Note** When RSVP is enabled, all packets are processed by the Route Switch Processor (RSP).

This command must be executed on both ends of an SVC driven by RSVP. This command is supported only for the Enhanced ATM port adapter (PA-A3) and its subinterfaces.

**Note** For this command to take effect, NetFlow must be enabled. Therefore, the **iproute-cacheflow** command must precede this command in the configuration.

Use the **showiprsvpinterface** command to determine whether this command is in effect for any interface or subinterface.

## Examples

The following example signals RSVP that reservations made on ATM interface 2/0/0 will be serviced by creation of an SVC:

```
interface atm2/0/0
 ip rsvp svc-required
```

## Related Commands

| Command | Description |
|---|---|
| **ip route-cache flow** | Enables NetFlow switching for IP routing. |
| **ip rsvp atm-peak-rate-limit** | Sets a limit on the peak cell rate of reservations for all newly created RSVP SVCs established on the current interface or any of its subinterfaces. |
| **ip rsvp precedence** | Allows you to set the IP Precedence values to be applied to packets that either conform to or exceed the RSVP flowspec. |
| **show ip rsvp interface** | Displays RSVP-related interface information. |

# ip rsvp tos

To enable the router to mark the five low-order type of service (ToS) bits of the IP header ToS byte for packets in a Resource Reservation Protocol (RSVP) reserved path using the specified values for traffic that either conforms to or exceeds the RSVP flowspec, use the **iprsvptos** command in interface configuration mode. To remove existing settings for the ToS bits, use the **no** form of this command; if neither the **conform**nor **exceed** keyword is specified, all settings for the ToS bits are removed.

**ip rsvp tos conform** *tos-value* **exceed** *tos-value*

**no ip rsvp tos [conform] [exceed]**

## Syntax Description

| | |
|---|---|
| **conform** *tos-value* | Specifies a ToS value in the range from 0 to 31 for traffic that conforms to the RSVP flowspec. The ToS value is written to the five low-order bits (bits 0 to 4) of the ToS byte in the IP header of a packet. Either the **conform** or **exceed** keyword is required; both keywords may be specified.<br>When used with the **no** form of the command, the **conform** keyword is optional. |
| **exceed** *tos-value* | (Optional) Specifies a ToS value in the range from 0 to 31 for traffic that exceeds the RSVP flowspec. The ToS byte value is written to the five low-order bits (bits 0 to 4) of the ToS byte in the IP header of a packet. Either the **conform** or **exceed** keyword is required; both keywords may be specified.<br>When used with the **no** form of the command, the **exceed** keyword is optional. |

## Command Default

The ToS bits of the ToS byte are left unmodified when this command is not used. (The default behavior is equivalent to use of the **noiprsvptos** command.)

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

| Release | Modification |
|---|---|
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Packets in an RSVP reserved path are divided into two classes: those that conform to the reservation flowspec and those that correspond to a reservation but that exceed, or are outside, the reservation flowspec.

The **iprsvptos** command allows you to set the ToS values to be applied to packets belonging to these two classes. You must specify the ToS value for at least one class of traffic when you use this command. You can use a single instance of the command to specify values for both classes, in which case you can specify the **conform** and **exceed** keywords in either order.

As part of its input processing, RSVP uses the **iprsvptos** command configuration to set the ToS bits of the ToS byte on conforming and nonconforming packets. If per-virtual circuit (VC) VIP-distributed Weighted Random Early Detection (DWRED) is configured, the system uses the ToS bit and IP Precedence bit settings on the output interface in its packet drop process. The ToS bit and IP Precedence bit settings of a packet can also be used by interfaces on downstream routers.

Execution of the **iprsvptos** command causes ToS bit values for all preexisting reservations on the interface to be modified.

**Note** RSVP must be enabled on an interface before you can use this command; that is, use of the **iprsvpbandwidth** command must precede use of the **iprsvptos** command. RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

**Note** The **iprsvptos** command sets bits 0 to 4 so that in combination with the IP Precedence bit settings every bit in the ToS byte is set. Use of these bits is made with full knowledge of the fact that certain canonical texts that address the ToS byte specify that only bits 1 to 4 are used as the ToS bits.

RSVP receives packets from the underlying forwarding mechanism. Therefore, to use the **iprsvptos** command to set the ToS bits, one of the following features is required:

- Weighted fair queueing (WFQ) must be enabled on the interface.
- RSVP switched virtual circuits (SVCs) must be used.
- NetFlow must be configured to assist RSVP.

**Note** Use of the **no** form of this command is not equivalent to giving the**iprsvptos0**command, which sets all precedence on the packets to 0, regardless of previous precedence setting.

## Examples

The following example sets the ToS bits value to 4 for all traffic on ATM interface 1 that conforms to the RSVP flowspec. ToS bits on packets exceeding the flowspec are not altered.

```
interface atm1
 ip rsvp tos conform 4
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp bandwidth** | Enables RSVP for IP on an interface. |
| **ip rsvp flow-assist** | Enables RSVP to attach itself to NetFlow so that it can leverage NetFlow services. |
| **ip rsvp policy cops minimal** | Lowers the COPS server's load and improves latency times for messages on the governed router. |
| **show ip rsvp** | Displays the IP Precedence and ToS bit values to be applied to packets that either conform to or exceed the RSVP flowspec for a given interface. |

# ip rsvp transport

To create a Resource Reservation Protocol (RSVP) transport session, use the **iprsvptransport** command in global configuration mode. To disable the RSVP transport session, use the **no** form of this command.

**ip rsvp transport** {**client** *client-id*| **statistics**}

**no ip rsvp transport** {**client** *client-id*| **statistics**}

## Syntax Description

| | |
|---|---|
| **client** | Initiates RSVP transport client. |
| *client-id* | Client identifier. The range is from 1 to 65535. |
| **statistics** | Configures RSVP transport protocol (TP) information buffer size. |

## Command Default

RSVP is configured as transport protocol.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(3)T | This command was introduced. |
| 15.1(1)S | This command was integrated into Cisco IOS Release 15.1(1)S. |

## Usage Guidelines

You can use the **iprsvptransport** command to configure RSVP to be used as transport mechanism for the clients. The *client-id* is used for identification of the client that initiates the RSVP as a transport protocol. The **statistics** keyword is used to record statistics for RSVP TP sessions. The statistics recorded includes information passed by RSVP to the RSVP TP client as part of callback. The maximum amount of information that can be recorded is 32 MB.

The **iprsvptransport** command enables a router to simulate a host generating RSVP PATH message. This command is used for testing and debugging purposes.

## Examples

The following example shows how to identify a client to establish an RSVP transport session:

```
Router> enable
Router# configure terminal
Router(config)# ip rsvp transport client 12
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp transport sender-host** | Registers a transport client ID with RSVP. |

# ip rsvp transport sender-host

To register a transport client ID with Resource Reservation Protocol (RSVP), use the **iprsvptransportsender-host** command in global configuration mode. To disable the static RSVP host path configuration, use the **no** form of this command.

**ip rsvp transport sender-host** [**tcp**| **udp**] *destination-address source-address ip-protocol dest-port source-port client-id init-id instance-id* [**vrf** *vrf-name*] [**data** *data-value*]

**no ip rsvp transport sender-host** [**tcp**| **udp**] *destination-address source-address ip-protocol dest-port source-port client-id init-id instance-id* [**vrf** *vrf-name*] [**data** *data-value*]

## Syntax Description

| | |
|---|---|
| **tcp** | (Optional) Specifies TCP to be used as transport mechanism. |
| **udp** | (Optional) Specifies User Datagram Protocol (UDP) to be used as transport mechanism. |
| *destination-address* | Destination address to where the PATH message is sent. |
| *source-address* | Source address from where the PATH message is sent. |
| *ip-protocol* | Identifier for configuring RSVP as a transport protocol. The range is from 0 to 255. |
| *dest-port* | Destination port to which the PATH message is sent. |
| *source-port* | Source port from which the PATH message is sent. |
| *client-id* | Identifier that initiates RSVP client. |
| *init-id* | Hostname or IP address that identifies the node initiating the transport service request. |
| *instance-id* | Instance ID that identifies the transport service request from a particular client application and from a particular initiator. The range is from 1 to 65535. |
| **vrf** *vrf-name* | (Optional) Configures VPN Routing and Forwarding (VRF) instance on the RSVP client. |
| **data** *data-value* | (Optional) Configures the RSVP transport data value. |

## Command Default

The static RSVP host path is configured.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(3)T | This command was introduced. |
| 15.1(1)S | This command was integrated into Cisco IOS Release 15.1(1)S. |

## Usage Guidelines

Use the **iprsvptransportsender-host** command to configure the RSVP transport proxy path. When this command is configured, RSVP sends PATH messages downstream.

## Examples

The following example shows how to configure an RSVP sender host path:

```
Router> enable
Router# configure terminal
Router(config)# ip rsvp transport sender-host 10.1.1.1 10.2.1.1 2 3 4 3 192.168.1.2 2 vrf
vrf1 data d1
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp transport** | Configures RSVP as transport protocol. |

# ip rsvp tunnel overhead-percent

To manually override the Resource Reservation Protocol (RSVP) percentage bandwidth, use the **iprsvptunneloverhead-percent**command in interface configuration mode. To restore the tunnel overhead percentage to its default values, use the **no** form of this command.

**ip rsvp tunnel overhead-percent** *percentage*

**no ip rsvp tunnel overhead-percent**

## Syntax Description

| | |
|---|---|
| *percentage* | Percentage overhead on the tunnel. |

## Command Default

The percentage overhead for generic routing encapsulation (GRE) or multipoint generic routing encapsulation (mGRE) interfaces is 4 percent. The percentage overhead for GRE and mGRE with IPsec interfaces ranges from 4 to 15 percent, with an average of 10 percent.

## Command Modes

Interface configuration mode (config-if)

## Command History

| Release | Modification |
|---|---|
| 15.1(2)T | This command was introduced. |
| 15.1(1)S | This command was integrated into Cisco IOS Release 15.1(1)S. |

## Usage Guidelines

During the bandwidth admission control, the Cisco IOS software must consider the additional IP overhead introduced because of tunneling and a possible encryption over these tunnels. The default values for the overhead depends on the average size of an Internet packet. However, you can manually override the default values by using the **iprsvptunneloverhead-percent**command.

For example, when the Cisco IOS software gets a reservation request for 100 bytes, and if the outbound interface is a GRE or an mGRE interface, then a bandwidth reservation request for 104 bytes is made available locally on that tunnel interface. In case the GRE or mGRE interface is in protected mode, 110 bytes is requested on the respective link. This IP overhead does not affect the bandwidth signaled via RSVP.

## Examples

The following example shows how to configure the router to manually override the percentage bandwidth:

```
Router(config)# interface tunnel 1
Router(config-if)# ip rsvp tunnel overhead-percent 20
```

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp interface detail** | Displays the hello configuration for all interfaces. |

# ip rsvp udp-multicasts

To instruct the router to generate User Datagram Protocol (UDP)-encapsulated Resource Reservation Protocol (RSVP) multicasts whenever it generates an IP-encapsulated multicast packet, use the **iprsvpudp-multicasts**command in interface configuration mode. To disable this function, use the **no** form of this command.

**ip rsvp udp-multicasts** [ *multicast-address* ]

**no ip rsvp udp-multicasts** [ *multicast-address* ]

## Syntax Description

| | |
|---|---|
| *multicast-address* | (Optional) Host name or UDP multicast address of router. |

## Command Default

The generation of UDP multicasts is disabled. If a system sends a UDP-encapsulated RSVP message to the router, the router begins using UDP for contact with the neighboring system. The router uses multicast address 224.0.0.14 and starts sending to UDP port 1699. If the command is entered with no specifying multicast address, the router uses the same multicast address.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use this command to instruct a router to generate UDP-encapsulated RSVP multicasts whenever it generates an IP-encapsulated multicast packet. Some hosts require this trigger from the router.

RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

## Examples

The following example reserves up to 7500 kbps on Ethernet interface 2, with up to 1 Mbps per flow. The router is configured to use UDP encapsulation with the multicast address 224.0.0.14.

```
interface ethernet 2
 ip rsvp bandwidth 7500 1000
 ip rsvp udp-multicasts 224.0.0.14
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp bandwidth** | Enables RSVP for IP on an interface. |
| **ip rsvp neighbor** | Enables neighbors to request a reservation. |
| **ip rsvp reservation** | Enables a router to simulate receiving and forwarding RSVP RESV messages. |
| **ip rsvp sender** | Enables a router to simulate receiving and forwarding RSVP PATH messages. |

# ip rsvp udp neighbor

To enable neighbor routers to process and send Resource Reservation Protocol (RSVP) control packets over UDP, use the **ip rsvp udp neighbor** command in global configuration mode. To disable neighbor routers to process and send RSVP control packets over UDP, use the **no** form of the command.

**ip rsvp udp neighbor** *neighbor-IP-address* **router** [**vrf** *vrf-name*]

**no ip rsvp udp neighbor** *neighbor-IP-address* **router** [**vrf** *vrf-name*]

## Syntax Description

| | |
|---|---|
| *neighbor-IP-address* | IP address of the neighbor router. |
| **router** | Specifies that the neighbor is a router. |
| **vrf** *vrf-name* | (Optional). Specifies the Virtual Routing and Forwarding (VRF) instance name. |

## Command Default

The **ip rsvp udp neighbor** command is disabled by default.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(4)M | This command was introduced. |

## Usage Guidelines

The **ip rsvp udp neighbor** command can be used to enable a neighbor router to communicate to the first hop router over UDP and not raw IP. Also, this command can be used in a scenario where a firewall that is located in between two routers drops raw IP packets due to security concerns, but allows UDP packets.

## Examples

The following example shows how to enable a neighbor router with IP address 10.1.1.1 to process and send RSVP control packets over UDP:

```
Device> enable
Device# configure terminal
Device(config)# ip rsvp udp neighbor 10.1.1.1 router vrf vrf-1
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp bandwidth** | Enables RSVP for an IP on an interface. |

# ip rtp compression-connections

To specify the total number of Real-Time Transport Protocol (RTP) header compression connections that can exist on an interface, use the **iprtpcompression-connections**command in interface configuration mode. To restore the default value, use the **no** form of this command.

**ip rtp compression-connections** *number*

**no ip rtp compression-connections**

## Syntax Description

| | |
|---|---|
| *number* | Number of RTP header compression connections the cache supports, in the range from 3 to 1000. |

## Command Default

For PPP and High-Level Data Link Control (HDLC) interfaces, the default is 16 compression connections.

For Frame Relay interfaces, the default is 256 compression connections.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |
| 12.0(7)T | For PPP and HDLC interfaces, the maximum number of compression connections increased from 256 to 1000.<br>For Frame Relay interfaces, the maximum number of compression connections increased from 32 to 256. The default number of compression connections was increased from 32 (fixed) to 256 (configurable). |
| 12.1(4)E | This command was implemented on the Cisco 7100 series. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

You should configure one connection for each RTP call through the specified interface.

Each connection sets up a compression cache entry, so you are in effect specifying the maximum number of cache entries and the size of the cache. Too few cache entries for the specified interface can lead to degraded performance, and too many cache entries can lead to wasted memory.

**Note** Both ends of the serial connection must use the same number of cache entries.

## Examples

The following example changes the number of RTP header compression connections supported to 150:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression
Router(config-if)# ip rtp compression-connections 150
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **ip rtp header-compression** | Enables RTP header compression. |
| **show ip rtp header-compression** | Displays RTP header compression statistics. |

# ip rtp header-compression

To enable Real-Time Transport Protocol ( RTP) header compression, use the **iprtpheader-compression**command in interface configuration mode. To disable RTP header compression, use the **no** form of this command.

**ip rtp header-compression** [**passive**| **iphc-format**| **ietf-format**] **[periodic-refresh]**

**no ip rtp header-compression** [**passive**| **iphc-format**| **ietf-format**] **[periodic-refresh]**

## Syntax Description

| | |
|---|---|
| **passive** | (Optional) Compresses outgoing RTP packets only if incoming RTP packets on the same interface are compressed. If you do not specify the **passive** keyword, all RTP packets are compressed. |
| **iphc-format** | (Optional) Indicates that the IP Header Compression (IPHC) format of header compression will be used. |
| **ietf-format** | (Optional) Indicates that the Internet Engineering Task Force (IETF) format of header compression will be used. |
| **periodic-refresh** | (Optional) Indicates that the compressed IP header will be refreshed periodically. |

## Command Default

Disabled

For PPP interfaces, the default format for header compression is the IPHC format.

For High-Level Data Link Control (HDLC) and Frame Relay interfaces, the default format for header compression is the original proprietary Cisco format. The maximum number of compression connections for the proprietary Cisco format is 256.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |
| 12.0 | This command was integrated into Cisco IOS Release 12.0. This command was modified to include the **iphc-format** keyword. |
| 12.3(2)T | This command was integrated into Cisco IOS Release 12.3(2)T. This command was modified to include the **periodic-refresh** keyword. |

| Release | Modification |
|---|---|
| 12.3(4)T | This command was modified to include the **ietf-format** keyword. |
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

### Compressing Headers

You can compress IP/User Datagram Protocol (UDP)/RTP headers to reduce the size of your packets. Compressing headers is especially useful for RTP because RTP payload size can be as small as 20 bytes, and the uncompressed header is 40 bytes.

### The passive Keyword

By default, the **iprtpheader-compression** command compresses outgoing RTP traffic. If you specify the **passive** keyword, outgoing RTP traffic is compressed only if *incoming* RTP traffic on the *same* interface is compressed. If you do not specify the **passive** keyword, *all* outgoing RTP traffic is compressed.

The **passive** keyword is ignored on PPP interfaces. PPP interfaces negotiate the use of header-compression, regardless of whether the **passive** keyword is specified. Therefore, on PPP interfaces, the **passive** keyword is replaced by the IPHC format, the default format for PPP interfaces.

### The iphc-format Keyword

The **iphc-format** keyword indicates that the IPHC format of header compression that will be used. For PPP and HDLC interfaces, when the **iphc-format** keyword is specified, TCP header compression is also enabled. For this reason, the **iptcpheader-compression** command appears in the output of the **showrunning-config** command. Since both RTP header compression and TCP header compression are enabled, both UDP packets and TCP packets are compressed.

The **iphc-format** keyword includes checking whether the destination port number is even and is in the ranges of 16,385 to 32,767 (for Cisco audio) or 49,152 to 65,535 (for Cisco video). Valid RTP packets that meet the criteria (that is, the port number is even and is within the specified range) are compressed using the compressed RTP packet format. Otherwise, packets are compressed using the less-efficient compressed non-TCP packet format.

The **iphc-format** keyword is not available for interfaces that use Frame Relay encapsulation.

**Note** The header compression format (in this case, IPHC) must be the same at *both* ends of the network. That is, if you specify the **iphc-format** keyword on the local router, you must also specify the **iphc-format** keyword on the remote router.

### The ietf-format Keyword

The **ietf-format**keyword indicates that the IETF format of header compression will be used. For HDLC interfaces, the**ietf-format**keyword compresses only UDP packets. For PPP interfaces, when the **ietf-format** keyword is specified, TCP header compression is also enabled. For this reason, the **iptcpheader-compression**

command appears in the output of the **showrunning-config** command. Since both RTP header compression and TCP header compression are enabled, both UDP packets and TCP packets are compressed.

With the **ietf-format** keyword, any even destination port number higher than 1024 can be used. Valid RTP packets that meet the criteria (that is, the port number is even and is higher than 1024) are compressed using the compressed RTP packet format. Otherwise, packets are compressed using the less-efficient compressed non-TCP packet format.

The **ietf-format** keyword is not available for interfaces that use Frame Relay encapsulation.

**Note** The header compression format (in this case, IETF) must be the same at *both* ends of the network. That is, if you specify the **ietf-format**keyword on the local router, you must also specify the **ietf-format** keyword on the remote router.

**Support for Serial Lines**

RTP header compression is supported on serial lines using Frame Relay, HDLC, or PPP encapsulation. You must enable compression on both ends of a serial connection.

**Unicast or Multicast RTP Packets**

This command can compress unicast or multicast RTP packets, and, hence, multicast backbone (MBONE) traffic can also be compressed over slow links. The compression scheme is beneficial only when you have small payload sizes, as in audio traffic.

**Custom or Priority Queueing**

When you use the**iprtpheader-compression** command and configure custom or priority queueing on an encapsulated HDLC or Frame Relay interface, the compressed packets may go to the default queue instead of the user-defined queue, which results in protocol flaps (loss of keepalives). Therefore, we recommend that you use the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) model for configuring QoS features.

## Examples

The following example enables RTP header compression on the Serial1/0 interface and limits the number of RTP header compression connections to 10. In this example, the optional **iphc-format** keyword of the**iprtpheader-compression**command is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression iphc-format
Router(config-if)# ip rtp compression-connections 10
Router(config-if)# end
```

The following example enables RTP header compression on the Serial2/0 interface and limits the number of RTP header compression connections to 20. In this example, the optional **ietf-format** keyword of the**iprtpheader-compression**command is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression ietf-format
Router(config-if)# ip rtp compression-connections 20
Router(config-if)# end
```

In the following example, RTP header compression is enabled on the Serial1/0 interface and the optional **periodic-refresh** keyword of the**iprtpheader-compression**command is specified:

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0
Router(config-if)# encapsulation ppp
Router(config-if)# ip rtp header-compression iphc-format periodic-refresh
Router(config-if)# ip rtp compression-connections 10
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **clear ip rtp header-compression** | Clears RTP header compression structures and statistics. |
| **ip rtp compression-connections** | Specifies the total number of RTP header compression connections that can exist on an interface. |
| **show ip rtp header-compression** | Displays RTP header compression statistics. |
| **show running-config** | Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information. |

# ip rtp priority

**Note** Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **iprtppriority**command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

**Note** Effective with Cisco IOS XE Release 3.2S, the **iprtppriority**command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To reserve a strict priority queue for a set of Real-Time Transport Protocol (RTP) packet flows belonging to a range of User Datagram Protocol (UDP) destination ports, use the **iprtppriority** command in interface configuration mode. To disable the strict priority queue, use the **no** form of this command.

**ip rtp priority** *starting-rtp-port-number port-number-range bandwidth*

**no ip rtp priority**

## Syntax Description

| | |
|---|---|
| *starting-rtp-port-number* | The starting RTP port number. The lowest port number to which the packets are sent. The port number can be a number from 2000 to 65,535. |
| *port-number-range* | The range of UDP destination ports. Number, when added to the *starting-rtp-port-number*argument, that yields the highest UDP port number. The range of UDP destination ports is from 0 to 16,383. |
| *bandwidth* | Maximum allowed bandwidth, in kbps. The maximum allowed bandwidth is from 0 to 2000. |

## Command Default

Disabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.6 | This command was modified. This command was hidden. |
| 15.0(1)S | This command was modified. This command was hidden. |
| 15.1(3)T | This command was modified. This command was hidden. |
| Cisco IOS XE Release 3.2S | This command was replaced by an MQC command (or sequence of MQC commands). |

## Usage Guidelines

This command is most useful for voice applications, or other applications that are delay-sensitive.

This command extends and improves on the functionality offered by the **iprtpreserve** command by allowing you to specify a range of UDP/RTP ports whose voice traffic is guaranteed strict priority service over any other queues or classes using the same output interface. Strict priority means that if packets exist in the priority queue, they are dequeued and sent first--that is, before packets in other queues are dequeued. We recommend that you use the **iprtppriority** command instead of the **iprtpreserve** command for voice configurations.

This command can be used in conjunction with either weighted fair queueing (WFQ) or class-based WFQ (CBWFQ) on the same outgoing interface. In either case, traffic matching the range of ports specified for the priority queue is guaranteed strict priority over other CBWFQ classes or WFQ flows; voice packets in the priority queue are always serviced first.

Remember the following guidelines when using the **iprtppriority** command:

- When used in conjunction with WFQ, the **iprtppriority** command provides strict priority to voice, and WFQ scheduling is applied to the remaining queues.
- When used in conjunction with CBWFQ, the **iprtppriority** command provides strict priority to voice. CBWFQ can be used to set up classes for other types of traffic (such as Systems Network Architecture [SNA]) that need dedicated bandwidth and need to be treated better than best effort and not as strict priority; the nonvoice traffic is serviced fairly based on the weights assigned to the enqueued packets. CBWFQ can also support flow-based WFQ within the default CBWFQ class if so configured.

Remember the following guidelines when configuring the *bandwidth* argument:

- It is always safest to allocate to the priority queue slightly more than the known required amount of bandwidth, to allow room for network bursts.
- The IP RTP Priority admission control policy takes RTP header compression into account. Therefore, while configuring the *bandwidth* argument of the **iprtppriority** command you need to configure only

for the bandwidth of the compressed call. Because the *bandwidth* argument is the maximum total bandwidth, you need to allocate enough bandwidth for all calls if there will be more than one call.

- Configure a bandwidth that allows room for Layer 2 headers. The bandwidth allocation takes into account the payload plus the IP, UDP, and RTP headers but does not account for Layer 2 headers. Allowing 25 percent bandwidth for other overhead is conservative and safe.
- The sum of all bandwidth allocation for voice and data flows on an interface cannot exceed 75 percent of the total available bandwidth, unless you change the default maximum reservable bandwidth. To change the maximum reservable bandwidth, use the **max-reserved-bandwidth** command on the interface.

For more information on IP RTP Priority bandwidth allocation, refer to the section "IP RTP Priority" in the chapter "Congestion Management Overview" in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

## Examples

The following example first defines a CBWFQ configuration and then reserves a strict priority queue with the following values: a starting RTP port number of 16384, a range of 16383 UDP ports, and a maximum bandwidth of 40 kbps:

```
! The following commands define a class map:
class-map class1
 match access-group 101
 exit
! The following commands create and attach a policy map:
policy-map policy1
class class1
 bandwidth 3000
 queue-limit 30
 random-detect
 random-detect precedence 0 32 256 100
 exit
interface Serial1
 service-policy output policy1
! The following command reserves a strict priority queue:
 ip rtp priority 16384 16383 40
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth (policy-map class)** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map. |
| **fair queue (WFQ)** | Enables WFQ for an interface. |
| **frame-relay ip rtp priority** | Reserves a strict priority queue on a Frame Relay PVC for a set of RTP packet flows belonging to a range of UDP destination ports. |
| **ip rtp reserve** | Reserves a special queue for a set of RTP packet flows belonging to a range of UDP destination ports. |
| **max-reserved-bandwidth** | Changes the percent of interface bandwidth allocated for CBWFQ, LLQ, and IP RTP Priority. |

| Command | Description |
|---|---|
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **ppp multilink** | Enables MLP on an interface and, optionally, enables dynamic bandwidth allocation. |
| **ppp multilink fragment-delay** | Configures a maximum delay allowed for transmission of a packet fragment on an MLP bundle. |
| **ppp multilink interleave** | Enables interleaving of RTP packets among the fragments of larger packets on an MLP bundle. |
| **priority** | Gives priority to a class of traffic belonging to a policy map. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |

# ip tcp compression-connections

To specify the total number of Transmission Control Protocol (TCP) header compression connections that can exist on an interface, use the **ip tcp compression-connections** command in interface configuration mode.To restore the default, use the **no**form of this command.

**ip tcp compression-connections** *number*

**no ip tcp compression-connections**

## Syntax Description

| | |
|---|---|
| *number* | Number of TCP header compression connections the cache supports, in the range from 3 to 256. |

## Command Default

For PPP and High-Level Data Link Control (HDLC) interfaces, the default is 16 compression connections.

For Frame Relay interfaces, the default is 256 compression connections.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.0(7)T | For Frame Relay interfaces, the maximum number of compression connections increased from 32 to 256. The default number of compression connections was increased from 32 (fixed) to 256 (configurable). |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

You should configure one connection for each TCP connection through the specified interface.

Each connection sets up a compression cache entry, so you are in effect specifying the maximum number of cache entries and the size of the cache. Too few cache entries for the specified interface can lead to degraded performance, and too many cache entries can lead to wasted memory.

**Note** Both ends of the serial connection must use the same number of cache entries.

## Examples

The following example sets the first serial interface for header compression with a maximum of ten cache entries:

```
Router> enable
Router# configure terminal
Router(config)# interface serial 0
Router(config-if)# ip tcp header-compression
Router(config-if)# ip tcp compression-connections 10
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **ip tcp header-compression** | Enables TCP header compression. |
| **show ip tcp header-compressions** | Displays TCP header compression statistics. |

# ip tcp header-compression

To enable Transmission Control Protocol (TCP) header compression, use the **ip tcp header-compression** command in interface configuration mode.To disable compression, use the **no**form of this command.

**ip tcp header-compression** [**passive**| **iphc-format**| **ietf-format**]

**no ip tcp header-compression** [**passive**| **iphc-format**| **ietf-format**]

## Syntax Description

| | |
|---|---|
| **passive** | (Optional) Compresses outgoing TCP packets only if incoming TCP packets on the same interface are compressed. If you do not specify the **passive** keyword, all TCP packets are compressed. |
| **iphc-format** | (Optional) Indicates that the IP Header Compression (IPHC) format of header compression will be used. |
| **ietf-format** | (Optional) Indicates that the Internet Engineering Task Force (IETF) format of header compression will be used. |

## Command Default

For PPP interfaces, the default format for header compression is the IPHC format.

For High-Level Data Link Control (HDLC) and Frame Relay interfaces, the default format is as described in RFC 1144, *Compressing TCP/IP Headers for Low-Speed Serial Links.*

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.0 | This command was integrated into Cisco IOS Release 12.0. This command was modified to include the **iphc-format** keyword. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T. This command was modified to include the **ietf-format** keyword. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

You can compress the headers of your TCP/IP packets in order to reduce the size of your packets. TCP header compression is supported on serial lines using Frame Relay, HDLC, or PPP encapsulation. You must enable compression on both ends of a serial connection. Compressing the TCP header can speed up Telnet connections dramatically.

In general, TCP header compression is advantageous when your traffic consists of many small packets, not for traffic that consists of large packets. Transaction processing (usually using terminals) tends to use small packets and file transfers use large packets. This feature only compresses the TCP header, so it has no effect on User Datagram Protocol (UDP) packets or other protocol headers.

### The passive Keyword

By default, the **ip tcp header-compression** command compresses outgoing TCP traffic. If you specify the **passive** keyword, outgoing TCP traffic is compressed only if incoming TCP traffic on the same interface is compressed. If you do not specify the **passive** keyword, all outgoing TCP traffic is compressed.

For PPP interfaces, the **passive** keyword is ignored. PPP interfaces negotiate the use of header-compression, regardless of whether the **passive** keyword is specified. Therefore, on PPP interfaces, the **passive** keyword is replaced by the IPHC format, the default format for PPP interfaces.

### The iphc-format Keyword

The **iphc-format** keyword indicates that the IPHC format of header compression will be used. For PPP and HDLC interfaces, when the **iphc-format** keyword is specified, Real-Time Transport Protocol (RTP) header compression is also enabled. For this reason, the **ip rtp header-compression** command appears in the output of the **show running-config** command. Since both TCP header compression and RTP header compression are enabled, both TCP packets and UDP packets are compressed.

The **iphc-format** keyword is not available for interfaces that use Frame Relay encapsulation.

**Note** The header compression format (in this case, IPHC) must be the same at *both* ends of the network. That is, if you specify the **iphc-format** keyword on the local router, you must also specify the **iphc-format** keyword on the remote router.

### The ietf-format Keyword

The **ietf-format** keyword indicates that the IETF format of header compression will be used. For HDLC interfaces, the **ietf-format** keyword compresses only TCP packets. For PPP interfaces, when the **ietf-format** keyword is specified, RTP header compression is also enabled. For this reason, the **ip rtp header-compression** command appears in the output of the **show running-config** command. Since both TCP header compression and RTP header compression are enabled, both TCP packets and UDP packets are compressed.

The **ietf-format** keyword is not available for interfaces that use Frame Relay encapsulation.

**Note** The header compression format (in this case, IETF) must be the same at *both* ends of the network. That is, if you specify the **ietf-format**keyword on the local router, you must also specify the **ietf-format** keyword on the remote router.

## Examples

The following example sets the first serial interface for header compression with a maximum of ten cache entries:

```
Router> enable
Router# configure terminal
Router(config)# interface serial 0
Router(config-if)# ip tcp header-compression
Router(config-if)# ip tcp compression-connections 10
Router(config-if)# end
```

The following example enables RTP header compression on the Serial1/0.0 subinterface and limits the number of RTP header compression connections to 10. In this example, the optional **iphc-format** keyword of the **ip tcp header-compression** command is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial1/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip tcp header-compression iphc-format
Router(config-if)# ip tcp compression-connections 10
Router(config-if)# end
```

The following example enables RTP header compression on the Serial2/0.0 subinterface and limits the number of RTP header compression connections to 20. In this example, the optional **ietf-format** keyword of the **ip tcp header-compression** command is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface Serial2/0.0
Router(config-if)# encapsulation ppp
Router(config-if)# ip tcp header-compression ietf-format
Router(config-if)# ip tcp compression-connections 20
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **ip tcp compression-connections** | Specifies the total number of TCP header compression connections that can exist on an interface. |
| **show ip tcp header-compression** | Displays TCP/IP header compression statistics. |
| **show running-config** | Displays the contents of the currently running configuration file or the configuration for a specific interface, or map class information. |

# iphc-profile

To create an IP Header Compression (IPHC) profile and to enter IPHC-profile configuration mode, use the **iphc-profile** command in global configuration mode. To attach an existing IPHC profile to an interface or subinterface, use the **iphc-profile** command in interface configuration mode. To delete the IPHC profile, use the **no** form of this command.

**iphc-profile** *profile-name* {**ietf**| **van-jacobson**}

**no iphc-profile** *profile-name*

## Syntax Description

| | |
|---|---|
| *profile-name* | Name of the IPHC profile to be created or attached. The IPHC profile name can be a maximum of 32 characters. The name may not include quotation marks, white space, or special characters. |
| **ietf** | Specifies that the IPHC profile is for Internet Engineering Task Force (IETF) header compression. |
| **van-jacobson** | Specifies that the IPHC profile is for Van Jacobson header compression. |

## Command Default

No IPHC profile is created or attached.

## Command Modes

Global configuration (to create an IPHC profile) Interface configuration (to attach an existing IPHC profile to an interface or subinterface)

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

The **iphc-profile** command creates an IPHC profile used for enabling header compression and enters IPHC-profile configuration mode (config-iphcp). An IPHC profile is a template within which you can configure the type of header compression that you want to use, enable any optional features and settings for header compression, and then apply the profile to an interface, a subinterface, or a Frame Relay permanent virtual circuit (PVC).

### Specifying the IPHC Profile Type

When you create an IPHC profile, you must specify the IPHC profile type by using either the **ietf** keyword or the **van-jacobson** keyword. The IETF profile type conforms to and supports the standards established with RFC 2507, RFC 2508, RFC 3544, and RFC 3545 and is typically associated with non-TCP header compression

(for example, RTP header compression). The Van Jacobson profile type conforms to and supports the standards established with RFC 1144 and is typically associated with TCP header compression.

**Note** If you are using Frame Relay encapsulation, you must specify the **ietf**keyword (not the **van-jacobson** keyword).

### Considerations When Specifying the IPHC Profile Type

When specifying the IPHC profile type, consider whether you are compressing TCP traffic or non-TCP traffic (that is, RTP traffic). Also consider the header compression format capabilities of the remote network link that will receive traffic. The IPHC profile type that you specify directly affects the header compression format used on the remote network links to which the IPHC profile is applied. *Only* TCP traffic is compressed on remote network links using a Van Jacobson IPHC profile, whereas TCP *and/or* non-TCP traffic (for example, RTP traffic) is compressed on remote network links using an IETF IPHC profile.

**Note** The header compression format in use on the router that you are configuring and the header compression format in use on the remote network link must match.

### Configurable Header Compression Features and Settings

The specific set of header compression features and settings that you can configure (that is, enable or modify) is determined by the IPHC profile type that you specify (either IETF or Van Jacobson) when you create the IPHC profile. Both sets are listed below.

If you specify Van Jacobson as the IPHC profile type, you can enable TCP header compression and set the number of TCP contexts. The table below lists each available Van Jacobson IPHC profile type header compression feature and setting and the command used to enable it.

***Table 7: Van Jacobson IPHC Profile Type Header Compression Features and Settings***

| Command | Feature or Setting |
|---|---|
| **tcp** | Enables TCP header compression. |
| **tcp contexts** | Sets the number of contexts available for TCP header compression. |

If you specify IETF as the IPHC profile type, you can enable non-TCP header compression (that is, RTP header compression), along with a number of additional features and settings. The table below lists each available IETF IPHC profile type header compression feature and setting and the command or commands used to enable it.

***Table 8: IETF IPHC Profile Type Header Compression Features and Settings***

| Command | Feature or Setting |
|---|---|
| **feedback** | Enables the context-status feedback messages from the interface or link. |

| Command | Feature or Setting |
|---|---|
| **maximum header** | Sets the maximum size of the compressed IP header. |
| **non-tcp** | Enables non-TCP header compression. |
| **non-tcp contexts** | Sets the number of contexts available for non-TCP header compression. |
| **rtp** | Enables RTP header compression. |
| **recoverable-loss** | Enables Enhanced Compressed Real-Time Transport Protocol (ECRTP) on an interface. |
| **refresh max-period refresh max-time refresh rtp** | Sets the context refresh (full-header refresh) options, such as the amount of time to wait before a full header is refreshed. |
| **tcp** | Enables TCP header compression. |
| **tcp contexts** | Sets the number of contexts available for TCP header compression. |

### For More Information About IPHC Profiles

For more information about using IPHC profiles to configure header compression, see the "Header Compression" module and the "Configuring Header Compression Using IPHC Profiles" module of the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4T.

## Examples

In the following example, an IPHC profile called profile1 is created, and the Van Jacobson IPHC profile type is specified.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile1 van-jacobson
Router(config-iphcp)# end
```

In the following example, a second IPHC profile called profile2 is created. For this IPHC profile, the IETF IPHC profile type is specified.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# end
```

In the following example, an existing IPHC profile called profile2 is attached to serial interface 3/0. For this IPHC profile, the IPHC profile type (in this case, IETF) of profile2 is specified.

```
Router> enable
Router# configure terminal
Router(config)# interface serial 3/0
Router(config-if)# iphc-profile profile2 ietf
Router(config-iphcp)# end
```

## Related Commands

| Command | Description |
|---|---|
| **feedback** | Enables the context-status feedback messages from the interface or link. |
| **maximum header** | Specifies the maximum size of the compressed IP header. |
| **non-tcp** | Enables non-TCP header compression within an IPHC profile. |
| **non-tcp contexts** | Sets the number of contexts available for non-TCP header compression. |
| **recoverable-loss** | Enables ECRTP on an interface. |
| **refresh max-period** | Sets the number of packets sent between full-header refresh occurrences. |
| **refresh max-time** | Sets the amount of time to wait before a full-header refresh occurrence. |
| **refresh rtp** | Enables a context refresh occurrence for RTP header compression. |
| **rtp** | Enables RTP header compression within an IPHC profile. |
| **show iphc-profile** | Displays configuration information for one or more IPHC profiles. |
| **tcp** | Enables TCP header compression within an IPHC profile. |
| **tcp contexts** | Set the number of contexts available for TCP header compression. |

# lane client qos

To apply a LAN Emulation (LANE) quality of service (QoS) database to an interface, use the **laneclient** qos command in subinterface configuration mode. To remove the QoS over LANE feature from the interface, use the **no** form of this command.

**lane client qos** *database-name*

**no lane client qos** *database-name*

## Syntax Description

| | |
|---|---|
| *database-name* | Name of the QoS database. |

## Command Default

This command is not configured by default.

## Command Modes

Subinterface configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(2)E | This command was introduced. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Examples

This example shows how to apply a LANE QoS database to a subinterface:

```
Router(config-subif)# lane client qos user1
```

## Related Commands

| Command | Description |
|---|---|
| **atm-address** | Specifies the QoS parameters associated with a particular ATM address. |
| **lane qos database** | Begins the process of building a QoS over LANE database |

| Command | Description |
|---|---|
| **show lane qos database** | Displays the contents of a specific QoS over LANE database. |
| **ubr+ cos** | Maps a CoS value to a UBR+ VCC. |

# lane qos database

To build the LAN Emulation (LANE) quality-of-service database, use the **laneqosdatabase**command in global configuration mode. To remove a LANE QoS database name, use the **no** form of this command.

**lane qos database** *name*

**no lane qos database** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of the LANE QoS database. |

## Command Default

This command is not configured by default.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(2)E | This command was introduced. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command specifies a named database of QoS parameters. The database can be applied on the subinterfaces on which a LANE client is configured.

## Examples

This example shows how to begin configuring a QoS over LANE database named user1 on a Catalyst 5000 family ATM switch:

```
ATM# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
ATM(config)# lane qos database user1
```

This example shows how to begin configuring a QoS over LANE database named user2 on a router:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# lane qos database user2
```

## Related Commands

| Command | Description |
|---|---|
| **atm-address** | Specifies the QoS parameters associated with a particular ATM address. |
| **lane client qos** | Applies a QoS over LANE database to an interface. |
| **show lane qos database** | Displays the contents of a specific QoS over LANE database. |
| **ubr+ cos** | Maps a CoS value to a UBR+ VCC. |

# load protocol

To load a protocol header description file (PHDF) onto a router, use the **loadprotocol**command in global configuration mode. To unload all protocols from a specified location or a single protocol, use the **no** form of this command.

**load protocol** *location* **:** *filename*

**no load protocol** {*location* **:** *filename*| *protocol-name*}

## Syntax Description

| | |
|---|---|
| *location* **:** *filename* | Location of the PHDF that is to be loaded onto the router.<br>When used with the no version of this command, all protocols loaded from the specified filename will be unloaded.<br>**Note** The location must be local to the router. |
| *protocol-name* | Unloads only the specified protocol.<br>**Note** If you attempt to unload a protocol that is being referenced by a filter, you will receive an error. |

## Command Default

If this command is not issued, no PHDFs will be loaded onto the router.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |
| 12.2(18)ZY | This command was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA). |

## Usage Guidelines

Flexible packet matching allows users to classify traffic on the basis of any portion of a packet header given the protocol field, length, and pattern. Protocol headers are defined in separate files called PHDFs; the field names that are defined within the PHDFs are used for defining the packet filters. A PHDF is a file that allows the user to leverage the flexibility of extensible markup language (XML) to describe almost any protocol header. The important components of the PHDF are the version, the XML file schema location, and the protocol field definitions. The protocol field definitions name the appropriate field in the protocol header,

allow for a comment describing the field, provide the location of the protocol header field in the header (the offset is relative to the start of the protocol header), and provide the length of the field. Users can choose to specify the measurement in bytes or in bits.

**Note** The total length of the header must be specified at the end of each PHDF.

In case of a redundant setup, users should ensure all PHDFs that are used in the flexible packet matching configuration are present on the corresponding standby disk. If the PHDFs are not on standby disk, all flexible packet matching policies using the PHDFs will be broken.

Users can write their own custom PHDFs via XML. However, the following standard PHDFs can also be loaded onto the router: ip.phdf, ether.phdf, tcp.phdf, and udp.phdf.

Standard PHDFs are available on Cisco.com at the following URL: http://www.cisco.com/cgi-bin/tablebuild.pl/fpm

Because PHDFs are defined via XML, they are not shown in a running configuration.

Issue the **loadprotocol** command to apply filters to a protocol by defining and loading a PHDF for that protocol header.

## Examples

The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header.

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf
class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp
class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp
class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster3
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030
policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
 drop
policy-map type access-control fpm-udp-policy
 class blaster3
 drop
policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy
interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

The following example is the XML setup for the PHDF “ip.phdf:”

```
<?xml version="1.0" encoding="UTF-8"?>
<phdf xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchem
aLocation="D:\harinadh\Doc\Projects\FPME\XML\ex.xsd">
<protocol name="ip" description="Definition-for-the-IP-protocol">
```

```
<field name="version" description="IP-version">
<offset type="fixed-offset" units="bits"> 0 </offset>
<length type="fixed" units="bits">4</length>
</field>
<field name="ihl" description="IP-Header-Length">
<offset type="fixed-offset" units="bits">4</offset>
<length type="fixed" units="bits">4</length>
</field>
<field name="tos" description="IP-Type-of-Service">
<offset type="fixed-offset" units="bits">8</offset>
<length units="bits" type="fixed">8</length>
</field>
<field name="length" description="IP-Total-Length">
<offset type="fixed-offset" units="bytes">2</offset>
<length type="fixed" units="bytes">2</length>
</field>
<field name="identification" description="IP-Identification">
<offset type="fixed-offset" units="bytes">4</offset>
<length type="fixed" units="bytes">2</length>
</field>
<field name="flags" description="IP-Fragmentation-Flags">
<offset type="fixed-offset" units="bytes">6</offset>
<length type="fixed" units="bits">3</length>
</field>
<field name="fragment-offset" description="IP-Fragmentation-Offset">
<offset type="fixed-offset" units="bits">51</offset>
<length type="fixed" units="bits">13</length>
</field>
<field name="ttl" description="Definition-for-the-IP-TTL">
<offset type="fixed-offset" units="bytes">8</offset>
<length type="fixed" units="bytes">1</length>
</field>
<field name="protocol" description="IP-Protocol">
<offset type="fixed-offset" units="bytes">9</offset>
<length type="fixed" units="bytes">1</length>
</field>
<field name="checksum" description="IP-Header-Checksum">
<offset type="fixed-offset" units="bytes">10</offset>
<length type="fixed" units="bytes">2</length>
</field>
<field name="source-addr" description="IP-Source-Address">
<offset type="fixed-offset" units="bytes">12</offset>
<length type="fixed" units="bytes">4</length>
</field>
<field name="dest-addr" description="IP-Destination-Address">
<offset type="fixed-offset" units="bytes">16</offset>
<length type="fixed" units="bytes">4</length>
</field>
<headerlength type="fixed" value="20"></headerlength>
</protocol>
</phdf>
```

# match access-group through mls ip pbr


- mac packet-classify, page 446
- mac packet-classify use vlan, page 448
- map ip, page 450
- map ipv6, page 453
- map mpls, page 455
- match access-group, page 457
- match application (class-map), page 461
- match any, page 465
- match atm-clp, page 467
- match atm oam, page 469
- match atm-vci, page 471
- match class-map, page 473
- match cos, page 476
- match cos inner, page 479
- match destination-address mac, page 481
- match discard-class, page 483
- match dscp, page 485
- match field, page 488
- match flow pdp, page 491
- match fr-dlci, page 493
- match input vlan, page 495
- match input-interface, page 499
- match ip dscp, page 502
- match ip precedence, page 503

- match ip rtp, page 504
- match mpls experimental, page 506
- match mpls experimental topmost, page 509
- match not, page 511
- match packet length (class-map), page 513
- match port-type, page 516
- match precedence, page 518
- match protocol, page 522
- match protocol attribute application-group, page 536
- match protocol attribute category, page 539
- match protocol attribute encrypted, page 541
- match protocol attribute sub-category, page 543
- match protocol attribute tunnel, page 546
- match protocol (NBAR), page 548
- match protocol citrix, page 649
- match protocol fasttrack, page 651
- match protocol gnutella, page 653
- match protocol http, page 655
- match protocol pppoe-discovery, page 661
- match protocol rtp, page 663
- match qos-group, page 665
- match source-address mac, page 668
- match start, page 670
- match tag (class-map), page 673
- match vlan (QoS), page 674
- match vlan inner, page 676
- maximum (local policy), page 678
- maximum bandwidth ingress, page 680
- maximum bandwidth percent, page 682
- maximum header, page 684
- max-reserved-bandwidth, page 686
- metadata application-params, page 690
- metadata flow, page 693

- metadata flow (troubleshooting), page 695
- mls ip pbr, page 697

# mac packet-classify

To classify Layer 3 packets as Layer 2 packets, use the **macpacket-classify** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

**mac packet-classify [bpdu]**

**no mac packet-classify [bpdu]**

## Syntax Description

| | |
|---|---|
| **bpdu** | (Optional) Specifies Layer 2 policy enforcement for BPDU packets. |

## Command Default

Layer 3 packets are not classified as Layer 2 packets.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXD | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(50)SY | Added support for MAC ACLs on BPDU packets. |

## Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

You can configure these interface types for multilayer MAC access control list (ACL) quality of service (QoS) filtering:

- VLAN interfaces without Layer 3 addresses
- Physical LAN ports that are configured to support Ethernet over Multiprotocol Label Switching (EoMPLS)
- Logical LAN subinterfaces that are configured to support EoMPLS

The ingress traffic that is permitted or denied by a MAC ACL on an interface configured for multilayer MAC ACL QoS filtering is processed by egress interfaces as MAC-layer traffic. You cannot apply egress IP ACLs to traffic that was permitted or denied by a MAC ACL on an interface configured for multilayer MAC ACL QoS filtering.

Microflow policing does not work on interfaces that have the **macpacket-classify** command enabled.

The **macpacket-classify** command causes the Layer 3 packets to be classified as Layer 2 packets and disables IP classification.

Traffic is classified based on 802.1Q class of service (CoS), trunk VLAN, EtherType, and MAC addresses.

## Examples

This example shows how to classify incoming and outgoing Layer 3 packets as Layer 2 packets:

```
Router(config-if)# mac packet-classify
Router(config-if)#
```

This example shows how to disable the classification of incoming and outgoing Layer 3 packets as Layer 2 packets:

```
Router(config-if)# no mac packet-classify
Router(config-if)#
```

This example shows how to enforce Layer 2 policies on BPDU packets:

```
Router(config-if)# mac packet-classify bpdu
Router(config-if)#
```

This example shows how to disable Layer 2 policies on BPDU packets:

```
Router(config-if)# no mac packet-classify bpdu
Router(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **mac packet-classify use vlan** | Enables VLAN-based QoS filtering in the MAC ACLs. |

# mac packet-classify use vlan

To enable VLAN-based quality of service (QoS) filtering in the MAC access control lists (ACLs), use the **macpacket-classifyusevlan** command in global configuration mode. To return to the default settings, use the **no** form of this command.

**mac packet-classify use vlan**

**no mac packet-classify use vlan**

## Syntax Description

This command has no arguments or keywords.

## Command Default

VLAN-based QoS filtering in the MAC ACLs is disabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXD | Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is supported in PFC3BXL or PFC3B mode only.

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

You must use the **nomacpacket-classifyusevlan** command to disable the VLAN field in the Layer 2 key if you want to apply QoS to the Layer 2 Service Advertising Protocol (SAP)-encoded packets (for example, Intermediate System-to-Intermediate System [IS-IS] and Internet Packet Exchange [IPX]).

QoS does not allow policing of non-Advanced Research Protocol Agency (ARPA) Layer 2 packets (for example, IS-IS and IPX) if the VLAN field is enabled.

## Examples

This example shows how to enable Layer 2 classification of IP packets:

```
Router(config)# mac packet-classify use vlan
Router(config)
```

This example shows how to disable Layer 2 classification of IP packets:

```
Router(config)# no mac packet-classify use vlan
Router(config)
```

## Related Commands

| Command | Description |
|---|---|
| **mac packet-classify** | Classifies Layer 3 packets as Layer 2 packets. |

# map ip

T o classify either all the IPv4 packets, or the IPv4 packets based on either differentiated service code point (DSCP) values or precedence values into high priority or low priority for POS, channelized, and clear-channel SPAs, use the following forms of the **mapip** command in ingress class-map mode. Use the **no** forms of this command listed here to remove the IPv4 settings.

### Command to Classify all the IPv4 Packets

**map ip all queue** {**strict-priority**| **0**}

**no map ip all queue** {**strict-priority**| **0**}

### Command to Classify IPv4 Packets Based on DSCP Values

**map ip** {**dscp-based**| **dscp** {*dscp-value*| *dscp-range*} **queue** {**strict-priority**| **0**}}

**no map ip** {**dscp-based**| **dscp** {*dscp-value*| *dscp-range*} **queue** {**strict-priority**| **0**}}

### Command to Classify IPv4 Packets Based on Precedence Values

**map ip** {**precedence-based**| **precedence** {*precedence-value*| *precedence-range*} **queue strict-priority**| **0**}

**no map ip** {**precedence-based**| **precedence** {*precedence-value*| *precedence-range*} **queue strict-priority**| **0**}

## Syntax Description

| | |
|---|---|
| **all queue** | Implies the high priority or low priority configuration of all the IPv4 packets. |
| **strict-priority** | Classifies all the IPv4 packets as high priority (strict-priority). |
| **0** | Classifies all the IPv4 packets as low priority. |
| **dscp-based** | Enables classification based on DSCP value in IPv4. |
| dscp | Allows you to configure the DSCP value or range as high priority or low priority for IPv4 packets. |
| *dscp-value* | DSCP value for which the priority is to be configured as high or low. |
| *dscp-range* | Range of dscp-values for which the priority is to be configured as high or low. |
| **queue** | Enables the classification of an entire queue, DSCP values, or precedence values as high priority or low priority. |
| **precedence-based** | Enables the classification based on IPv4 precedence values. |

| | |
|---|---|
| precedence | Allows you to configure an IPv4 precedence value or range as high priority or low priority for IPv4 packets. |
| *precedence-value* | Precedence-value for which the priority is to be configured as high or low. |
| *precedence-range* | Range of precedence-values for which the priority is to be configured as high or low. |

## Command Default

If there is no configuration of IPv4 DSCP value or precedence values map to high priority specified, the system treats packets with DSCP range EF as high priority and precedence range 6-7 as high priority.

## Command Modes

Ingress-class-map configuration mode

## Command History

| Release | Modification |
|---|---|
| 3.1S | This command was introduced to classify either all the IPv4 packets, or the IPv4 packets based on either DSCP value or precedence values as high or low for POS, channelized, and clear-channel SPAs. |

## Usage Guidelines

To classify all IPv4 packets as high or low for POS, channelized, or clear-channel SPA, use the **mapipallqueue**command,

To classify IPv4 packets with specific DSCP values, enable the DSCP classification using the **mapipdscp-based**command. To classify IPV4 packets with specific DSCP values as high or low, use the **mapipdscp** {{*dscp-value* | *dscp-range*} **queue** {**strict-priority** | **0**}} command.

To classify IPv4 packets with specific precedence values, enable the precedence classification using the **mapipprecedence-based**command. To classify IPv4 packets with specific precedence values as high or low, use the **mapipprecedence** {{*precedence-value* | *precedence-range*} **queue** {**strict-priority** | **0**}} command.

## Examples

The following example shows how to classify all the IPv4 Packets as high priority using the **mapipallqueuestrict-priority**command:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ip all queue strict-priority
```

The following example shows how to classify IPv4 Packets with DSCP value of cs1 as high priority:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ip dscp-based
Router(config-ing-class-map)# map ip dscp cs1 queue strict-priority
```

The following example shows how to classify IPv4 Packets with a precedence value 3 and 5 as high priority:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ip precedence-based
Router(config-ing-class-map)# map ip precedence 3 5 queue strict-priority
```

## Related Commands

| Command | Description |
|---|---|
| **plim qos input class-map** | Attaches the classification template to an interface. |

# map ipv6

T o classify either all the IPv6 packets, or IPv6 packets based on specific traffic class (TC) values as high priority or low priority in the context of POS, channelized, and clear-channel SPAs use the following forms of **mapipv6** commands in ingress class-map mode. Use the **no** forms of this command listed here to remove the IPv6 settings.

### Command to Classify all the IPv6 Packets

**map ipv6 all queue** {**strict-priority| 0**}

**no map ipv6 all queue** {**strict-priority| 0**}

### Command to Classify IPv6 Traffic-Class values as High Priority or Low Priority

**map ipv6 tc** {*tc-value*| *tc-range*} **queue** {**strict-priority| 0**}

**no map ipv6 tc** {*tc-value*| *tc-range*} **queue** {**strict-priority| 0**}

## Syntax Description

| | |
|---|---|
| **all queue** | Implies the high priority or low priority configuration of all the IPv6 packets. |
| **strict-priority** | Classifies all the IPv6 packets as high priority (strict-priority). |
| **0** | Classifies all the IPv6 Packets as low priority. |
| tc | Allows you to configure the traffic class value or range as high priority or low priority for IPv6 packets. |
| *tc-value* | Specific traffic-class value for which the priority is to be configured as either high or low(0). |
| *tc-range* | Range of traffic-class values for which the priority is to be configured as either high or low(0). |
| **queue** | Enables classification of the entire queue, traffic-class values, or range of traffic-class values as either high priority or low priority. |

## Command Default

If a user does not configure which IPv6 traffic class values map to high priority, the system treats packets the packets with traffic class EF as high priority.

## Command Modes

Ingress-class-map configuration mode

## Command History

| Release | Modification |
|---|---|
| 3.1S | This command was introduced to classify, all the IPv6 packets or the IPv6 packets based on traffic class values as high priority or low priority for POS, channelized, and clear-channel SPAs. |

## Usage Guidelines

To classify all the IPv6 packets as high priority or low priority in the context of POS, channelized, or clear-channel SPAs, use the **mapipv6allqueue**command.

To classify the IPv6 packets with specific traffic class values, use the **mapipv6tccs2queuestrict-priority**command.

## Examples

The following example shows how to classify all the IPv6 packets as high priority using the **mapipv6allqueuestrict-priority** command:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ipv6 all queue strict-priority
```

The following example shows how to classify the IPv6 packets with traffic-class values cs2 as high priority:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map ip tc cs2 queue strict-priority
```

## Related Commands

| Command | Description |
|---|---|
| **plim qos input class-map** | Attaches the classification template to an interface. |

# map mpls

T o classify either all the Multiprotocol Label Switching (MPLS) packets or MPLS packets with specified EXP values or range as high priority or low priority for POS, channelized, and clear-channel SPAs the following forms of the **mapmpls** command are used in ingress class-map mode. Use the **no** forms of this command listed here to remove the MPLS settings.

### Command to Classify all the MPLS EXP Values as High Priority or Low Priority

**map mpls all queue** {**strict-priority**| **0**}

**no map mpls all queue**

### Command to Classify the MPLS EXP Values as High Priority or Low Priority

**map mpls exp** {*exp-value*| *exp-range*} **queue** {**strict-priority**| **0**}

**no map mpls exp** {*exp-value*| *exp-range*} **queue** {**strict-priority**| **0**}

## Syntax Description

| | |
|---|---|
| **all queue** | Implies the high priority or low priority configuration of all the MPLS Packets. |
| **strict-priority** | Classifies either all the MPLS packets or the MPLS packets with specific EXP values as high priority (strict priority). |
| **0** | Classifies MPLS packets as low priority. |
| exp | Allows you to configure an EXP value or a range of EXP values as high priority or low priority for MPLS packets. The valid range for EXP values is 0 to 7. |
| *exp-value* | A specific EXP value for which the priority is to be configured as high or low(0). |
| *exp-range* | A range of EXP values for which the priority is to be configured as high or low(0). The valid range for EXP values is 0 to 7. |
| **queue** | Enables the classification priority of an entire queue, EXP values, or range of EXP values as high priority or low priority. |

## Command Default

If a user does not configure which MPLS EXP values map to high priority, the system treats packets with an EXP value of 6-7 as high priority.

**Command Modes** Ingress-class-map configuration mode

**Command History**

| Release | Modification |
|---|---|
| 3.1S | This command was introduced to classify either all the MPLS packets or MPLS packets based on EXP values as high priority or low priority for POS, channelized, and clear-channel SPAs. |

**Usage Guidelines** To classify all the MPLS packets as high priority or low priority for POS, channelized, or clear-channel SPA, use the **mapmplsallqueue**command.

To classify the MPLS packets with specific EXP values, use the **mapmplsexp{exp-value|exp-range}queue{strict-priority|0}** command.

**Examples** The following example shows how to classify all the MPLS packets as high priority using the **mapmplsallqueuestrict-priority** command:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map mpls all queue strict-priority
```

The following example shows how to classify the MPLS packets with EXP value of 4 as high priority:

```
Router# config
Router(config)# ingress-class-map 1
Router(config-ing-class-map)# map mpls exp 4 queue strict-priority
```

**Related Commands**

| Command | Description |
|---|---|
| **plim qos input class-map** | Attaches the classification template to an interface. |

# match access-group

To configure the match criteria for a class map on the basis of the specified access control list (ACL), use the **match access-group** command in QoS class-map configuration or policy inline configuration mode. To remove the ACL match criteria from a class map, use the **no** form of this command.

**match access-group** {*access-group*| **name** *access-group-name*}

**no match** {*access-group*| **name** *access-group-name*}

## Syntax Description

| | |
|---|---|
| *access-group* | A numbered ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to the same class. The range is from 1 to 2699. |
| **name** *access-group-name* | Specifies a named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to the same class. The name can be up to 40 alphanumeric characters. |

## Command Default

No match criteria are configured.

## Command Modes

QoS class-map configuration (config-cmap)

Policy inline configuration (config-if-spolicy-inline)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE. |
| 12.0(7)S | This command was integrated into Cisco IOS Release 12.0(7)S. |
| 12.0(17)SL | This command was modified. This command was enhanced to include matching of access lists on the Cisco 10000 series routers. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.4(6)T | This command was modified. This command was enhanced to support the zone-based policy firewall. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB. |

| Release | Modification |
|---|---|
| 12.2SX | This command was integrated into the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode. |
| 12.2(58)SE | This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor. |

## Usage Guidelines

The **match access-group** command specifies a numbered or named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

A traffic rate is generated for packets that match an access group. In zone-based policy firewalls, only the first packet that creates a session matches the configured policy. Subsequent packets in the flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the inspect action.

Zone-based policy firewalls support only the **match access-group**, **match class-map**, and **match protocol** commands. If you specify more than one **match** command in a class map, only the last command that you specified will be applied to the class map. The last **match** command overrides the previously entered **match** commands.

The **match access-group** command specifies the numbered access list against whose contents packets are checked to determine if they match the criteria specified in the class map. Access lists configured with the **log** keyword of the **access-list** command are not supported when you configure the match criteria. For more information about the **access-list** command, refer to the *Cisco IOS IP Application Services Command Reference*.

When this command is configured in Cisco IOS Release 15.0(1)M and later releases, the firewall inspects only Layer 4 policy maps. In releases prior to Cisco IOS Release 15.0(1)M, the firewall inspects both Layer 4 and Layer 7 policy maps.

For class-based weighted fair queueing (CBWFQ), you can define traffic classes based on the match criteria that include ACLs, experimental (EXP) field values, input interfaces, protocols, and quality of service (QoS) labels. Packets that satisfy the match criteria for a class constitute the traffic for that class.

**Note** In zone-based policy firewalls, this command is not applicable for CBWFQ.

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration modes in which you can issue this command.

### Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

To use the **match access-group** command, you must configure the **service-policy type performance-monitor inline** command.

### Supported Platforms Other than Cisco 10000 Series Routers

To use the **match access-group** command, you must configure the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**
- **match protocol**

### Cisco 10000 Series Routers

To use the **match access-group** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

**Note** The **match access-group** command specifies the numbered access list against whose contents packets are checked to determine if they match the criteria specified in the class map. Access lists configured with the **log** keyword of the **access-list** command are not supported when you configure the match criteria.

### Cisco ASR 1000 Series Aggregation Services Routers

Cisco ASR 1000 Series Routers do not support more than 16 match statements per class map. An interface with more than 16 match statements rejects the service policy.

## Examples

The following example shows how to specify a class map named acl144 and to configure the ACL numbered 144 to be used as the match criterion for that class:

```
Device(config)# class-map acl144
Device(config-cmap)# match access-group 144
```

The following example shows how to define a class map named c1 and configure the ACL numbered 144 to be used as the match criterion for that class:

```
Device(config)# class-map type inspect match-all c1
Device(config-cmap)# match access-group 144
```

### Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

The following example shows how to configure a service policy for the Performance Monitor in policy inline configuration mode. The policy specifies that packets traversing Ethernet interface 0/0 must match ACL144.

```
Device(config)# interface ethernet 0/0
Device(config-if)# service-policy type performance-monitor inline input
Device(config-if-spolicy-inline)# match access-group name ACL144
Device(config-if-spolicy-inline)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **access-list (IP extended)** | Defines an extended IP access list. |

| Command | Description |
|---|---|
| **access-list (IP standard)** | Defines a standard IP access list. |
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **match access-group** | Configures the match criteria for a class map on the basis of the specified ACL. |
| **match class-map** | Uses a traffic class as a classification policy. |
| **match input-interface** | Configures a class map to use the specified input interface as a match criterion. |
| **match mpls experimental** | Configures a class map to use the specified EXP field value as a match criterion. |
| **match protocol** | Configures the match criteria for a class map on the basis of the specified protocol. |
| **service-policy type performance-monitor** | Associates a Performance Monitor policy with an interface. |

# match application (class-map)

To use the metadata application as a match criterion for control plane classification, use the **match application** command in QoS class-map configuration mode. To remove a previously configured metadata application from being used as a match criterion for control plane classification, use the **no** form of this command.

**match application** {**application-group** *application-group-name* | **attribute** {**category** {**business-and-productivity-tools| voice-and-video**}| **device-class** *device-class-type* | **media-type** *media-type*| **sub-category** {**remote-access-terminal| voice-video-chat-collaboration**}}| *application-name* [**source** {**msp | nbar | rsvp**}| **vendor** *vendor-name* **version** *version-number*]}

**no match application** {**application-group** *application-group-name* | **attribute** {**category** {**business-and-productivity-tools| voice-and-video**}| **device-class** *device-class-type* | **media-type** *media-type*| **sub-category** {**remote-access-terminal| voice-video-chat-collaboration**}}| *application-name* [**source** {**msp | nbar | rsvp**}| **vendor** *vendor-name* **version** *version-number*]}

## Syntax Description

| | |
|---|---|
| **application-group** *application-group-name* | Specifies the application group that the control plane classification engine must match. Use one of the following values to specify the relevant application group: **telepresence-group**, **vmware-group**, **webex-group**. |
| **attribute** | Specifies the relevant attribute to match. |
| **category** | Specifies the category type that the control plane classification engine must match. |
| **business-and-productivity-tools** | Specifies the business and productivity tools. |
| **voice-and-video** | Specifies the voice and video category. |
| **device-class** *device-class-type* | Specifies the device class to match. Use one of the following values to specify the relevant device class: **desktop-conferencing**, **desktop-virtualisation**, **physical-phone**, **room-conferencing**, **software-phone**, **surveillance**. |
| **media-type** *media-type* | Specifies the type of media to match. Use one of the following values to specify the relevant media type: **audio**, **audio-video control**, **data**, and**video**. |
| **sub-category** | Specifies the subcategory to match. |
| **remote-access-terminal** | Specifies the remote access terminal subcategory. |
| **voice-video-chat-collaboration** | Specifies the voice, video, and collaboration subcategory. |

| | |
|---|---|
| *application-name* | Name of the application that the control plane classification engine must match. The following applications are supported: **cisco-phone**, **citrix**, **h323**, **jabber**, **rtp**, **rtsp**, **sip**, **telepresence-control**, **telepresence-data**, **telepresence-media**, **vmware-view**, **webex-data**, **webex-meeting**, **webex-streaming**, **webex-video**, **webex-voice**, **wyze-zero-client**. |
| **source** | (Optional) Specifies the source of the application. |
| **msp** | Specifies the application source as Media-Proxy Services (MSP). |
| **nbar** | Specifies the application source as Network Based Application Recognition (NBAR). |
| **rsvp** | Specifies the application source as the Resource Reservation Protocol (RSVP). |
| **vendor** *vendor-name* | (Optional) Specifies the name of the vendor. Enter ? after the **vendor** keyword to get a list of supported vendors for the respective application name. |
| **version** *version-number* | (Optional) Specifies the version number. |

## Command Default

Metadata-based control plane classification is disabled.

## Command Modes

QoS class-map configuration (config-cmap)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T | This command was introduced. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |
| 15.3(1)T | This command was modified. The **source**, **msp**, **nbar**, and **rsvp** keywords were added. |

## Usage Guidelines

Enabling metadata-based control plane classification on a per-platform, per-line card basis for Quality of Service (QoS) policies involves the following key steps:

- Creating a class map with metadata-based filters.
- Creating a policy map that uses classes.

- Attaching a policy map to the target.

You can use the **match application** command to enable metadata-based filters that can be applied to a class map. Specifying the required application name ensures that the respective policies can be applied only to those flows that match the application name. The classification engine makes its first match.

You can use the **match application** command in conjunction with the any other **match** commands for specifying match criteria for classes. For example, you can use the **match dscp** command along with the **match application** command as the classification criteria for flows.

You can use the **show metadata flow classification table** command to check the metadata-based classification information.

You can use the **debug metadata flow all** command to check if a particular classification has been successfully created.

**Note** With CSCub24690, the **webex-data**, **webex-streaming**, **webex-video**, and **webex-voice** keywords are not supported in the **match application** *application-name* command.

## Examples

The following example shows how to configure a class map c1 and specify metadata application webex-meeting as the matching criterion, thus achieving control plane classification. Only those flows that match the metadata application webex-meeting will be considered for the appropriate action.

```
Device(config)# class-map c1
Device(config-cmap)# match application webex-meeting
```

The following configuration is provided for the completeness of the example.

A policy map p1 that uses the previously configured class c1 is created. The requirement in this example is to provide a guaranteed bandwidth of 1 Mb/s to all the flows that match the criterion defined for class c1:

```
Device(config)# policy-map p1
Device(config-pmap)# class c1
Device(config-pmap-c)# priority 1
```

The following configuration example shows how to attach a policy to a target interface:

```
Device(config)# interface gigabitethernet 0/0
Device(config-if)# service-policy output p1
```

## Related Commands

| Command | Description |
|---|---|
| **class (policy-map)** | Specifies the name of the class whose policy you want to create or change. |
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **debug metadata** | Enables debugging for metadata flow. |
| **metadata application-params** | Enters metadata application entry configuration mode and creates new metadata application parameters. |

| Command | Description |
|---|---|
| **policy-map** | Enters policy-map configuration mode and creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **priority** | Gives priority to a class of traffic belonging to a policy map. |
| **service-policy** | Attaches a policy map to an input interface, a VC, an output interface, or a VC that will be used as the service policy for the interface or VC. |
| **show metadata flow** | Displays metadata flow information. |

# match any

To configure the match criteria for a class map to be successful match criteria for all packets, use the **matchany** command in class-map configuration or policy inline configuration mode. To remove all criteria as successful match criteria, use the **no** form of this command.

**match any**

**no match any**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No match criteria are specified.

## Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)XE | This command was introduced. |
| 12.0(5)T | This command was integrated into Cisco IOS Release 12.0(5)T. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode. |
| 12.2(58)SE | This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor. |

## Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

**Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE**

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

## Examples

In the following configuration, all packets traversing Ethernet interface 1/1 will be policed based on the parameters specified in policy-map class configuration mode:

```
Router(config)# class-map matchany
Router(config-cmap)# match any
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# exit
Router(config)# interface ethernet1/1
Router(config-if)# service-policy output policy1
```

## Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that all packets traversing Ethernet interface 0/0 will be matched and monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match any
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **service-policy type performance-monitor** | Associates a Performance Monitor policy with an interface. |
| **match input-interface** | Configures a class map to use the specified input interface as a match criterion. |
| **match protocol** | Configures the match criteria for a class map on the basis of the specified protocol. |

# match atm-clp

To enable packet matching on the basis of the ATM cell loss priority (CLP), use the **matchatm-clp**command in class-map configuration mode. To disable packet matching on the basis of the ATM CLP, use the **no** form of this command.

**match atm-clp**

**no match atm-clp**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Packets are not matched on the basis of the ATM CLP.

## Command Modes

Class-map configuration (config-cmap)

## Command History

| Release | Modification |
|---|---|
| 12.0(28)S | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| 12.2(33)SRC | Support for the Cisco 7600 series router was added. |
| 12.4(15)T2 | This command was integrated into Cisco IOS Release 12.4(15)T2. |
| 12.2(33)SB | Support for the Cisco 7300 series router was added. |
| Cisco IOS XE Release 2.3 | This command was integrated into Cisco IOS XE Release 2.3. |

## Usage Guidelines

This command is supported on policy maps that are attached to ATM main interfaces, ATM subinterfaces, or ATM permanent virtual circuits (PVCs). However, policy maps (containing the **matchatm-clp** command) that are attached to these types of ATM interfaces can be *input* policy maps *only* .

This command is supported on the PA-A3 adapter *only* .

## Examples

In the following example, a class called “class-c1” has been created using the **class-map** command, and the **matchatm-clp** command has been configured inside that class. Therefore, packets are matched on the basis of the ATM CLP and are placed into this class.

```
Router> enable
Router# configure terminal
```

```
Router(config)# class-map class-c1

Router(config-cmap)# match atm-clp
Router(config-cmap)# end
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **show atm pvc** | Displays all ATM PVCs and traffic information. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# match atm oam

To enable the control traffic classification on an ATM interface, use the **matchatmoam**command in class-map configuration mode. To disable the control traffic classification, use the **no** form of this command.

**match atm oam**

**no match atm oam**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No default behavior or values

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(30)S | This command was introduced. |

## Usage Guidelines

Use this command for policy maps attached to ATM interfaces or ATM permanent virtual circuits (PVCs). Policy maps containing the **matchatmoam** command attached to ATM interfaces or ATM PVCs can be input policy maps only.

## Examples

The following example shows the control traffic classification being configured as the match criterion in a class map. The policy map containing this class map is then applied to the ATM interface.

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# class-map class-oam

Router(config-cmap)# match atm oam

Router(config-cmap)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **show class-map** | Displays all class maps and their matching criteria. |
| **show policy-map** | Displays all policy maps. |

| Command | Description |
|---|---|
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified ATM interface or on a specific PVC on the interface. |

# match atm-vci

To enable packet matching on the basis of the ATM virtual circuit interface (VCI), use the **matchatm-vci**command in class map configuration mode. To disable packet matching on the basis of the ATM VCI, use the**no**form of this command.

**match atm-vci** *vc-id* [ *-vc-id* ]

**no match atm-vci**

## Syntax Description

| | |
|---|---|
| *vc-id* | The VC number assigned to the virtual circuit between two provider edge routers. You can specify one VC or a range of VCs. |
| **-** *vc-id* | (Optional) The second VC number, separated from the first by a hyphen. If two VC numbers are specified, the range is 32 to 65535. |

## Command Default

No match criteria are configured.

## Command Modes

Class map configuration (config-cmap)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 2.3 | This command was introduced. |
| 12.2(33)SRE | This command was modified. This command was integrated into Cisco IOS Release 12.2(33)SRE. |

## Usage Guidelines

When you configure the **matchatm-vci**command in class map configuration mode, you can add this class map to a policy map that can be attached only to an ATM permanent virtual path (PVP).

**Note** On the Cisco 7600 series router, the **matchatm-vci**command is supported only in the ingress direction on an ATM VP.

You can use the **matchnot** command to match any VC except those you specify in the command.

## Examples

The following example enables matching on VC ID 50:

```
Router(config)# class-map map1
Router(config-cmap)# match atm-vci 50
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **match not** | Specifies a single match criterion value to use as an unsuccessful match criterion. |

# match class-map

To use a traffic class as a classification policy, use the **match class-map** command in class-map or policy inline configuration mode. To remove a specific traffic class as a match criterion, use the **no** form of this command.

**match class-map** *class-map-nam e*

**no match class-map** *class-map-name*

## Syntax Description

| | |
|---|---|
| *class-map-name* | Name of the traffic class to use as a match criterion. |

## Command Default

No match criteria are specified.

## Command Modes

Class-map configuration (config-cmap)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)XE | This command was introduced. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.4(6)T | This command was enhanced to support Zone-Based Policy Firewall. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was implemented on the Cisco 10000 series. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 3.2S | This command was integrated into Cisco IOS XE Release 3.2S. |

## Usage Guidelines

The only method of including both match-any and match-all characteristics in a single traffic class is to use the **match class-map** command. To combine match-any and match-all characteristics into a single class, do one of the following:

- Create a traffic class with the match-anyinstruction and use a class configured with the match-all instruction as a match criterion (using the **match class-map** command).

- Create a traffic class with the match-allinstruction and use a class configured with the match-any instruction as a match criterion (using the **match class-map** command).

You can also use the **match class-map** command to nest traffic classes within one another, saving users the overhead of re-creating a new traffic class when most of the information exists in a previously configured traffic class.

When packets are matched to a class map, a traffic rate is generated for these packets. In a zone-based firewall policy, only the first packet that creates a session matches the policy. Subsequent packets in this flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the 'inspect' action.

## Examples

## Examples

In the following example, the traffic class called class1 has the same characteristics as traffic class called class2, with the exception that traffic class class1 has added a destination address as a match criterion. Rather than configuring traffic class class1 line by line, you can enter the **match class-map class2** command. This command allows all of the characteristics in the traffic class called class2 to be included in the traffic class called class1, and you can simply add the new destination address match criterion without reconfiguring the entire traffic class.

```
Router(config)# class-map match-any class2
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 3
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# class-map match-all class1
Router(config-cmap)# match class-map class2
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# exit
```

The following example shows how to combine the characteristics of two traffic classes, one with match-any and one with match-all characteristics, into one traffic class with the **match class-map** command. The result of traffic class called class4 requires a packet to match one of the following three match criteria to be considered a member of traffic class called class 4: IP protocol *and* QoS group 4, destination MAC address 1.1.1, or access group 2. Match criteria IP protocol *and* QoS group 4 are required in the definition of the traffic class named class3 and included as a possible match in the definition of the traffic class named class4 with the **match class-map class3** command.

In this example, only the traffic class called class4 is used with the service policy called policy1.

```
Router(config)# class-map match-all class3
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 4
Router(config-cmap)# exit
Router(config)# class-map match-any class4
Router(config-cmap)# match class-map class3
Router(config-cmap)# match destination-address mac 1.1.1
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |

# match cos

To match a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking, use the **matchcos** command in class-map configuration or policy inline configuration mode. To remove a specific Layer 2 CoS/ISL marking as a match criterion, use the **no** form of this command.

**match cos cos-value** [**cos-value** [**cos-value [cos-value]**]]

**no match cos cos-value** [**cos-value** [**cos-value [cos-value]**]]

## Syntax Description

| **Supported Platforms Other Than the Cisco 10000 Series Routers** | |
|---|---|
| *cos-value* | Specific IEEE 802.1Q/ISL CoS value. The *cos-value* is from 0 to 7; up to four CoS values, separated by a space, can be specified in one **matchcos** statement. |
| Cisco 10000 Series Routers | |
| *cos-value* | Specific packet CoS bit value. Specifies that the packet CoS bit value must match the specified CoS value. The *cos-value* is from 0 to 7; up to four CoS values, separated by a space, can be specified in one **matchcos** statement. |

## Command Default

Packets are not matched on the basis of a Layer 2 CoS/ISL marking.

## Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

## Command History

| Release | Modification |
|---|---|
| 12.1(5)T | This command was introduced. |
| 12.0(25)S | This command was integrated into Cisco IOS Release 12.0(25)S. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

| Release | Modification |
|---|---|
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC and support for the Cisco 7600 series routers was added. |
| 12.4(15)T2 | This command was integrated into Cisco IOS Release 12.4(15)T2. |
| 12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB and support for the Cisco 7300 series router was added. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode. |
| 12.2(58)SE | This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor. |
| 12.2(33)SCF | This command was integrated into Cisco IOS Release 12.2(33)SCF. |
| 3.2SE | This command was integrated into Cisco IOS XE Release 3.2SE. |
| 15.1(2)SNG | This command was integrated into Cisco ASR 901 Series Aggregation Services Routers. |

## Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

**Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE**

You must first enter the **service-policytypeperformance-monitorinline**command.

## Examples

In the following example, the CoS values of 1, 2, and 3 are successful match criteria for the interface that contains the classification policy named cos:

```
Router(config)# class-map cos
Router(config-cmap)# match cos 1 2 3
```

In the following example, classes named voice and video-n-data are created to classify traffic based on the CoS values. QoS treatment is then given to the appropriate packets in the CoS-based-treatment policy map (in this case, the QoS treatment is priority 64 and bandwidth 512). The service policy configured in this example is attached to all packets leaving Fast Ethernet interface 0/0.1. The service policy can be attached to any interface that supports service policies.

```
Router(config)# class-map voice
Router(config-cmap)# match cos 7
Router(config)# class-map video-n-data
Router(config-cmap)# match cos 5
Router(config)# policy-map cos-based-treatment
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 64
Router(config-pmap-c)# exit
Router(config-pmap)# class video-n-data
Router(config-pmap-c)# bandwidth 512
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

```
Router(config)# interface fastethernet0/0.1
Router(config-if)# service-policy output cos-based-treatment
```

## Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria of a CoS value of 2 will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match cos 2
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

## Examples

The following example shows how to match traffic classes for the 802.1p domain with packet CoS values:

```
Router> enable
Router# config terminal
Router(config)# class-map cos7
Router(config-cmap)# match cos 2
Router(config-cmap)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **service-policy type performance-monitor** | Associates a Performance Monitor policy with an interface. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **set cos** | Sets the Layer 2 CoS value of an outgoing packet. |
| **show class-map** | Displays all class maps and their matching criteria. |

# match cos inner

To match the inner cos of QinQ packets on a Layer 2 class of service (CoS) marking, use the **matchcosinner**command in class-map configuration mode. To remove a specific Layer 2 CoS inner tag marking, use the **no** form of this command.

**match cos cos-value**

**no match cos cos-value**

## Syntax Description

| | |
|---|---|
| *cos-value* | Specific IEEE 802.1Q/ISL CoS value. The *cos-value* is from 0 to 7; up to four CoS values can be specified in one **matchcos** statement. |

## Command Default

No match criteria are specified.

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXE | This command was introduced. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |

## Examples

In the following example, the inner CoS-values of 1, 2, and 3 are successful match criteria for the interface that contains the classification policy called cos:

```
Router(config)# class-map cos
Router(config-cmap)# match cos inner 1 2 3
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |

| Command | Description |
|---|---|
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **set cos** | Sets the Layer 2 CoS value of an outgoing packet. |
| **show class-map** | Displays all class maps and their matching criteria. |

# match destination-address mac

To use the destination MAC address as a match criterion, use the **matchdestination-addressmac**command in class-map configuration or policy inline configuration mode. To remove a previously specified destination MAC address as a match criterion, use the **no**form of this command.

**match destination-address mac** *address*

**no match destination-address mac** *address*

## Syntax Description

| | |
|---|---|
| *address* | Destination MAC address to be used as a match criterion. |

## Command Default

No destination MAC address is specified.

## Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)XE | This command was introduced. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode. |
| 12.2(58)SE | This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor. |

## Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

**Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE**

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

## Examples

The following example specifies a class map named macaddress and specifies the destination MAC address to be used as the match criterion for this class:

```
Router(config)# class-map macaddress
Router(config-cmap)# match destination-address mac 00:00:00:00:00:00
```

## Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the specified destination MAC address will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match
destination-address mac 00:00:00:00:00:00
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **service-policy type performance-monitor** | Associates a Performance Monitor policy with an interface. |

# match discard-class

To specify a discard class as a match criterion, use the **matchdiscard-class** command in class-map configuration or policy inline configuration mode. To remove a previously specified discard class as a match criterion, use the **no** form of this command.

**match discard-class** *class-number*

**no match discard-class** *class-number*

## Syntax Description

| | |
|---|---|
| *class-number* | Number of the discard class being matched. Valid values are 0 to 7. |

## Command Default

Packets will not be classified as expected.

## Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode. |
| 12.2(58)SE | This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor. |

## Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

A discard-class value has no mathematical significance. For example, the discard-class value 2 is not greater than 1. The value simply indicates that a packet marked with discard-class 2 should be treated differently than a packet marked with discard-class 1.

Packets that match the specified discard-class value are treated differently from packets marked with other discard-class values. The discard-class is a matching criterion only, used in defining per hop behavior (PHB) for dropping traffic.

**Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE**

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

## Examples

The following example shows that packets in discard class 2 are matched:

```
Router(config)# class-map d-class-2
Router(config-cmap)# match discard-class 2
```

## Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria specified by discard-class 2 will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match
discard-class 2
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **service-policy type performance-monitor** | Associates a Performance Monitor policy with an interface. |
| **set discard-class** | Marks a packet with a discard-class value. |

# match dscp

To identify one or more differentiated service code point (DSCP), Assured Forwarding (AF), and Certificate Server (CS) values as a match criterion, use the **match dscp** command in class-map configuration or policy inline configuration mode. To remove a specific DSCP value from a class map, use the **no** form of this command.

**match [ip] dscp** *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*]

**no match [ip] dscp** *dscp-value*

## Syntax Description

| | |
|---|---|
| **ip** | (Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets.<br>**Note** For the Cisco 10000 series routers, the **ip** keyword is required. |
| *dscp-value* | The DSCP value used to identify a DSCP value. For valid values, see the "Usage Guidelines" section. |

## Command Default

No match criteria are configured.

## Command Modes

class-map configuration (config-cmap) policy inline configuration (config-if-spolicy-inline)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. This command replaces the **match ip dscp** command. |
| 12.0(28)S | This command was integrated into Cisco IOS Release 12.0(28)S for support in IPv6. |
| 12.0(17)SL | This command was integrated into Cisco IOS Release 12.0(17)SL and implemented on the Cisco 10000 series routers. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 Series Routers. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode. |

| Release | Modification |
|---|---|
| 12.2(58)SE | This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor. |

## Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

**Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE**

You must first enter the **service-policy type performance-monitor inline** command.

**DSCP Values**

You must enter one or more differentiated service code point (DSCP) values. The command may include any combination of the following:

- Numbers (0 to 63) representing differentiated services code point values
- AF numbers (for example, af11) identifying specific AF DSCPs
- CS numbers (for example, cs1) identifying specific CS DSCPs
- **default—**Matches packets with the default DSCP.
- **ef—**Matches packets with EF DSCP.

For example, if you wanted the DCSP values of 0, 1, 2, 3, 4, 5, 6, or 7 (note that only one of the IP DSCP values must be a successful match criterion, not all of the specified DSCP values), enter the **match dscp 01234567** command.

This command is used by the class map to identify a specific DSCP value marking on a packet. In this context, *dscp-value* arguments are used as markings only and have no mathematical significance. For instance, the *dscp-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *dscp-value* of 2 is different than a packet marked with the *dscp-value* of 1. The treatment of these marked packets is defined by the user through the setting of Quality of Service (QoS) policies in policy-map class configuration mode.

**Match Packets on DSCP Values**

To match DSCP values for IPv6 packets only, the **match protocol ipv6** command must also be used. Without that command, the DSCP match defaults to match both IPv4 and IPv6 packets.

To match DSCP values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword the match occurs on both IPv4 and IPv6 packets. Alternatively, the **match protocol ip** command may be used with **match dscp** to classify only IPv4 packets.

After the DSCP bit is set, other QoS features can then operate on the bit settings.

The network can give priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain); data is then queued according to the precedence. Weighted fair queueing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Random Early Detection (WRED) can ensure that high-precedence traffic has lower loss rates than other traffic during times of congestion.

**Cisco 10000 Series Routers**

The Cisco 10000 series routers support DSCP matching of IPv4 packets only. You must include the ip keyword when specifying the DSCP values to use as match criterion.

You cannot use the set ip dscp command with the set ip precedence command to mark the same packet. DSCP and precedence values are mutually exclusive. A packet can have one value or the other, but not both.

## Examples

The following example shows how to set multiple match criteria. In this case, two IP DSCP values and one AF value.

```
Router(config)# class-map map1
Router(config-cmap)# match dscp 1 2 af11
```

## Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criterion specified by DSCP value 2 will be monitored based on the parameters specified in the flow monitor configuration named fm-2:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match dscp 2
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# end
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **match protocol ip** | Matches DSCP values for packets. |
| **match protocol ipv6** | Matches DSCP values for IPv6 packets. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **service-policy type performance-monitor** | Associates a Performance Monitor policy with an interface. |
| **set dscp** | Marks the DSCP value for packets within a traffic class. |
| **show class-map** | Displays all class maps and their matching criteria. |

# match field

**Note** Effective with Cisco IOS Release 15.2(4)M, the **match field** command is not available in Cisco IOS software.

To configure the match criteria for a class map on the basis of the fields defined in the protocol header description files (PHDFs), use the **match field** command in class-map configuration mode. To remove the specified match criteria, use the **no** form of this command.

**match field** *protocol protocol-field* {**eq [mask]**| **neq [mask]**| **gt**| **lt**| **range** *range*| **regex** *string*} *value* [**next** *next-protocol*]

**no match field** *protocol protocol-field* {**eq [mask]**| **neq [mask]**| **gt**| **lt**| **range** *range*| **regex** *string*} *value* [**next** *next-protocol*]

## Syntax Description

| | |
|---|---|
| *protocol* | Name of protocol whose PHDF has been loaded onto a router. |
| *protocol field* | *Match criteria is based upon the specified f*ield *within the loaded protocol.* |
| eq | *Match criteria is met if the* packet is equal to the specified value or mask. |
| neq | *Match criteria is met if the* packet is not equal to the specified value or mask. |
| mask *mask* | (Optional) Can be used when the **eq** or the **neq** keywords are issued. |
| gt | *Match criteria is met if the* packet does not exceed the specified value. |
| lt | *Match criteria is met if the* packet is less than the specified value. |
| range *range* | Match criteria is based upon a lower and upper boundary protocol field range. |
| regex *string* | Match criteria is based upon a string that is to be matched. |
| *value* | Value for which the packet must be in accordance with. |

| | |
|---|---|
| **next** *next-protocol* | Specify the next protocol within the stack of protocols that is to be used as the match criteria. |

**Command Default** No match criteria are configured.

**Command Modes** Class-map configuration

**Command History**

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |
| 12.2(18)ZY | This command was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA). |
| Cisco IOS XE 2.2 | This command was integrated into Cisco IOS XE Release 2.2. |
| 15.2(4)M | This command was removed from the Cisco IOS software. |

**Usage Guidelines** Before issuing the **match-field** command, you must load a PHDF onto the router via the **load protocol** command. Thereafter, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

Match criteria are defined via a start point, offset, size, value to match, and mask. A match can be defined on a pattern with any protocol field.

**Examples** The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header.

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf
class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp
class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp
class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster3
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030
policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
 drop
```

```
policy-map type access-control fpm-udp-policy
 class blaster3
 drop
policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy
interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **load protocol** | Loads a PHDF onto a router. |
| **match start** | Configures the match criteria for a class map on the basis of the datagram header (Layer 2) or the network header (Layer 3). |

# match flow pdp

To specify a Packet Data Protocol (PDP) flow as a match criterion in a class map, use the **matchflowpdp** command in class-map configuration mode. To remove a PDP flow as a match criterion, use the **no** form of this command.

**match flow pdp**

**no match flow pdp**

## Syntax Description

This command has no arguments or keywords.

## Command Default

A PDP flow is not specified as a match criterion.

## Command Modes

Class-map configuration (config-cmap)

## Command History

| Release | Modification |
|---|---|
| 12.3(8)XU | This command was introduced. |
| 12.3(11)YJ | This command was integrated into Cisco IOS Release 12.3(11)YJ. |
| 12.3(14)YQ | This command was integrated into Cisco IOS Release 12.3(14)YQ. |
| 12.3(14)YU | This command was integrated into Cisco IOS Release 12.3(14)YU. |
| 12.4(2)XB | This command was integrated into Cisco IOS Release 12.4(2)XB. |
| 12.4(9)T | This command was integrated into Cisco IOS Release 12.4(9)T. |

## Usage Guidelines

The **matchflowpdp** command allows you to match and classify traffic on the basis of a PDP flow.

The **matchflowpdp** command is included with the Flow-Based QoS for GGSN feature available with Cisco IOS Release 12.4(9)T. The Flow-Based QoS for GGSN feature is designed specifically for the Gateway General Packet Radio Service (GPRS) Support Node (GGSN).

**Per-PDP Policing**

The Flow-Based QoS for GGSN feature includes per-PDP policing (session-based policing).

The **matchflowpdp** command (when used in conjunction with the **class-map** command, the **policy-map** command, the **policeratepdp** command, and the **service-policy** command) allows you to configure per-PDP policing (session-based policing) for downlink traffic on a GGSN.

Note the following points related to per-PDP policing:

- When using the **class-map** command to define a class map for PDP flow classification, do not use the **match-any**keyword.
- Per-PDP policing functionality requires that you configure Universal Mobile Telecommunications System (UMTS) quality of service (QoS). For information on configuring UMTS QoS, see the "Configuring QoS on the GGSN" section of the Cisco GGSN Release 6.0 Configuration Guide , Cisco IOS Release 12.4(2)XB.
- The policy map created to configure per-PDP policing cannot contain multiple classes within which only the **matchflowpdp** command has been specified. In other words, if there are multiple classes in the policy map, the **matchflowpdp**command must be used in conjunction with another match statement (for example, **matchprecedence**) in at least one class.

**For More Information**

For more information about the GGSN, along with the instructions for configuring the Flow-Based QoS for GGSN feature, see the Cisco GGSN Release 6.0 Configuration Guide , Cisco IOS Release 12.4(2)XB.

**Note** To configure the Flow-Based QoS for GGSN feature, follow the instructions in the section called " Configuring Per-PDP Policing ."

For more information about the GGSN-specific commands, see the Cisco GGSN Release 6.0 Command Reference , Cisco IOS Release 12.4(2)XB.

## Examples

The following example specifies PDP flows as the match criterion in a class map named "class-pdp":

```
class-map class-pdp
 match flow pdp
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **match precedence** | Identifies IP precedence values as match criteria. |
| **police rate pdp** | Configures PDP traffic policing using the police rate. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **service-policy** | Attaches a policy map to an interface. |

# match fr-dlci

To specify the Frame Relay data-link connection identifier (DLCI) number as a match criterion in a class map, use the **matchfr-dlci**command in class-map configuration or policy inline configuration mode. To remove a previously specified DLCI number as a match criterion, use the **no** form of this command.

**match fr-dlci** *dlci-number*

**no match fr-dlci** *dlci-number*

## Syntax Description

| | |
|---|---|
| *dlci-number* | Number of the DLCI associated with the packet. |

## Command Default

No DLCI number is specified.

## Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode. |
| 12.2(58)SE | This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor. |

## Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

This match criterion can be used in main interfaces and point-to-multipoint subinterfaces in Frame Relay networks, and it can also be used in hierarchical policy maps.

**Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE**

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

## Examples

In the following example a class map named “class1” has been created and the Frame Relay DLCI number of 500 has been specified as a match criterion. Packets matching this criterion are placed in class1.

```
Router(config)# class-map class1
Router(config-cmap)# match fr-dlci 500
```

## Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the Frame Relay DLCI number of 500 will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match
fr-dlci 500
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **service-policy type performance-monitor** | Associates a Performance Monitor policy with an interface. |
| **show class-map** | Displays all class maps and their matching criteria. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# match input vlan

To configure a class map to match incoming packets that have a specific virtual local area network (VLAN) ID, use the **matchinputvlan**command in class map configuration mode. To remove the matching of VLAN IDs, use the **no** form of this command.

**match input vlan** *input-vlan-list*

**no match input vlan** *input-vlan-list*

## Syntax Description

| | |
|---|---|
| *input-vlan-list* | One or more VLAN IDs to be matched. The valid range for VLAN IDs is from 1 to 4094, and the list of VLAN IDs can include one or all of the following:<br>• Single VLAN IDs, separated by spaces. For example: 100 200 300<br>• One or more ranges of VLAN IDs, separated by spaces. For example: 1-1024 2000-2499 |

## Command Default

By default, no matching is done on VLAN IDs.

## Command Modes

Class map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXE | This command was introduced for Cisco Catalyst 6500 series switches and Cisco 7600 series routers. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

The **matchinputvlan** command allows you to create a class map that matches packets with one or more specific VLAN IDs, as they were received on the input (ingress) interface. This enables hierarchical Quality of Service (HQoS) for Ethernet over MPLS (EoMPLS) Virtual Circuits (VC), allowing parent and child relationships between QoS class maps and policy maps. This in turn enables service providers to easily classify and shape traffic for a particular EoMPLS network.

In EoMPLS applications, the parent class map typically specifies the maximum bandwidth for all of the VCs in a specific EoMPLS network. Then the child class maps perform other QoS operations, such as traffic shaping, on a subset of this traffic.

Do not confuse the **matchinputvlan** command with the **matchvlan** command, which is also a class-map configuration command.

- The **matchvlan** command matches the VLAN ID on packets for the particular interface at which the policy map is applied. Policy maps using the **matchvlan** command can be applied to either ingress or egress interfaces on the router, using the **service-policy** {**input** | **output**} command.
- The **matchinputvlan** command matches the VLAN ID that was on packets when they were received on the ingress interface on the router. Typically, policy maps using the **matchinputvlan** command are applied to egress interfaces on the router, using the **service-policyoutput** command.

The **matchinputvlan** command can also be confused with the **matchinput-interfacevlan** command, which matches packets being received on a logical VLAN interface that is used for inter-VLAN routing.

**Tip** Because class maps also support the **matchinput-interface** command, you cannot abbreviate the **input** keyword when giving the **matchinputvlan** command.

**Note** The **matchinputvlan** command cannot be used only on Layer 2 LAN ports on FlexWAN, Enhanced FlexWAN, and Optical Service Modules (OSM) line cards.

The following restrictions apply when using the **matchinputvlan** command:

- You cannot attach a policy with **matchinputvlan** to an interface if you have already attached a service policy to a VLAN interface (a logical interface that has been created with the **interfacevlan** command).
- Class maps that use the **matchinputvlan** command support only the **match-any** option. You cannot use the **match-all** option in class maps that use the **matchinputvlan** command.
- If the parent class contains a class map with a **matchinputvlan** command, you cannot use a **matchexp** command in a child class map.

## Examples

The following example creates a class map and policy map that matches packets with a VLAN ID of 1000. The policy map shapes this traffic to a committed information rate (CIR) value of 10 Mbps (10,000,000 bps). The final lines then apply this policy map to a specific gigabit Ethernet WAN interface.

```
Router# configure terminal
Router(config)# class-map match-any vlan1000
Router(config-cmap)# match input vlan 1000
Router(config-cmap)# exit
Router(config)# policy-map policy1000
Router(config-pmap)# class vlan1000
Router(config-pmap-c)# exit
Router(config-pmap)# shape average 10000000
Router(config-pmap)# interface GE-WAN 3/0
Router(config-if)# service-policy output policy1000
Router(config-if)#
```

The following example shows a class map being configured to match VLAN IDs 100, 200, and 300:

```
Router# configure terminal

Router(config)# class-map match-any hundreds

Router(config-cmap)# match input vlan 100 200 300

Router(config-cmap)#
```

The following example shows a class map being configured to match all VLAN IDs from 2000 to 2999 inclusive:

```
Router# configure terminal

Router(config)# class-map match-any vlan2000s

Router(config-cmap)# match input vlan 2000-2999

Router(config-cmap)#
```

The following example shows a class map being configured to match both a range of VLAN IDs, as well as specific VLAN IDs:

```
Router# configure terminal

Router(config)# class-map match-any misc

Router(config-cmap)# match input vlan 1 5 10-99 2000-2499

Router(config-cmap)#
```

## Related Commands

| Command | Description |
|---|---|
| **clear cef linecard** | Clears Cisco Express Forwarding (CEF) information on one or more line cards, but does not clear the CEF information on the main route processor (RP). This forces the line cards to synchronize their CEF information with the information that is on the RP. |
| **match qos-group** | Identifies a specified QoS group value as a match criterion. |
| **mls qos trust** | Sets the trusted state of an interface, to determine which incoming QoS field on a packet, if any, should be preserved. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |

| Command | Description |
|---|---|
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |
| **show platform qos policy-map** | Displays the type and number of policy maps that are configured on the router. |

# match input-interface

To configure a class map to use the specified input interface as a match criterion, use the **match input-interface** command in class-map configuration or policy inline configuration mode. To remove the input interface match criterion from a class map, use the **no** form of this command.

**match input-interface** *interface-name*

**no match input-interface** *interface-name*

## Syntax Description

| | |
|---|---|
| *interface-name* | Name of the input interface to be used as match criteria. |

## Command Default

No match criteria are specified.

## Command Modes

Class-map configuration (config-cmap)

Policy inline configuration (config-if-spolicy-inline)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE. |
| 12.0(7)S | This command was integrated into Cisco IOS Release 12.0(7)S. |
| 12.0(17)SL | This command was enhanced to include matching on the input interface. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode. |
| 12.2(58)SE | This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor. |

## Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

**Note** With CSCtx62310, the minimum string you must enter to uniquely identify this command is **match input-**. The device no longer accepts **match input** as an abbreviated version of this command.

### Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

To enter policy inline configuration mode, you must first enter the **service-policy type performance-monitor inline** command.

### Supported Platforms Other Than Cisco 10000 Series Routers

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria including input interfaces, access control lists (ACLs), protocols, quality of service (QoS) labels, and experimental (EXP) field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match input-interface** command specifies the name of an input interface to be used as the match criterion against which packets are checked to determine if they belong to the class specified by the class map.

To use the **match input-interface** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**
- **match protocol**

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

### Cisco 10000 Series Routers

For CBWFQ, you define traffic classes based on match criteria including input interfaces, ACLs, protocols, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

To use the **match input-interface** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

## Examples

The following example specifies a class map named ethernet1 and configures the input interface named ethernet1 to be used as the match criterion for this class:

```
Router(config)# class-map ethernet1
Router(config-cmap)# match input-interface ethernet1
```

## Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria of the input interface named ethernet1 will be monitored based on the parameters specified in the flow monitor configuration named fm-2:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match input-interface ethernet 1
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **match access-group** | Configures the match criteria for a class map based on the specified ACL. |
| **match mpls experimental** | Configures a class map to use the specified EXP field value as a match criterion. |
| **match protocol** | Configures the match criteria for a class map on the basis of the specified protocol. |
| **service-policy type performance-monitor** | Associates a Performance Monitor policy with an interface. |

# match ip dscp

The **matchipdscp**command is replaced by the match dscpcommand. See the match dscpcommand for more information.

# match ip precedence

The **matchipprecedence**command is replaced by the match precedencecommand. See the match precedencecommand for more information.

# match ip rtp

To configure a class map to use the Real-Time Protocol (RTP) port as the match criterion, use the **matchiprtp**command in class-map configuration or policy inline configuration mode. To remove the RTP port match criterion, use the **no** form of this command.

**match ip rtp** *starting-port-number port-range*

**no match ip rtp**

## Syntax Description

| | |
|---|---|
| *starting-port-number* | The starting RTP port number. Values range from 2000 to 65535. |
| *port-range* | The RTP port number range. Values range from 0 to 16383. |

## Command Default

No match criteria are specified.

## Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

## Command History

| Release | Modification |
|---|---|
| 12.1(2)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode. |
| 12.2(58)SE | This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor. |

## Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

This command is used to match IP RTP packets that fall within the specified port range. It matches packets destined to all even User Datagram Port (UDP) port numbers in the range from the *starting port number* argument to the *starting port number* plus the *port range* argument.

Use of an RTP port range as the match criterion is particularly effective for applications that use RTP, such as voice or video.

**Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE**

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

## Examples

The following example specifies a class map named ethernet1 and configures the RTP port number 2024 and range 1000 to be used as the match criteria for this class:

```
Router(config)# class-map ethernet1
Router(config-cmap)# match ip rtp 2024 1000
```

## Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria of RTP port number 2024 and range 1000 will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match
ip rtp 2024 1000
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **service-policy type performance-monitor** | Associates a Performance Monitor policy with an interface. |
| **ip rtp priority** | Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports. |
| **match access-group** | Configures the match criteria for a class map based on the specified ACL number. |

# match mpls experimental

To configure a class map to use the specified value or values of the experimental (EXP) field as a match criteria, use the **matchmplsexperimental**command in class-map configuration mode. To remove the EXP field match criteria from a class map, use the **no** form of this command.

**match mpls experimental** *number*

**no match mpls experimental** *number*

## Syntax Description

| | |
|---|---|
| *number* | EXP field value (any number from 0 through 7) to be used as a match criterion. You can specify multiple values, separated by a space (for example, 3 4 7). |

## Command Default

No match criteria are specified.

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(7)XE1 | This command was introduced. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.2(4)T | This command was implemented on the Cisco MGX 8850 switch and the MGX 8950 switch with a Cisco MGX RPM-PR card. |
| 12.2(4)T2 | This command was implemented on the Cisco 7500 series. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

**Supported Platforms Other Than the Cisco 10000 Series**

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria such as input interfaces, access control lists (ACLs), protocols, quality of service (QoS) labels, and experimental (EXP) field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **matchmplsexperimental** command specifies the name of an EXP field value to be used as the match criterion against which packets are compared to determine if they belong to the class specified by the class map.

To use the **matchmplsexperimental** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**
- **match protocol**

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

**Cisco 10000 Series**

This command is available only on the ESR-PRE1 module.

For CBWFQ, you define traffic classes based on match criteria such as input interfaces, ACLs, protocols, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

To use the **matchmplsexperimental** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

## Examples

The following example specifies a class map called ethernet1 and configures the Multiprotocol Label Switching (MPLS) experimental values of 1 and 2 to be used as the match criteria for this class:

```
Router(config)# class-map ethernet1
Router(config-cmap)# match mpls experimental 1 2
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **match access-group** | Configures the match criteria for a class map based on the specified ACL. |
| **match input-interface** | Configures a class map to use the specified input interface as a match criterion. |
| **match mpls experimental topmost** | Matches the EXP value in the topmost label. |
| **match protocol** | Matches traffic by a particular protocol. |

| Command | Description |
|---|---|
| **match qos-group** | Configures the match criteria for a class map based on the specified protocol. |

# match mpls experimental topmost

To match the experimental (EXP) value in the topmost label header, use the **matchmplsexperimentaltopmost**command in class-map configuration or policy inline configuration mode. To remove the EXP match criterion, use the no form of this command.

**match mpls experimental topmost number**

**no match mpls experimental topmost number**

## Syntax Description

| | |
|---|---|
| *number* | Multiprotocol Label Switching (MPLS) EXP field in the topmost label header. Valid values are 0 to 7. |

## Command Default

No EXP match criterion is configured for the topmost label header.

## Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB. |
| Cisco IOS XE Release 2.3 | This command was integrated into Cisco IOS XE Release 2.3. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode. |
| 12.2(58)SE | This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor. |
| 12.2(33)SCF | This command was integrated into Cisco IOS Release 12.2(33)SCF. |

## Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

You can enter this command on the input interfaces and the output interfaces. It will match only on MPLS packets.

**Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE**

You must first enter the **service-policytypeperformance-monitorinline**command.

## Examples

The following example shows that the EXP value 3 in the topmost label header is matched:

```
Router(config)# class-map mpls exp
Router(config-cmap)# match mpls experimental topmost 3
```

## Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria of a EXP value of 3 in the topmost label header will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match mpls experimental topmost 3
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **service-policy type performance-monitor** | Associates a Performance Monitor policy with an interface. |
| **set mpls experimental topmost** | Sets the MPLS EXP field value in the topmost MPLS label header at the input or output interfaces. |

# match not

To specify the single match criterion value to use as an unsuccessful match criterion, use the **matchnot**command inclass-map configuration or policy inline configuration mode. To remove a previously specified source value to not use as a match criterion, use the **no**form of this command.

**match not** *match-criterion*

**no match not** *match-criterion*

## Syntax Description

| | |
|---|---|
| *match-criterion* | The match criterion value that is an unsuccessful match criterion. All other values of the specified match criterion will be considered successful match criteria. |

## Command Default

No unsuccessful match criterion is configured.

## Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)XE | This command was introduced. |
| 12.0(5)T | This command was integrated into Cisco IOS Release 12.0(5)T. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode. |
| 12.2(58)SE | This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor. |

## Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

The **matchnot**command is used to specify a quality of service (QoS) policy value that is not used as a match criterion. When the**matchnot** command is used, all other values of that QoS policy become successful match criteria.

For instance, if the **matchnotqos-group4** command is issued in QoS class-map configuration mode, the specified class will accept all QoS group values except 4 as successful match criteria.

**Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE**

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

## Examples

In the following traffic class, all protocols except IP are considered successful match criteria:

```
Router(config)# class-map noip
Router(config-cmap)# match not protocol ip
```

## Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 for all protocols except IP will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match not protocol ip
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **service-policy type performance-monitor** | Associates a Performance Monitor policy with an interface. |

# match packet length (class-map)

To specify the Layer 3 packet length in the IP header as a match criterion in a class map, use the **matchpacketlength** command in class-map configuration or policy inline configuration mode. To remove a previously specified Layer 3 packet length as a match criterion, use the **no** form of this command.

**match packet length** {**max** *maximum-length-value* [**min** *minimum-length-value*]| **min** *minimum-length-value* [**max** *maximum-length-value*]}

**no match packet length** {**max** *maximum-length-value* [**min** *minimum-length-value*]| **min** *minimum-length-value* [**max** *maximum-length-value*]}

## Syntax Description

| | |
|---|---|
| **max** | Indicates that a maximum value for the Layer 3 packet length is to be specified. |
| *maximum-length-value* | Maximum length value of the Layer 3 packet length, in bytes. The range is from 1 to 2000. |
| **min** | Indicates that a minimum value for the Layer 3 packet length is to be specified. |
| *minimum-length-value* | Minimum length value of the Layer 3 packet length, in bytes. The range is from 1 to 2000. |

## Command Default

The Layer 3 packet length in the IP header is not used as a match criterion.

## Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| Cisco IOS XE Release 2.2 | This command was integrated into Cisco IOS XE Release 2.2 and implemented on the Cisco ASR 1000 Series Routers. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode. |

| Release | Modification |
|---|---|
| 12.2(58)SE | This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor. |

## Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

This command considers only the Layer 3 packet length in the IP header. It does not consider the Layer 2 packet length in the IP header.

When using this command, you must at least specify the maximum or minimum value. However, you do have the option of entering both values.

If only the minimum value is specified, a packet with a Layer 3 length greater than the minimum is viewed as matching the criterion.

If only the maximum value is specified, a packet with a Layer 3 length less than the maximum is viewed as matching the criterion.

**Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE**

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

## Examples

In the following example a class map named “class 1” has been created, and the Layer 3 packet length has been specified as a match criterion. In this example, packets with a minimum Layer 3 packet length of 100 bytes and a maximum Layer 3 packet length of 300 bytes are viewed as meeting the match criteria.

```
Router(config)# class-map match-all class1
Router(config-cmap)# match packet length min 100 max 300
```

## Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria of a minimum Layer 3 packet length of 100 bytes and a maximum Layer 3 packet length of 300 bytes will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match packet length min 100 max 300
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **service-policy type performance-monitor** | Associates a Performance Monitor policy with an interface. |
| **show class-map** | Displays all class maps and their matching criteria. |

| Command | Description |
|---|---|
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# match port-type

To match the access policy on the basis of the port for a class map, use the **matchport-type** command in class-map configuration mode. To delete the port type, use the **no** form of this command.

**match port-type** {**routed**| **switched**}

**no match port-type** {**routed**| **switched**}

## Syntax Description

| | |
|---|---|
| **routed** | Matches the routed interface. Use this keyword if the class map has to be associated with only a routed interface. |
| **switched** | Matches the switched interface. Use this keyword if the class map has to be associated with only a switched interface. |

## Command Default

Access policy is not matched.

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

This command is used because, on the basis of the port on which a user is connecting, the access policies that are applied to it can be different.

## Examples

The following example shows that an access policy has been matched on the basis of the port for a class map:

Router(config-cmap)# **matchport-typerouted**

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **match tag (class-map)** | Specifies the tag to be matched for a tag type of class map. |

# match precedence

To identify IP precedence values to use as the match criterion, use the **matchprecedence** command in class-map configuration or policy inline configuration mode. To remove IP precedence values from a class map, use the **no** form of this command.

**match [ip] precedence** {*precedence-criteria1*| *precedence-criteria2*| *precedence-criteria3*| *precedence-criteria4*}

**no match [ip] precedence** {*precedence-criteria1*| *precedence-criteria2*| *precedence-criteria3*| *precedence-criteria4*}

## Syntax Description

| | |
|---|---|
| **ip** | (Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets.<br>**Note** For the Cisco 10000 series routers, the **ip** keyword is required. |
| *precedence-criteria1*<br>*precedence-criteria2*<br>*precedence-criteria3*<br>*precedence-criteria4* | Identifies the precedence value. You can enter up to four different values, separated by a space. See the "Usage Guidelines" section for valid values. |

## Command Default

No match criterion is configured.

## Command Modes

class-map configuration (config-cmap) policy inline configuration (config-if-spolicy-inline)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. This command replaces the **matchipprecedence** command. |
| 12.0(17)SL | This command was integrated into Cisco IOS Release 12.0(17)SL and implemented on the Cisco 10000 series routers. |
| 12.0(28)S | This command was integrated into Cisco IOS Release 12.0(28)S for IPv6. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode. |

| Release | Modification |
|---|---|
| 12.2(58)SE | This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor. |
| Cisco IOS XE Release 3.6 | This command was implemented on the Cisco ASR 903 Router. |

## Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

You can enter up to four matching criteria, a number abbreviation (0 to 7) or criteria names (critical, flash, and so on), in a single match statement. For example, if you wanted the precedence values of 0, 1, 2, or 3 (note that only one of the precedence values must be a successful match criterion, not all of the specified precedence values), enter the **matchipprecedence0123**command. The *precedence-criteria* numbers are not mathematically significant; that is, the *precedence-criteria* of 2 is not greater than 1. The way that these different packets are treated depends upon quality of service (QoS) policies, set in policy-map configuration mode.

You can configure a QoS policy to include IP precedence marking for packets entering the network. Devices within your network can then use the newly marked IP precedence values to determine how to treat the packets. For example, class-based weighted random early detection (WRED) uses IP precedence values to determine the probability that a packet is dropped. You can also mark voice packets with a particular precedence. You can then configure low-latency queueing (LLQ) to place all packets of that precedence into the priority queue.

**Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE**

You must first enter the **service-policytypeperformance-monitorinline** command.

**Matching Precedence for IPv6 and IPv4 Packets on the Cisco 7600 and 10000 and Series Routers**

On the Cisco 7600 series and 10000 series routers, you set matching criteria based on precedence values for only IPv6 packets using the **matchprotocol**command with the **ipv6** keyword. Without that keyword, the precedence match defaults to match both IPv4 and IPv6 packets. You set matching criteria based on precedence values for IPv4 packets only using the **ip** keyword. Without the **ip** keyword the match occurs on both IPv4 and IPv6 packets.

**Precedence Values and Names**

The following table lists all criteria conditions by value, name, binary value, and recommended use. You may enter up to four criteria, each separated by a space. Only one of the precedence values must be a successful match criterion. The table below lists the IP precedence values.

***Table 9: IP Precedence Values***

| Precedence Value | Precedence Name | Binary Value | Recommended Use |
|---|---|---|---|
| 0 | routine | 000 | Default marking value |
| 1 | priority | 001 | Data applications |
| 2 | immediate | 010 | Data applications |
| 3 | flash | 011 | Call signaling |

| Precedence Value | Precedence Name | Binary Value | Recommended Use |
|---|---|---|---|
| 4 | flash-override | 100 | Video conferencing and streaming video |
| 5 | critical | 101 | Voice |
| 6 | internet (control) | 110 | Network control traffic (such as routing, which is typically precedence 6) |
| 7 | network (control) | 111 | |

Do not use IP precedence 6 or 7 to mark packets, unless you are marking control packets.

## Examples

## Examples

The following example shows how to configure the service policy named priority50 and attach service policy priority50 to an interface, matching for IPv4 traffic only. In a network where both IPv4 and IPv6 are running, you might find it necessary to distinguish between the protocols for matching and traffic segregation. In this example, the class map named ipprec5 will evaluate all IPv4 packets entering Fast Ethernet interface 1/0/0 for a precedence value of 5. If the incoming IPv4 packet has been marked with the precedence value of 5, the packet will be treated as priority traffic and will be allocated with bandwidth of 50 kbps.

```
Router(config)# class-map ipprec5
Router(config-cmap)# match ip precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority50
```

## Examples

The following example shows the same service policy matching on precedence for IPv6 traffic only. Notice that the **match protocol** command with the **ipv6** keyword precedes the **match precedence** command. The **match protocol** command is required to perform matches on IPv6 traffic alone.

```
Router(config)# class-map ipprec5
Router(config-cmap)# match protocol ipv6
Router(config-cmap)# match precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority50
```

## Examples

The following example shows how to use policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criterion

of a match precedence of 4 will be monitored based on the parameters specified in the flow monitor configuration named fm-2:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match precedence 4
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# end
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **match protocol** | Configures the match criteria for a class map on the basis of a specified protocol. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **service-policy type performance-monitor** | Associates a Performance Monitor policy with an interface. |
| **set ip precedence** | Sets the precedence value in the IP header. |
| **show class-map** | Displays all class maps and their matching criteria, or a specified class map and its matching criteria. |

# match protocol

To configure the match criterion for a class map on the basis of a specified protocol, use the **matchprotocol** command in class-map configuration or policy inline configuration mode. To remove the protocol-based match criterion from the class map, use the **no** form of this command.

**match protocol** *protocol-name*

**no match protocol** *protocol-name*

## Syntax Description

| | |
|---|---|
| *protocol-name* | Name of the protocol (for example, bgp) used as a matching criterion. See the "Usage Guidelines" for a list of protocols supported by most routers. |

## Command Default

No match criterion is configured.

## Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE. |
| 12.0(7)S | This command was integrated into Cisco IOS Release 12.0(7)S. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(13)E | This command was integrated into Cisco IOS Release 12.1(13)E and implemented on Catalyst 6000 family switches without FlexWAN modules. |
| 12.2(8)T | This command was integrated into Cisco IOS Release 12.2(8)T. |
| 12.2(13)T | This command was modified to remove **apollo**, **vines**, and **xns** from the list of protocols used as matching criteria. These protocols were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems (XNS) were removed in this release. The IPv6 protocol was added to support matching on IPv6 packets. |
| 12.0(28)S | This command was integrated into Cisco IOS Release 12.0(28)S for IPv6. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(17a)SX1 | This command was integrated into Cisco IOS Release 12.2(17a)SX1. |

| Release | Modification |
|---|---|
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE and implemented on the Supervisor Engine 720. |
| 12.4(6)T | This command was modified. The Napster protocol was removed because it is no longer supported. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2 and implemented on the Cisco 10000 series routers. |
| 12.2(18)ZY | This command was integrated into Cisco IOS Release 12.2(18)ZY. This command was modified to enhance Network-Based Application Recognition (NBAR) functionality on the Catalyst 6500 series switch that is equipped with the Supervisor 32/programmable intelligent services accelerator (PISA) engine. |
| 12.4(15)XZ | This command was integrated into Cisco IOS Release 12.4(15)XZ. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T and implemented on the Cisco 1700, Cisco 1800, Cisco 2600, Cisco 2800, Cisco 3700, Cisco 3800, Cisco 7200, and Cisco 7300 series routers. |
| Cisco IOS XE Release 2.2 | This command was integrated into Cisco IOS XE Release 2.2 and implemented on the Cisco ASR 1000 Series Routers. |
| Cisco IOS XE Release 3.1S | This command was modified. Support for more protocols was added. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode. |
| 12.2(58)SE | This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor. |

## Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

**Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE**

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

**Supported Platforms Other Than Cisco 7600 Routers and Cisco 10000 Series Routers**

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria protocols, access control lists (ACLs), input interfaces, quality of service (QoS) labels, and Experimental (EXP) field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **matchprotocol** command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

The **matchprotocolipx** command matches packets in the output direction only.

To use the **matchprotocol** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

To configure NBAR to match protocol types that are supported by NBAR traffic, use the **matchprotocol(NBAR)**command.

**Cisco 7600 Series Routers**

The **matchprotocol** command in QoS class-map configuration configures NBAR and sends all traffic on the port, both ingress and egress, to be processed in the software on the Multilayer Switch Feature Card 2 (MSFC2).

For CBWFQ, you define traffic classes based on match criteria like protocols, ACLs, input interfaces, QoS labels, and Multiprotocol Label Switching (MPLS) EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **matchprotocol**command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

If you want to use the **matchprotocol**command, you must first enter the **class-map** command to specify the name of the class to which you want to establish the match criteria.

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

This command can be used to match protocols that are known to the NBAR feature. For a list of protocols supported by NBAR, see the “Classification” part of the *Cisco IOS Quality of Service Solutions Configuration Guid*e.

**Cisco 10000 Series Routers**

For CBWFQ, you define traffic classes based on match criteria including protocols, ACLs, input interfaces, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **matchprotocol** command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

The **matchprotocolipx** command matches packets in the output direction only.

To use the **matchprotocol** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

If you are matching NBAR protocols, use the **matchprotocol**(NBAR) command.

**Match Protocol Command Restrictions (Catalyst 6500 Series Switches Only)**

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) on the basis of a protocol type or application. You can create as many traffic classes as needed.

Cisco IOS Release 12.2(18)ZY includes software intended for use on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine. For this release and platform, note the following restrictions for using policy maps and **matchprotocol** commands:

- A single traffic class can be configured to match a maximum of 8 protocols or applications.
- Multiple traffic classes can be configured to match a cumulative maximum of 95 protocols or applications.

### Supported Protocols

The table below lists the protocols supported by most routers. Some routers support a few additional protocols. For example, the Cisco 7600 router supports the AARP and DECnet protocols, while the Cisco 7200 router supports the directconnect and PPPOE protocols. For a complete list of supported protocols, see the online help for the **matchprotocol** command on the router that you are using.

***Table 10: Supported Protocols***

| Protocol Name | Description |
|---|---|
| 802-11-iapp | IEEE 802.11 Wireless Local Area Networks Working Group Internet Access Point Protocol |
| ace-svr | ACE Server/Propagation |
| aol | America-Online Instant Messenger |
| appleqtc | Apple QuickTime |
| **arp** * | IP Address Resolution Protocol (ARP) |
| **bgp** | Border Gateway Protocol |
| biff | Biff mail notification |
| bootpc | Bootstrap Protocol Client |
| bootps | Bootstrap Protocol Server |
| **bridge** * | bridging |
| **cddbp** | CD Database Protocol |
| **cdp** * | Cisco Discovery Protocol |
| cifs | CIFS |
| **cisco-fna** | Cisco FNATIVE |
| cisco-net-mgmt | cisco-net-mgmt |
| cisco-svcs | Cisco license/perf/GDP/X.25/ident svcs |

| Protocol Name | Description |
|---|---|
| cisco-sys | Cisco SYSMAINT |
| cisco-tdp | cisco-tdp |
| cisco-tna | Cisco TNATIVE |
| **citrix** | Citrix Systems Metaframe |
| citriximaclient | Citrix IMA Client |
| **clns** * | ISO Connectionless Network Service |
| **clns_es** * | ISO CLNS End System |
| **clns_is** * | ISO CLNS Intermediate System |
| clp | Cisco Line Protocol |
| **cmns** * | ISO Connection-Mode Network Service |
| **cmp** | Cluster Membership Protocol |
| **compressedtcp** * | Compressed TCP |
| creativepartnr | Creative Partner |
| creativeserver | Creative Server |
| **cuseeme** | CU-SeeMe desktop video conference |
| daytime | Daytime (RFC 867) |
| dbase | dBASE Unix |
| dbcontrol_agent | Oracle Database Control Agent |
| ddns-v3 | Dynamic DNS Version 3 |
| **dhcp** | Dynamic Host Configuration |
| dhcp-failover | DHCP Failover |
| **directconnect** | Direct Connect |
| discard | Discard port |
| **dns** | Domain Name Server lookup |

| Protocol Name | Description |
|---|---|
| dnsix | DNSIX Security Attribute Token Map |
| echo | Echo port |
| **edonkey** | eDonkey |
| **egp** | Exterior Gateway Protocol |
| **eigrp** | Enhanced Interior Gateway Routing Protocol |
| entrust-svc-handler | Entrust KM/Admin Service Handler |
| entrust-svcs | Entrust sps/aaas/aams |
| exec | Remote Process Execution |
| **exchange** | Microsoft RPC for Exchange |
| **fasttrack** | FastTrack Traffic (KaZaA, Morpheus, Grokster, and so on) |
| fcip-port | FCIP |
| **finger** | Finger |
| **ftp** | File Transfer Protocol |
| ftps | FTP over TLS/SSL |
| gdoi | Group Domain of Interpretation |
| giop | Oracle GIOP/SSL |
| **gnutella** | Gnutella Version 2 Traffic (BearShare, Shareeza, Morpheus, and so on) |
| **gopher** | Gopher |
| **gre** | Generic Routing Encapsulation |
| gtpv0 | GPRS Tunneling Protocol Version 0 |
| gtpv1 | GPRS Tunneling Protocol Version 1 |
| h225ras | H225 RAS over Unicast |
| **h323** | H323 Protocol |

| Protocol Name | Description |
|---|---|
| h323callsigalt | H323 Call Signal Alternate |
| hp-alarm-mgr | HP Performance data alarm manager |
| hp-collector | HP Performance data collector |
| hp-managed-node | HP Performance data managed node |
| hsrp | Hot Standby Router Protocol |
| **http** | Hypertext Transfer Protocol |
| https | Secure Hypertext Transfer Protocol |
| ica | ica (Citrix) |
| icabrowser | icabrowser (Citrix) |
| icmp | Internet Control Message Protocol |
| ident | Authentication Service |
| igmpv3lite | IGMP over UDP for SSM |
| **imap** | Internet Message Access Protocol |
| imap3 | Interactive Mail Access Protocol 3 |
| imaps | IMAP over TLS/SSL |
| **ip** * | IP (version 4) |
| ipass | IPASS |
| **ipinip** | IP in IP (encapsulation) |
| **ipsec** | IP Security Protocol (ESP/AH) |
| ipsec-msft | Microsoft IPsec NAT-T |
| **ipv6** * | IP (version 6) |
| ipx | IPX |
| **irc** | Internet Relay Chat |
| irc-serv | IRC-SERV |

| Protocol Name | Description |
|---|---|
| ircs | IRC over TLS/SSL |
| ircu | IRCU |
| isakmp | ISAKMP |
| iscsi | iSCSI |
| iscsi-target | iSCSI port |
| **kazaa2** | Kazaa Version 2 |
| **kerberos** | Kerberos |
| **l2tp** | Layer 2 Tunnel Protocol |
| **ldap** | Lightweight Directory Access Protocol |
| ldap-admin | LDAP admin server port |
| ldaps | LDAP over TLS/SSL |
| **llc2 *** | llc2 |
| login | Remote login |
| lotusmtap | Lotus Mail Tracking Agent Protocol |
| lotusnote | Lotus Notes |
| **mgcp** | Media Gateway Control Protocol |
| microsoft-ds | Microsoft-DS |
| **msexch-routing** | Microsoft Exchange Routing |
| **msnmsgr** | MSN Instant Messenger |
| **msrpc** | Microsoft Remote Procedure Call |
| **msrpc-smb-netbios** | MSRPC over TCP port 445 |
| **ms-cluster-net** | MS Cluster Net |
| **ms-dotnetster** | Microsoft .NETster Port |
| **ms-sna** | Microsoft SNA Server/Base |

| Protocol Name | Description |
|---|---|
| **ms-sql** | Microsoft SQL |
| **ms-sql-m** | Microsoft SQL Monitor |
| **mysql** | MySQL |
| n2h2server | N2H2 Filter Service Port |
| ncp | NCP (Novell) |
| net8-cman | Oracle Net8 Cman/Admin |
| **netbios** | Network Basic Input/Output System |
| netbios-dgm | NETBIOS Datagram Service |
| netbios-ns | NETBIOS Name Service |
| netbios-ssn | NETBIOS Session Service |
| **netshow** | Microsoft Netshow |
| netstat | Variant of systat |
| **nfs** | Network File System |
| **nntp** | Network News Transfer Protocol |
| **novadigm** | Novadigm Enterprise Desktop Manager (EDM) |
| **ntp** | Network Time Protocol |
| oem-agent | OEM Agent (Oracle) |
| oracle | Oracle |
| oracle-em-vp | Oracle EM/VP |
| oraclenames | Oracle Names |
| orasrv | Oracle SQL*Net v1/v2 |
| **ospf** | Open Shortest Path First |
| **pad** * | Packet assembler/disassembler (PAD) links |
| **pcanywhere** | Symantec pcANYWHERE |

| Protocol Name | Description |
|---|---|
| pcanywheredata | pcANYWHEREdata |
| pcanywherestat | pcANYWHEREstat |
| **pop3** | Post Office Protocol |
| pop3s | POP3 over TLS/SSL |
| pppoe | Point-to-Point Protocol over Ethernet |
| pptp | Point-to-Point Tunneling Protocol |
| **printer** | Print spooler/ldp |
| pwdgen | Password Generator Protocol |
| qmtp | Quick Mail Transfer Protocol |
| radius | RADIUS & Accounting |
| **rcmd** | Berkeley Software Distribution (BSD) r-commands (rsh, rlogin, rexec) |
| rdb-dbs-disp | Oracle RDB |
| realmedia | RealNetwork's Realmedia Protocol |
| realsecure | ISS Real Secure Console Service Port |
| **rip** | Routing Information Protocol |
| router | Local Routing Process |
| **rsrb** * | Remote Source-Route Bridging |
| rsvd | RSVD |
| **rsvp** | Resource Reservation Protocol |
| rsvp-encap | RSVP ENCAPSULATION-1/2 |
| rsvp_tunnel | RSVP Tunnel |
| rtc-pm-port | Oracle RTC-PM port |
| rtelnet | Remote Telnet Service |
| **rtp** | Real-Time Protocol |

| Protocol Name | Description |
|---|---|
| **rtsp** | Real-Time Streaming Protocol |
| r-winsock | remote-winsock |
| **secure-ftp** | FTP over Transport Layer Security/Secure Sockets Layer (TLS/SSL) |
| **secure-http** | Secured HTTP |
| **secure-imap** | Internet Message Access Protocol over TLS/SSL |
| **secure-irc** | Internet Relay Chat over TLS/SSL |
| **secure-ldap** | Lightweight Directory Access Protocol over TLS/SSL |
| **secure-nntp** | Network News Transfer Protocol over TLS/SSL |
| **secure-pop3** | Post Office Protocol over TLS/SSL |
| **secure-telnet** | Telnet over TLS/SSL |
| send | SEND |
| shell | Remote command |
| **sip** | Session Initiation Protocol |
| sip-tls | Session Initiation Protocol-Transport Layer Security |
| **skinny** | Skinny Client Control Protocol |
| sms | SMS RCINFO/XFER/CHAT |
| **smtp** | Simple Mail Transfer Protocol |
| **snapshot** | Snapshot routing support |
| **snmp** | Simple Network Protocol |
| snmptrap | SNMP Trap |
| **socks** | Sockets network proxy protocol (SOCKS) |
| **sqlnet** | Structured Query Language (SQL)*NET for Oracle |
| sqlserv | SQL Services |
| sqlsrv | SQL Service |

| Protocol Name | Description |
|---|---|
| **sqlserver** | Microsoft SQL Server |
| **ssh** | Secure shell |
| sshell | SSLshell |
| ssp | State Sync Protocol |
| **streamwork** | Xing Technology StreamWorks player |
| stun | cisco Serial Tunnel |
| **sunrpc** | Sun remote-procedure call (RPC) |
| **syslog** | System Logging Utility |
| syslog-conn | Reliable Syslog Service |
| tacacs | Login Host Protocol (TACACS) |
| tacacs-ds | TACACS-Database Service |
| tarantella | Tarantella |
| tcp | Transport Control Protocol |
| **telnet** | Telnet |
| telnets | Telnet over TLS/SSL |
| **tftp** | Trivial File Transfer Protocol |
| time | Time |
| timed | Time server |
| tr-rsrb | cisco RSRB |
| tto | Oracle TTC/SSL |
| udp | User Datagram Protocol |
| uucp | UUCPD/UUCP-RLOGIN |
| **vdolive** | VDOLive streaming video |
| **vofr** * | Voice over Frame Relay |

| Protocol Name | Description |
|---|---|
| vqp | VLAN Query Protocol |
| webster | Network Dictionary |
| who | Who's service |
| wins | Microsoft WINS |
| x11 | X Window System |
| xdmcp | XDM Control Protocol |
| **xwindows *** | X-Windows remote access |
| ymsgr | Yahoo! Instant Messenger |

* This protocol is not supported on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine.

## Examples

The following example specifies a class map named ftp and configures the FTP protocol as a match criterion:

```
Router(config)# class-map ftp
Router(config-cmap)
#
 match protocol ftp
```

**Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE**

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 for the IP protocol will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match protocol ip
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **service-policy type performance-monitor** | Associates a Performance Monitor policy with an interface. |
| **match access-group** | Configures the match criteria for a class map based on the specified ACL. |

| Command | Description |
|---|---|
| **match input-interface** | Configures a class map to use the specified input interface as a match criterion. |
| **match mpls experimental** | Configures a class map to use the specified value of the experimental field as a match criterion. |
| **match precedence** | Identifies IP precedence values as match criteria. |
| **match protocol (NBAR)** | Configures NBAR to match traffic by a protocol type known to NBAR. |
| **match qos-group** | Configures a class map to use the specified EXP field value as a match criterion. |

# match protocol attribute application-group

To configure the match criterion for a class map based on the specified application group, use the **match protocol attribute application-group** command in class-map configuration mode. To remove the application-group match criterion from the class map, use the **no** form of this command.

**match protocol attribute application-group** *application-group* [*application-name*]

**no match protocol attribute application-group** *application-group*

## Syntax Description

| | |
|---|---|
| *application-group* | Name of the application group as a matching criterion. See the "Usage Guidelines" section for a list of application groups supported by most routers. |
| *application-name* | (Optional) Name of the application. When the application name is specified, the application is configured as the match criterion instead of the application group. |

## Command Default

No match criterion is configured.

## Command Modes

Class-map configuration (config-cmap)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.4S | This command was introduced. |

## Usage Guidelines

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) based on an application group. Multiple traffic classes can be created. The following table lists the supported application groups.

***Table 11: Supported Application Groups***

| Application Group | Description |
|---|---|
| **apple-talk-group** | AppleTalk-related applications. |
| **banyan-group** | Banyan-related applications. |
| **bittorrent-group** | Bittorrent-related applications. |

| Application Group | Description |
|---|---|
| **corba-group** | Corba-related applications. |
| **edonkey-emule-group** | edonkey-emule-related applications. |
| **fasttrack-group** | Fasttrack-related applications. |
| **flash-group** | Flash-related applications. |
| **fring-group** | Fring-related applications. |
| **ftp-group** | FTP-related applications. |
| **gnutella-group** | Gnutella-related applications. |
| **icq-group** | I Seek You (ICQ)-related applications. |
| **imap-group** | Internet Message Access Protocol (IMAP)-related applications. |
| **irc-group** | Internet Relay Chap (IRC)-related applications. |
| **kerberos-group** | Kerberos-related applications. |
| **ldap-group** | Lightweight Directory Access Protocol (LDAP)-related applications. |
| **my-jabber-group** | My-jabber-related applications. |
| **netbios-group** | NetBIOS-related applications. |
| **nntp-group** | Network News Transfer Protocol (NNTP)-related applications. |
| **npmp-group** | Network Peripheral Management Protocol (NPMP)-group related objectives. |
| **other** | Other applications. |
| **pop3-group** | Post Office Protocol 3 (pop3)-related applications. |
| **prm-group** | Performance Report Message (PRM)-related applications. |
| **skinny-group** | Skinny-related applications. |
| **skype-group** | Skype-related applications. |

| Application Group | Description |
|---|---|
| **smtp-group** | Simple Mail Transfer Protocol (SMTP)-related applications. |
| **snmp-group** | Simple Network Management Protocol (SNMP)-related applications. |
| **sqlsvr-group** | Structured Query Language (SQL)-server-related applications. |
| **telepresence-group** | Telepresence-related applications. |
| **tftp-group** | TFTP-related applications. |
| **wap-group** | Wireless Application Protocol (WAP)-related applications. |
| **webex-group** | Webex-related applications. |
| **windows-live-messenger-group** | Windows-live-messenger-related applications. |
| **xns-xerox-group** | Xerox Network Services (XNS)-xerox related applications. |
| **yahoo-messenger-group** | Yahoo Messenger-related applications. |

## Examples

The following example shows how to configure an application group as a match criterion:

```
Router(config)# class-map apps
Router(config-cmap)# match protocol attribute application-group skype-group
```

## Related Commands

| Command | Description |
|---|---|
| **match protocol (NBAR)** | Configures NBAR to match traffic by a protocol type known to NBAR. |

# match protocol attribute category

To configure the match criterion for a class map based on the specified application category, use the **match protocol attribute category** command in class-map configuration mode. To remove the application category match criterion from the class map, use the **no** form of this command.

**match protocol attribute category** *application-category* [*application-name*]

**no match protocol attribute category** *application-category*

## Syntax Description

| | |
|---|---|
| *application-category* | Name of the application category used as a matching criterion. See the "Usage Guidelines" section for a list of application categories supported by most routers. |
| *application-name* | (Optional) Name of the application. When the application name is specified, the application is configured as the match criterion instead of the application category. |

## Command Default

No match criterion is configured.

## Command Modes

Class-map configuration (config-cmap)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.4S | This command was introduced. |

## Usage Guidelines

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) based on an application category. You can create as many traffic classes as needed.

The following table lists the supported application categories.

***Table 12: Supported Application Categories***

| Category Name | Description |
|---|---|
| **browsing** | Browsing-related applications. |
| **business-and-productivity-tools** | Business and productivity tools-related applications. |

| Category Name | Description |
|---|---|
| **email** | Email-related applications. |
| **file-sharing** | File-sharing related applications. |
| **gaming** | Gaming-related applications. |
| **industrial-protocols** | Industrial protocols-related applications. |
| **instant-messaging** | Instant messaging-related applications. |
| **internet-privacy** | Internet privacy-related applications. |
| **layer2-non-ip** | Layer2 non-ip-related applications. |
| **layer3-over-ip** | Layer3-over-IP-related applications. |
| **location-based-services** | Location-based services-related applications. |
| **net-admin** | Net-admin-related applications. |
| **newsgroup** | Newsgroup-related applications. |
| **obsolete** | Obsolete applications. |
| **other** | Other applications. |
| **trojan** | Trojan-related applications. |
| **voice-and-video** | Voice and video-related applications. |

## Examples

The following example shows how to configure email-related applications as a match criterion:

```
Router(config)# class-map mygroup
Router(config-cmap)# match protocol attribute category email
```

## Related Commands

| Command | Description |
|---|---|
| **match protocol attribute sub-category** | Configures the match criterion for a specified application subcategory. |

# match protocol attribute encrypted

To configure the match criterion for a class map based on encryption, use the **match protocol attribute encrypted** command in class-map configuration mode. To remove the encryption match criterion from the class map, use the **no** form of this command.

**match protocol attribute encrypted** {**encrypted-no| encrypted-unassigned| encrypted-yes**} [*application-name*]

**no match protocol attribute encrypted** {**encrypted-no| encrypted-unassigned| encrypted-yes**}

## Syntax Description

| | |
|---|---|
| **encrypted-no** | Specifies applications without encryption. |
| **encrypted-unassigned** | Specifies applications without an encrypted networking protocol application tag. |
| **encrypted-yes** | Specifies encrypted applications. |
| *application-name* | (Optional) Name of the application. When the application name is specified, the application within the specified encrypted status is configured as the match criterion instead of all the applications within the group. |

## Command Default

No match criterion is configured.

## Command Modes

Class-map configuration (config-cmap)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.4S | This command was introduced. |

## Usage Guidelines

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) based on encryption. Multiple traffic classes can be created.

## Examples

The following examples show how to specify a class map with encryption as a match criterion:

```
Router(config)# class-map my-class
Router(config-cmap)# match protocol attribute encrypted encrypted-no ayiya-ipv6-tunneled

Router(config)# class-map my-class
Router(config-cmap)# match protocol attribute encrypted encrypted-unassigned aurora-cmgr
```

```
Router(config)# class-map my-class
Router(config-cmap)# match protocol attribute encrypted encrypted-yes citrix
```

## Related Commands

| Command | Description |
|---|---|
| **match protocol (NBAR)** | Configures NBAR to match traffic by a protocol type known to NBAR. |

# match protocol attribute sub-category

To configure the match criterion for a class map based on the specified application subcategory, use the **match protocol attribute sub-category** command in class-map configuration mode. To remove the application subcategory match criterion from the class map, use the **no** form of this command.

**match protocol attribute sub-category** *sub-category-name* [*aplication-name*]

**no match protocol attribute sub-category** *sub-category-name*

## Syntax Description

| | |
|---|---|
| *sub-category-name* | Name of the application subcategory used as a matching criterion. See the "Usage Guidelines" section for a list of application subcategories supported by most routers. |
| *application-name* | (Optional) Name of the application. When the application name is specified, the application is configured as the match criterion instead of the subcategory. |

## Command Default

No match criterion is configured.

## Command Modes

Class-map configuration (config-cmap)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.4S | This command was introduced. |

## Usage Guidelines

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) based on an application subcategory. You can create as many traffic classes as needed.

#unique_250 lists the supported application subcategories.

***Table 13: Supported Application Subcategories***

| Sub-Category Name | Description |
|---|---|
| **authentication-services** | Authentication services-related applications. |
| **backup-systems** | Backup systems-related applications. |

| Sub-Category Name | Description |
|---|---|
| **client-server** | Client-server-related applications. |
| **commercial-media-distribution** | Commercial media distribution-related applications. |
| **control-and-signaling** | Control and signaling-related applications. |
| **database** | Database-related applications. |
| **epayement** | Epayement-related applications. |
| **inter-process-rpc** | Inter-process remote procedure call-related applications. |
| **license-manager** | License manager-related applications. |
| **naming-services** | Naming services-related applications. |
| **network-management** | Network management-related applications |
| **network-protocol** | Network protocol-related applications. |
| **other** | Other related applications. |
| **p2p-file-transfer** | Peer-to-peer file transfer-related applications. |
| **p2p-networking** | Peer-to-peer networking-related applications. |
| **remote-access-terminal** | Remote access terminal-related applications. |
| **rich-media-http-content** | Rich media HTTP content-related applications. |
| **routing-protocol** | Routing protocol-related applications. |
| **storage** | Storage-related applications. |
| **streaming** | Streaming-related applications. |
| **terminal** | Terminal-related applications. |
| **tunneling-protocols** | Tunneling protocols-related applications. |
| **voice-video-chat-collaboration** | Voice-video chat collaboration-related applications. |

## Examples

The following example shows how to configure client-server applications as a match criterion:

```
Router(config)# class-map newmap
Router(config-cmap)# match protocol attribute sub-category client-server
```

## Related Commands

| Command | Description |
|---|---|
| **match protocol attribute category** | Configures the match criterion for a specified application category. |

# match protocol attribute tunnel

To configure the match criterion for a class map based on tunneling, use the **match protocol attribute tunnel** command in class-map configuration mode. To remove the tunneling match criterion from the class map, use the **no** form of this command.

**match protocol attribute tunnel** {**tunnel-no| tunnel-unassigned| tunnel-yes**} [*application-name*]

**no match protocol attribute tunnel** {**tunnel-no| tunnel-unassigned| tunnel-yes**} [*application-name*]

## Syntax Description

| | |
|---|---|
| **tunnel-no** | Specifies the applications without tunneling. |
| **tunnel-unassigned** | Specifies the unassigned tunneled applications. |
| **tunnel-yes** | Specifies tunneled applications. |
| *application-name* | (Optional) Name of the application. When the application name is specified, the application within the specified tunneling status is configured as the match criterion instead of all the applications within the tunneling group. |

## Command Default

No match criterion is configured.

## Command Modes

Class-map configuration (config-cmap)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.4S | This command was introduced. |

## Usage Guidelines

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) based on tunneling. Multiple traffic classes can be created.

## Examples

The following examples show how to specify a class map with tunneling as a match criterion:

```
Router(config)# class-map mygroup
Router(config-cmap)# match protocol attribute tunnel tunnel-no agentx

Router(config)# class-map mygroup
Router(config-cmap)# match protocol attribute tunnel tunnel-unassigned aris

Router(config)# class-map mygroup
Router(config-cmap)# match protocol attribute tunnel tunnel-yes rsvp_tunnel
```

## Related Commands

| Command | Description |
|---|---|
| **match protocol (NBAR)** | Configures NBAR to match traffic by a protocol type known to NBAR. |

# match protocol (NBAR)

To configure Network-Based Application Recognition (NBAR) to match traffic by a protocol type that is known to NBAR, use the **matchprotocol**commandinclass map configuration mode. To disable NBAR from matching traffic by a known protocol type, use the **no** form of this command.

**match protocol** *protocol-name* [*variable-field-name value*]

**no match protocol** *protocol-name* [*variable-field-name value*]

## Syntax Description

| | |
|---|---|
| *protocol-name* | Particular protocol type that is known to NBAR. These known protocol types can be used to match traffic. For a list of protocol types that are known to NBAR, see the table below in "Usage Guidelines." |
| *variable-field-name* | (Optional and usable only with custom protocols) Predefined variable that was created when you created a custom protocol. The value for the *variable-field-name*argument will match the *field-name* variable entered when you created the custom protocol using the**ip nbar custom**command. |
| *value* | (Optional and usable only with custom protocols) Specific value in the custom payload to match. A value can be entered along with a value for the *variable-field-name*argument only. The value can be expressed in decimal or hexadecimal format. |

## Command Default

Traffic is not matched by a protocol type that is known to NBAR.

## Command Modes

Class map configuration (config-cmap)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)XE2 | This command was introduced. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E, and the *variable-field-namevalue*argument was added. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.1(13)T | This command was implemented on Catalyst 6000 family switches without FlexWAN modules. |

| Release | Modification |
|---|---|
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(17a)SX1 | This command was integrated into Cisco IOS Release 12.2(17a)SX1. |
| 12.4(2)T | This command was modified to include support for additional protocols, such as the BitTorrent protocol. |
| 12.4(4)T | This command was modified to include support for additional protocols, such as the Skype and DirectConnect protocols. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(18)ZY | This command was integrated into Cisco IOS Release 12.2(18)ZY. This command was modified to enhance NBAR functionality on the Catalyst 6500 series switch that is equipped with the Supervisor 32/programmable intelligent services accelerator (PISA) engine. |
| 12.2(18)ZYA | This command was modified to integrate NBAR and Firewall Service Module (FWSM) functionality on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine and to recognize additional protocols as noted in the table below in “Usage Guidelines.” |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 Series Aggregation Services Routers. |
| 12.2(18)ZYA1 | This command was modified to recognize additional protocols as noted in the table below in “Usage Guidelines.” |
| Cisco IOS XE Release 2.3 | This command was modified to recognize additional protocols as noted in the table below in “Usage Guidelines.” |
| 12.2(18)ZYA2 | This command was modified to recognize additional protocols, such as the TelePresence protocol. |
| Cisco IOS XE Release 2.5 | This command was modified to recognize additional protocols as noted in the table below in “Usage Guidelines.” |
| 12.2XN | This command was modified to recognize additional protocols as noted in the table below in “Usage Guidelines.” |
| 12.4(24)T | This command was modified to recognize additional protocols as noted in the table below in “Usage Guidelines.” |
| 12.4(24)MDA | This command was modified to recognize additional protocols as noted in the table below in “Usage Guidelines.” |
| Cisco IOS XE Release 3.4S | This command was modified to recognize additional protocols as noted in the table below in “Usage Guidelines.” |

| Release | Modification |
|---|---|
| 15.1(3)S | This command was modified. Support was removed from Cisco 7200 series routers. |

## Usage Guidelines

Use the **matchprotocol**(NBAR) command to match protocol types that are known to NBAR. NBAR is capable of classifying the following types of protocols:

- Non-UDP and non-TCP IP protocols
- TCP and UDP protocols that use statically assigned port numbers
- TCP and UDP protocols that use statically assigned port numbers but still require stateful inspection
- TCP and UDP protocols that dynamically assign port numbers and therefore require stateful inspection

The table below lists the NBAR-supported protocols available in Cisco IOS software, sorted by category. The table also provides information about the protocol type, the well-known port numbers (if applicable), and the syntax for entering the protocol in NBAR. The table is modified as new protocols are added or supported by different releases.

**Note** The table below includes the NBAR-supported protocols available with the 12.2(18)ZY and 12.2(18)ZYA releases. Protocols included in the 12.2(18)ZY and 12.2(18)ZYA releases are supported on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine.

*Table 14: NBAR-Supported Protocols*

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Enterprise Applications | Novadigm | TCP/ UDP | 3460-3465 | Novadigm Enterprise Desktop Manager (EDM) | novadigm | Cisco IOS XE Release 2.3 |
| | Citrix (ICA, CGP, IMA, SB) | TCP/ UDP | TCP: 1494, 2512, 2513, 2598 UDP: 1604 | Citrix ICA traffic | citrix citrix app citrix ica-tag | 12.1(2)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.5 |
| | Oracle | TCP | 1525 | Oracle | ora-srv | Cisco IOS XE Release 2.3 |
| | PCAnywhere | TCP/UDP | TCP: 5631, 65301 UDP: 22, 5632 | Symantic PCAnywhere | pcanywhere | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 |
| | SAP | TCP | 3300-3315 3200-3215 3600-3615 | Application server to application server traffic (sap-pgm.pdlm)<br>Client to application server traffic (sap-app.pdlm)<br>Client to message server traffic (sap-msg.pdlm) | sap | 12.1E 12.2T 12.3 12.3T 12.2(18)ZYA1 Cisco IOS XE Release 2.5 |
| | Exchange [1] | TCP | 135 | MS-RPC for Exchange | exchange | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| | | | | | | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZY<br>12.2(18)ZYA<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.5 |
| Routing Protocols | BGP | TCP/ UDP | 179 | Border Gateway Protocol | bgp | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |
| | EGP | IP | 8 | Exterior Gateway Protocol | egp | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |
| | EIGRP | IP | 88 | Enhanced Interior Gateway Routing Protocol | eigrp | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |
| | OSPF | IP | 89 | Open Shortest Path First | ospf | 12.3(8)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |
| | RIP | UDP | 520 | Routing Information Protocol | rip | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Database | CIFS | TCP | 139, 445 | Common Internet File System | cifs | 12.2(18)ZYA<br>12.2(18)ZYA1 |
| | MS-SQLServer | TCP | 1433 | Microsoft SQL Server Desktop Videoconferencing | sqlserver | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1 |
| | SQL-exec | TCP/UDP | 9088 | SQL Exec | sqlexec | Cisco IOS XE Release 2.3 |
| | SQL*NET | TCP/ UDP | 1521 | SQL*NET for Oracle | sqlnet | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.5 |
| Financial | FIX | TCP | Heuristic | Financial Information Exchange | fix | 12.2(18)ZYA<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.5 |
| Security and Tunneling | GRE | IP | 47 | Generic Routing Encapsulation | gre | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |
| IPINIP | IP | 4 | IP in IP | ipinip | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| IPsec | IP/TCP | 50, 51 TCP-Heuristic | IP Encapsulating Security Payload/ Authentication-Header | ipsec | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 | |
| L2TP | UDP | 1701 | L2F/L2TP Tunnel | l2tp | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 | |
| PPTP | TCP | 1723 | Point-to-Point Tunneling Protocol for VPN | pptp | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 | |
| SFTP | TCP | 990 | Secure FTP | secure-ftp | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 | |
| SHTTP | TCP | 443 | Secure HTTP | secure-http | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.3 | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| STELNET | TCP | 992 | Secure Telnet | secure-telnet | Cisco IOS XE Release 2.3 | |
| | SIMAP | TCP/ UDP | 585, 993 | Secure Internet Message Access Protocol | secure-imap | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |
| | SIRC | TCP/ UDP | 994 | Secure Internet Relay Chat | secure-irc | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |
| | SLDAP | TCP/ UDP | 636 | Secure Lightweight Directory Access Protocol | secure-ldap | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |
| | SNNTP | TCP/ UDP | 563 | Secure Network News Transfer Protocol | secure-nntp | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |
| | SOCKS | TCP | 1080 | Firewall Security Protocol | socks | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| | SPOP3 | TCP/ UDP | 995 | Secure POP3 | secure-pop3 | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |
| | SSH | TCP | 22 | Secured Shell | ssh | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |
| | STELNET | TCP | 992 | Secure Telnet | secure-telnet | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |
| Network Management | ICMP | IP | 1 | Internet Control Message Protocol | icmp | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |
| | SNMP | TCP/ UDP | 161, 162 | Simple Network Management Protocol | snmp | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |
| | Syslog | UDP | 514 | System Logging Utility | syslog | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Network Mail Services | IMAP | TCP/ UDP | 143, 220 | Internet Message Access Protocol | imap | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 |
| | Notes | TCP/ UDP | 1352 | Lotus Notes | notes | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 |
| | POP3 | TCP/ UDP | 110, Heuristic | Post Office Protocol | pop3 | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.3 |
| | SMTP | TCP | 25, Heuristic | Simple Mail Transfer Protocol | smtp | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Directory | DHCP/ BOOTP | UDP | 67, 68 | Dynamic Host Configuration Protocol/Bootstrap Protocol | dhcp | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.1 |
| | DNS | TCP/ UDP | 53 | Domain Name System | dns | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.1 |
| | Finger | TCP | 79 | Finger User Information Protocol | finger | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |
| | Kerberos | TCP/ UDP | 88, 749 | Kerberos Network Authentication Service | kerberos | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |
| | LDAP | TCP/ UDP | 389 | Lightweight Directory Access Protocol | ldap | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Internet | FTP | TCP | 21, 21000, Heuristic | File Transfer Protocol | ftp | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1 |
| | Gopher | TCP/ UDP | 70 | Internet Gopher Protocol | gopher | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 |
| | HTTP | TCP | 80[2], Heuristic | Hypertext Transfer Protocol | http | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.5 |
| | IRC | TCP/ UDP | 194 | Internet Relay Chat | irc | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 |
| | NNTP | TCP/ UDP | 119, Heuristic | Network News Transfer Protocol | nntp | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 |
| | Telnet | TCP | 23 | Telnet Protocol | telnet | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| | | | | | | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.1 |
| | TFTP | UDP | 69 | Trivial File Transfer Protocol | tftp | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.5 |
| Signaling | AppleQTC | TCP/UDP | 458 | Apple Quick Time | appleqtc | 12.2(18)ZYA<br>12.2(18)ZYA1 Cisco IOS XE Release 2.3 |
| Chargen | TCP/UDP | 19 | Character Generator | chargen | 12.2(18)ZYA<br>12.2(18)ZYA1 Cisco IOS XE Release 2.3 | |
| ClearCase | TCP/UDP | 371 | Clear Case Protocol Software Informer | clearcase | 12.2(18)ZYA<br>12.2(18)ZYA1 Cisco IOS XE Release 2.3 | |
| Corba | TCP/UDP | 683, 684 | Corba Internet Inter-Orb Protocol (IIOP) | corba-iiop | 12.2(18)ZYA<br>12.2(18)ZYA1 Cisco IOS XE Release 2.3 | |
| Daytime | TCP/UDP | 13 | Daytime Protocol | daytime | 12.2(18)ZYA<br>12.2(18)ZYA1 Cisco IOS XE Release 2.3 | |
| Doom | TCP/UDP | 666 | Doom | doom | 12.2(18)ZYA<br>12.2(18)ZYA1 Cisco IOS XE Release 2.3 | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Echo | TCP/UDP | 7 | Echo Protocol | echo | 12.2(18)ZYA 12.2(18)ZYA1Cisco IOS XE Release 2.3 | |
| IBM DB2 | TCP/UDP | 523 | IBM Information Management | ibm-db2 | 12.2(18)ZYA 12.2(18)ZYA1Cisco IOS XE Release 2.3 | |
| IPX | TCP/UDP | 213 | Internet Packet Exchange | server-ipx | 12.2(18)ZYA 12.2(18)ZYA1Cisco IOS XE Release 2.3 | |
| ISAKMP | TCP/UDP | 500 | Internet Security Association and Key Management Protocol | isakmp | 12.2(18)ZYA 12.2(18)ZYA1Cisco IOS XE Release 2.3 | |
| ISI-GL | TCP/UDP | 55 | Interoperable Self Installation Graphics Language | isi-gl | 12.2(18)ZYA 12.2(18)ZYA1Cisco IOS XE Release 2.3 | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release | | |
|---|---|---|---|---|---|---|---|---|
| | | | KLogin | TCP | 543 | KLogin | klogin | 12.2(18)ZYA 122(18)ZYA1Cisco IOS XE Release 2.3 |
| KShell | TCP | | 544 | KShell | kshell | 12.2(18)ZYA 122(18)ZYA1Cisco IOS XE Release 2.3 | | |
| LockD | TCP/UDP | | 4045 | LockD | lockd | 12.2(18)ZYA Cisco IOS XE Release 2.3 | | |
| MSSQL | TCP | | 1433 | Microsoft Structured Query Language (SQL) Server | mssql | Cisco IOS XE Release 2.3 | | |
| RSVP | IP/ UDP | | IP: 46 UDP: 1698, 1699 | Resource Reservation Protocol | rsvp | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 | | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| RPC | AOL-messenger | TCP | 5190, 443 | AOL Instant Messenger Chat Messages | aol-messenger | 12.2(18)ZYA<br>12.2(18)ZYA1 |
| | NFS | TCP/UDP | 2049 | Network File System | nfs | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |
| | Sunrpc | TCP/ UDP | 111, Heuristic | Sun Remote Procedure Call | sunrpc | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.5 |
| Non-IP and LAN/ Legacy | NetBIOS | TCP/ UDP | TCP-137, 138<br>UDP-137,139 | NetBIOS over IP (MS Windows) | netbios | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |
| | Nickname | TCP/UDP | 43 | Nickname | nicname | 12.2(18)ZYA<br>12.2(18)ZYA1Cisco IOS XE Release 2.3 |
| | NPP | TCP/UDP | 92 | Network Payment Protocol | npp | 12.2(18)ZY<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.3 |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Voice | Google Talk VoIP | TCP/UDP | Dynamically assigned | Google Talk VoIP Protocol | gtalk-voip | 12.2XN 12.4(24)MDA |
| | H.323 | TCP | Heuristic | H.323 Teleconferencing Protocol | h323 | Cisco IOS XE Release 2.1 |
| | MSN VoIP | UDP | Dynamically assigned | MSN Messenger Protocol | msn-voip | 12.4(24)MDA 12.4(24)T |
| | RTCP | TCP/ UDP | Dynamically assigned | Real-Time Control Protocol | rtcp | 12.1E 12.2T 12.2(18)ZYA1 12.3 12.3T |
| | RTP | TCP/ UDP | Dynamically assigned | Real-Time Transport Protocol Payload Classification | rtp | 12.2(8)T 12.2(18)ZYA1 Cisco IOS XE Release 2.5 |
| | | | | | | |
| | SIP | TCP/UPD | 5060 | Session Initiation Protocol | sip | 12.3(7)T Cisco IOS XE Release 2.1 12.2(18)ZYA1 Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.3 |
| | STUN | UDP | Dynamically assigned | Simple Traversal of UDP through NAT (STUN) | stun-nat | 12.4(24)MDA 12.4(24)T |
| | Skype[3] | TCP/UDP | TCP-80, Heuristic | VoIP Client Software | skype | Cisco IOS XE Release 2.1 Cisco IOS XE Release 2.5 |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| | Yahoo VoIP | TCP/UDP | Dynamically assigned | Yahoo Messenger VoIP Protocol | yahoo-voip | 12.4(24)MDA<br>12.4(24)T |
| Desktop Media | CUSeeMe | TCP/UDP | TCP: 7648, 7649 UDP: 24032 | CU-SeeMe Desktop Video Conference | cuseeme | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.1 |
| Streaming Media | RealAudio | TCP/ UDP | Dynamically assigned | RealAudio Streaming Protocol | realaudio | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T |
| | RTSP | TCP | 554, 8554 | Real-Time Streaming Protocol | rtsp | 12.2(18)ZYA1<br>12.3(11)T<br>Cisco IOS XE Release 2.1 |
| | StreamWorks | UDP | Dynamically assigned | Xing Technology Stream Works Audio and Video | streamwork | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1 |
| | VDOLive | TCP/ UDP | Static (7000) with inspection | VDOLive Streaming Video | vdolive | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1 |
| | YouTube[4] | TCP | Both static (80) and dynamically assigned | Online Video-Sharing Website | youtube | 12.2(18)ZYA<br>12.2(18)ZYA1 |
| Peer-to-Peer File-Sharing Applications | BitTorrent[5] | TCP | Heuristic, or 6881-6889 | BitTorrent File Transfer Traffic | bittorrent | 12.2(18)ZYA1<br>12.4(2)T<br>Cisco IOS XE Release 2.5 |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| DirectConnect | TCP | 80, 411-413, Heuristic | Direct Connect File Transfer Traffic | directconnect | Cisco IOS XE Release 2.5 | |
| eDonkey/eMule[6] | TCP | 80, 4662, Heuristic | eDonkey File-Sharing Application<br>eMule traffic is also classified as eDonkey traffic in NBAR. | edonkey | 12.2(18)ZYA1<br>12.3(11)T<br>Cisco IOS XE Release 2.5 | |
| | | | | | | |
| Encrypted Emule | TCP | Heuristic | P2P file sharing encrypted protocol | encrypted-emule | Cisco IOS XE Release 3.4S | |
| FastTrack | — | Heuristic | FastTrack traffic | fasttrack | 12.1(12c)E<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.5 | |
| FastTrack Static | — | Heuristic | FastTrack Static | fasttrack-static | Cisco IOS XE Release 3.3S | |
| Gnutella | TCP/UDP | Heuristic, or TCP-80, 6346-6349, 6355,5634 | Gnutella traffic | gnutella | Cisco IOS XE Release 2.5 | |
| Gnutella Networking | TCP/UDP | Heuristic, or UDP-6346-6348 | Gnutella Networking traffic | networking-gnutella | Cisco IOS XE Release 3.4S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| KaZaA | TCP/ UPD | Heuristic | KaZaA<br>Note that earlier KaZaA version 1 traffic can be classified using FastTrack. | kazaa2 | 12.2(8)T<br>12.2(18)ZYA1<br>Cisco IOS XE Release 2.5 | |
| WinMX | TCP | 6699 | WinMX Peer-to-Peer File-Sharing | winmx | 12.2(18)ZYA1<br>12.3(7)T<br>Cisco IOS XE Release 2.5 | |
| Miscellaneous | 3Com AMP3 | TCP/UDP | 629 | 3Com AMP3 | 3com-amp3 | Cisco IOS XE Release 3.1S |
| | 3Com TSMUX | TCP/UDP | 106 | 3Com TSMUX | 3com-tsmux | Cisco IOS XE Release 3.1S |
| 3PC | TCP/UDP | 34 | Third Party Connect Protocol | 3pc | Cisco IOS XE Release 3.1S | |
| 914 C/G | TCP/UDP | 211 | Texas Instruments 914 Terminal | 914c/g | Cisco IOS XE Release 3.1S | |
| 9PFS | TCP/UDP | 564 | Plan 9 file service | 9pfs | Cisco IOS XE Release 3.1S | |
| ACAP | TCP/UDP | 674 | ACAP | acap | Cisco IOS XE Release 3.1S | |
| ACAS | TCP/UDP | 62 | ACA Services | acas | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| AccessBuilder | TCP/UDP | 888 | Access Builder | accessbuilder | Cisco IOS XE Release 3.1S | |
| AccessNetwork | TCP/UDP | 699 | Access Network | accessnetwork | Cisco IOS XE Release 3.1S | |
| ACP | TCP/UDP | 599 | Aeolon Core Protocol | acp | Cisco IOS XE Release 3.1S | |
| ACR-NEMA | TCP/UDP | 104 | ACR-NEMA Digital Img | acr-nema | Cisco IOS XE Release 3.1S | |
| AED-512 | TCP/UDP | 149 | AED 512 Emulation service | aed-512 | Cisco IOS XE Release 3.1S | |
| Agentx | TCP/UDP | 705 | AgentX | agentx | Cisco IOS XE Release 3.1S | |
| Alpes | TCP/UDP | 463 | Alpes | alpes | Cisco IOS XE Release 3.1S | |
| AMInet | TCP/UDP | 2639 | AMInet | aminet | Cisco IOS XE Release 3.1S | |
| AN | TCP/UDP | 107 | Active Networks | an | Cisco IOS XE Release 3.1S | |
| ANET | TCP/UDP | 212 | ATEXSSTR | anet | Cisco IOS XE Release 3.1S | |
| ANSANotify | TCP/UDP | 116 | ANSA REX Notify | ansanotify | Cisco IOS XE Release 3.1S | |
| ANSATrader | TCP/UDP | 124 | ansatrader | ansatrader | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| AODV | TCP/UDP | 654 | AODV | aodv | Cisco IOS XE Release 3.1S | |
| | Apertus-LDP | TCP/UDP | 539 | Apertus Tech Load Distribution | apertus-ldp | Cisco IOS XE Release 3.1S |
| | AppleQTC | TCP/UDP | 458 | apple quick time | appleqtc | Cisco IOS XE Release 3.1S |
| AppleQTSRVR | TCP/UDP | 545 | appleqtcsrvr | appleqtcsrvr | Cisco IOS XE Release 3.1S | |
| Applix | TCP/UDP | 999 | Applix ac | applix | Cisco IOS XE Release 3.1S | |
| ARCISDMS | TCP/UDP | 262 | arcisdms | arcisdms | Cisco IOS XE Release 3.1S | |
| ARGUS | TCP/UDP | 13 | ARGUS | argus | Cisco IOS XE Release 3.1S | |
| Ariel1 | TCP/UDP | 419 | Ariel1 | ariel1 | Cisco IOS XE Release 3.1S | |
| Ariel2 | TCP/UDP | 421 | Ariel2 | ariel2 | Cisco IOS XE Release 3.1S | |
| Ariel3 | TCP/UDP | 422 | Ariel3 | ariel3 | Cisco IOS XE Release 3.1S | |
| ARIS | TCP/UDP | 104 | ARIS | aris | Cisco IOS XE Release 3.1S | |
| ARNS | TCP/UDP | 384 | A remote network server system | arns | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| ASA | TCP/UDP | 386 | ASA Message router object def | asa | Cisco IOS XE Release 3.1S | |
| ASA-Appl-Proto | TCP/UDP | 502 | asa-appl-proto | asa-appl-proto | Cisco IOS XE Release 3.1S | |
| ASIPRegistry | TCP/UDP | 687 | asipregistry | asipregistry | Cisco IOS XE Release 3.1S | |
| ASIP-Webadmin | TCP/UDP | 311 | AppleShare IP WebAdmin | asip-webadmin | Cisco IOS XE Release 3.1S | |
| AS-Servermap | TCP/UDP | 449 | AS Server Mapper | as-servermap | Cisco IOS XE Release 3.1S | |
| AT-3 | TCP/UDP | 203 | AppleTalk Unused | at-3 | Cisco IOS XE Release 3.1S | |
| AT-5 | TCP/UDP | 205 | AppleTalk Unused | at-5 | Cisco IOS XE Release 3.1S | |
| AT-7 | TCP/UDP | 207 | AppleTalk Unused | at-7 | Cisco IOS XE Release 3.1S | |
| AT-8 | TCP/UDP | 208 | AppleTalk Unused | at-8 | Cisco IOS XE Release 3.1S | |
| | AT-Echo | TCP/UDP | 204 | AppleTalk Echo | at-echo | Cisco IOS XE Release 3.1S |
| AT-NBP | TCP/UDP | 202 | AppleTalk Name Binding | at-nbp | Cisco IOS XE Release 3.1S | |
| AT-RTMP | TCP/UDP | 201 | AppleTalk Routing Maintenance | at-rtmp | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| AT-ZIS | TCP/UDP | 206 | AppleTalk Zone Information | at-zis | Cisco IOS XE Release 3.1S | |
| Audit | TCP/UDP | 182 | Unisys Audit SITP | audit | Cisco IOS XE Release 3.1S | |
| Auditd | TCP/UDP | 48 | Digital Audit daemon | auditd | Cisco IOS XE Release 3.1S | |
| Aurora-CMGR | TCP/UDP | 364 | Aurora CMGR | aurora-cmgr | Cisco IOS XE Release 3.1S | |
| AURP | TCP/UDP | 387 | Appletalk Update-Based Routing Protocol | aurp | Cisco IOS XE Release 3.1S | |
| AUTH | TCP/UDP | 113 | Authentication Service | auth | Cisco IOS XE Release 3.1S | |
| Avian | TCP/UDP | 486 | avian | avian | Cisco IOS XE Release 3.1S | |
| AX25 | TCP/UDP | 93 | AX.25 Frames | ax25 | Cisco IOS XE Release 3.1S | |
| Banyan-RPC | TCP/UDP | 567 | Banyan-RPC | banyan-rpc | Cisco IOS XE Release 3.1S | |
| Banyan-VIP | TCP/UDP | 573 | Banyan-VIP | banyan-vip | Cisco IOS XE Release 3.1S | |
| BBNRCCMON | TCP/UDP | 10 | BBN RCC Monitoring | bbnrccmon | Cisco IOS XE Release 3.1S | |
| BDP | TCP/UDP | 581 | Bundle Discovery protocol | bdp | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| BFTP | TCP/UDP | 152 | Background File Transfer Program | bftp | Cisco IOS XE Release 3.1S | |
| BGMP | TCP/UDP | 264 | Border Gateway Multicast Protocol | bgmp | Cisco IOS XE Release 3.1S | |
| BGP | TCP/UDP | 179 | Border Gateway Protocol | bgp | Cisco IOS XE Release 3.1S | |
| BGS-NSI | TCP/UDP | 482 | BGS-NSI | bgs-nsi | Cisco IOS XE Release 3.1S | |
| | Bhevent | TCP/UDP | 357 | Bhevent | bhevent | Cisco IOS XE Release 3.1S |
| | BHFHS | TCP/UDP | 248 | BHFHS | bhfhs | Cisco IOS XE Release 3.1S |
| BHMDS | TCP/UDP | 310 | BHMDS | bhmds | Cisco IOS XE Release 3.1S | |
| BL-IDM | TCP/UDP | 142 | Britton Lee IDM | bl-idm | Cisco IOS XE Release 3.1S | |
| BMPP | TCP/UDP | 632 | BMPP | bmpp | Cisco IOS XE Release 3.1S | |
| BNA | TCP/UDP | 49 | BNA | bna | Cisco IOS XE Release 3.1S | |
| Bnet | TCP/UDP | 415 | BNET | bnet | Cisco IOS XE Release 3.1S | |
| Borland-DSJ | TCP/UDP | 707 | Borland-dsj | borland-dsj | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| BR-SAT-Mon | TCP/UDP | 76 | Backroom SATNET Monitoring | br-sat-mon | Cisco IOS XE Release 3.1S | |
| Cableport-AX | TCP/UDP | 282 | Cable Port A/X | cableport-ax | Cisco IOS XE Release 3.1S | |
| Cab-Protocol | TCP/UDP | 595 | CAB Protocol | cab-protocol | Cisco IOS XE Release 3.1S | |
| Cadlock | TCP/UDP | 770 | Cadlock | cadlock | Cisco IOS XE Release 3.1S | |
| CAIlic | TCP/UDP | 216 | Computer Associates Intl License Server | CAIlic | Cisco IOS XE Release 3.1S | |
| CBT | TCP/UDP | 7 | CBT | cbt | Cisco IOS XE Release 3.1S | |
| CDC | TCP/UDP | 223 | Certificate Distribution Center | cdc | Cisco IOS XE Release 3.1S | |
| CFDPTKT | TCP/UDP | 120 | cfdptkt | cfdptkt | Cisco IOS XE Release 3.1S | |
| CFTP | TCP/UDP | 62 | CFTP | cftp | Cisco IOS XE Release 3.1S | |
| CHAOS | TCP/UDP | 16 | Chaos | chaos | Cisco IOS XE Release 3.1S | |
| CharGen | TCP/UDP | 19 | Character Generator | chargen | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| | ChShell | TCP/UDP | 562 | chcmd | chshell | Cisco IOS XE Release 3.1S |
| | Cimplex | TCP/UDP | 673 | Cimplex | cimplex | Cisco IOS XE Release 3.1S |
| Cisco-FNA | TCP/UDP | 130 | Cisco FNATIVE | cisco-fna | Cisco IOS XE Release 3.1S | |
| Cisco-phone[7] | UDP | 5060 | Cisco IP Phones and PC-Based Unified Communicators | cisco-phone | 12.2(18)ZYA 12.2(18)ZYA1 | |
| Cisco-SYS | TCP/UDP | 132 | Cisco SYSMAINT | cisco-sys | Cisco IOS XE Release 3.1S | |
| Cisco-TDP | TCP/UDP | 711 | Cisco TDP | cisco-tdp | Cisco IOS XE Release 3.1S | |
| Cisco-TNA | TCP/UDP | 131 | Cisco TNATIVE | cisco-tna | Cisco IOS XE Release 3.1S | |
| Clearcase | TCP/UDP | 371 | Clearcase | clearcase | Cisco IOS XE Release 3.1S | |
| Cloanto-Net-1 | TCP/UDP | 356 | Cloanto-net-1 | cloanto-net-1 | Cisco IOS XE Release 3.1S | |
| CMIP-Agent | TCP/UDP | 164 | CMIP/TCP Agent | cmip-agent | Cisco IOS XE Release 3.1S | |
| CMIP-Man | TCP/UDP | 163 | CMIP/TCP Manager | cmip-man | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Coauthor | TCP/UDP | 1529 | Oracle | coauthor | Cisco IOS XE Release 3.1S | |
| Codaauth2 | TCP/UDP | 370 | Codaauth2 | codaauth2 | Cisco IOS XE Release 3.1S | |
| Collaborator | TCP/UDP | 622 | Collaborator | collaborator | Cisco IOS XE Release 3.1S | |
| Commerce | TCP/UDP | 542 | Commerce | commerce | Cisco IOS XE Release 3.1S | |
| Compaq-Peer | TCP/UDP | 110 | Compaq Peer Protocol | compaq-peer | Cisco IOS XE Release 3.1S | |
| Compressnet | TCP/UDP | 2 | Management Utility | compressnet | Cisco IOS XE Release 3.1S | |
| COMSCM | TCP/UDP | 437 | COMSCM | comscm | Cisco IOS XE Release 3.1S | |
| CON | TCP/UDP | 759 | Con | con | Cisco IOS XE Release 3.1S | |
| Conference | TCP/UDP | 531 | Chat | conference | Cisco IOS XE Release 3.1S | |
| | Connendp | TCP/UDP | 693 | Almanid Connection Endpoint | connendp | Cisco IOS XE Release 3.1S |
| | ContentServer | TCP/UDP | 3365 | Contentserver | contentserver | Cisco IOS XE Release 3.1S |
| CoreRJD | TCP/UDP | 284 | Corerjd | corerjd | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Courier | TCP/UDP | 530 | RPC | courier | Cisco IOS XE Release 3.1S | |
| Covia | TCP/UDP | 64 | Communications Integrator | covia | Cisco IOS XE Release 3.1S | |
| CPHB | TCP/UDP | 73 | Computer Protocol Heart Beat | cphb | Cisco IOS XE Release 3.1S | |
| CPNX | TCP/UDP | 72 | Computer Protocol Network Executive | cpnx | Cisco IOS XE Release 3.1S | |
| Creativepartnr | TCP/UDP | 455 | Creativepartnr | creativepartnr | Cisco IOS XE Release 3.1S | |
| Creativeserver | TCP/UDP | 453 | Creativeserver | creativeserver | Cisco IOS XE Release 3.1S | |
| CRS | TCP/UDP | 507 | CRS | crs | Cisco IOS XE Release 3.1S | |
| CRTP | TCP/UDP | 126 | Combat Radio Transport Protocol | crtp | Cisco IOS XE Release 3.1S | |
| CRUDP | TCP/UDP | 127 | Combat Radio User Datagram | crudp | Cisco IOS XE Release 3.1S | |
| CryptoAdmin | TCP/UDP | 624 | Crypto Admin | cryptoadmin | Cisco IOS XE Release 3.1S | |
| CSI-SGWP | TCP/UDP | 348 | Cabletron Management Protocol | csi-sgwp | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| CSNET-NS | TCP/UDP | 105 | Mailbox Name Nameserver | csnet-ns | Cisco IOS XE Release 3.1S | |
| CTF | TCP/UDP | 84 | Common Trace Facility | ctf | Cisco IOS XE Release 3.1S | |
| CUSTIX | TCP/UDP | 528 | Customer Ixchange | custix | Cisco IOS XE Release 3.1S | |
| CVC_Hostd | TCP/UDP | 442 | CVC_Hostd | cvc_hostd | Cisco IOS XE Release 3.1S | |
| Cybercash | TCP/UDP | 551 | Cybercash | cybercash | Cisco IOS XE Release 3.1S | |
| Cycleserv | TCP/UDP | 763 | Cycleserv | cycleserv | Cisco IOS XE Release 3.1S | |
| | Cycleserv2 | TCP/UDP | 772 | Cycleserv2 | cycleserv2 | Cisco IOS XE Release 3.1S |
| Dantz | TCP/UDP | 497 | Dantz | dantz | Cisco IOS XE Release 3.1S | |
| DASP | TCP/UDP | 439 | Dasp | dasp | Cisco IOS XE Release 3.1S | |
| DataSurfSRV | TCP/UDP | 461 | DataRamp Svr | datasurfsrv | Cisco IOS XE Release 3.1S | |
| DataSurfSRVSec | TCP/UDP | 462 | DataRamp Svr svs | datasurfsrvsec | Cisco IOS XE Release 3.1S | |
| Datex-ASN | TCP/UDP | 355 | datex-asn | datex-asn | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Daytime | TCP/UDP | 13 | Daytime (RFC 867) | daytime | Cisco IOS XE Release 3.1S | |
| Dbase | TCP/UDP | 217 | dBASE Unix | dbase | Cisco IOS XE Release 3.1S | |
| DCCP | TCP/UDP | 33 | Datagram Congestion Control Protocol | dccp | Cisco IOS XE Release 3.1S | |
| DCN-Meas | TCP/UDP | 19 | DCN Measurement Subsystems | dcn-meas | Cisco IOS XE Release 3.1S | |
| DCP | TCP/UDP | 93 | Device Control Protocol | dcp | Cisco IOS XE Release 3.1S | |
| DCTP | TCP/UDP | 675 | DCTP | dctp | Cisco IOS XE Release 3.1S | |
| DDM-DFM | TCP/UDP | 447 | DDM Distributed File management | ddm-dfm | Cisco IOS XE Release 3.1S | |
| DDM-RDB | TCP/UDP | 446 | DDM-Remote Relational Database Access | ddm-rdb | Cisco IOS XE Release 3.1S | |
| DDM-SSL | TCP/UDP | 448 | DDM-Remote DB Access Using Secure Sockets | ddm-ssl | Cisco IOS XE Release 3.1S | |
| DDP | TCP/UDP | 37 | Datagram Delivery Protocol | ddp | Cisco IOS XE Release 3.1S | |
| DDX | TCP/UDP | 116 | D-II Data Exchange | ddx | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| DEC_DLM | TCP/UDP | 625 | dec_dlm | dec_dlm | Cisco IOS XE Release 3.1S | |
| Decap | TCP/UDP | 403 | Decap | decap | Cisco IOS XE Release 3.1S | |
| | Decauth | TCP/UDP | 316 | Decauth | decauth | Cisco IOS XE Release 3.1S |
| Decbsrv | TCP/UDP | 579 | Decbsrv | decbsrv | Cisco IOS XE Release 3.1S | |
| Decladebug | TCP/UDP | 410 | DECLadebug Remote Debug Protocol | decladebug | Cisco IOS XE Release 3.1S | |
| Decvms-sysmgt | TCP/UDP | 441 | Decvms-sysmgt | decvms-sysmgt | Cisco IOS XE Release 3.1S | |
| DEI-ICDA | TCP/UDP | 618 | dei-icda | dei-icda | Cisco IOS XE Release 3.1S | |
| DEOS | TCP/UDP | 76 | Distributed External Object Store | deos | Cisco IOS XE Release 3.1S | |
| Device | TCP/UDP | 801 | Device | device | Cisco IOS XE Release 3.1S | |
| DGP | TCP/UDP | 86 | Dissimilar Gateway Protocol | dgp | Cisco IOS XE Release 3.1S | |
| DHCP-Failover | TCP/UDP | 647 | DHCP Failover | dhcp-failover | Cisco IOS XE Release 3.1S | |
| DHCP-Failover2 | TCP/UDP | 847 | dhcp-failover2 | dhcp-failover2 | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| DHCPv6-client | TCP/UDP | 546 | DHCPv6 Client | dhcpv6-client | Cisco IOS XE Release 3.1S | |
| DHCPv6-server | TCP/UDP | 547 | DHCPv6 Server | dhcpv6-server | Cisco IOS XE Release 3.1S | |
| Dicom | TCP/UDP | Heuristic | Digital Imaging and Communications in Medicine | dicom | 12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.3S | |
| Digital-VRC | TCP/UDP | 466 | digital-vrc | digital-vrc | Cisco IOS XE Release 3.1S | |
| Directplay | TCP/UDP | 2234 | DirectPlay | directplay | Cisco IOS XE Release 3.1S | |
| Directplay8 | TCP/UDP | 6073 | DirectPlay8 | directplay8 | Cisco IOS XE Release 3.1S | |
| Directv-Catlg | TCP/UDP | 3337 | Direct TV Data Catalog | directv-catlg | Cisco IOS XE Release 3.1S | |
| Directv-Soft | TCP/UDP | 3335 | Direct TV Software Updates | directv-soft | Cisco IOS XE Release 3.1S | |
| | Directv-Tick | TCP/UDP | 3336 | Direct TV Tickers | directv-tick | Cisco IOS XE Release 3.1S |
| | Directv-Web | TCP/UDP | 3334 | Direct TV Webcasting | directv-web | Cisco IOS XE Release 3.1S |
| Discard | TCP/UDP | 9 | Discard | discard | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Disclose | TCP/UDP | 667 | campaign contribution disclosures | disclose | Cisco IOS XE Release 3.1S | |
| Dixie | TCP/UDP | 96 | DIXIE Protocol Specification | dixie | Cisco IOS XE Release 3.1S | |
| DLS | TCP/UDP | 197 | Directory Location Service | dls | Cisco IOS XE Release 3.1S | |
| DLS-Mon | TCP/UDP | 198 | Directory Location Service Monitor | dls-mon | Cisco IOS XE Release 3.1S | |
| DN6-NLM-AUD | TCP/UDP | 195 | DNSIX Network Level Module Audit | dn6-nlm-aud | Cisco IOS XE Release 3.1S | |
| DNA-CML | TCP/UDP | 436 | DNA-CML | dna-cml | Cisco IOS XE Release 3.1S | |
| DNS | TCP/UDP | 53 | Domain Name Server lookup | dns | Cisco IOS XE Release 3.1S | |
| DNSIX | TCP/UDP | 90 | DNSIX Security Attribute Token Map | dnsix | Cisco IOS XE Release 3.1S | |
| DOOM | TCP/UDP | 666 | Doom Id Software | doom | Cisco IOS XE Release 3.1S | |
| DPSI | TCP/UDP | 315 | DPSI | dpsi | Cisco IOS XE Release 3.1S | |
| DSFGW | TCP/UDP | 438 | DSFGW | dsfgw | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| DSP | TCP/UDP | 33 | Display Support Protocol | dsp | Cisco IOS XE Release 3.1S | |
| DSP3270 | TCP/UDP | 246 | Display Systems Protocol | dsp3270 | Cisco IOS XE Release 3.1S | |
| DSR | TCP/UDP | 48 | Dynamic Source Routing Protocol | dsr | Cisco IOS XE Release 3.1S | |
| DTAG-DTE-SB | TCP/UDP | 352 | DTAG | dtag-ste-sb | Cisco IOS XE Release 3.1S | |
| DTK | TCP/UDP | 365 | DTK | dtk | Cisco IOS XE Release 3.1S | |
| | | | | | | |
| | DWR | TCP/UDP | 644 | DWR | dwr | Cisco IOS XE Release 3.1S |
| Echo | TCP/UDP | 7 | Echo | echo | Cisco IOS XE Release 3.1S | |
| EGP | TCP/UDP | 8 | Exterior Gateway Protocol | egp | Cisco IOS XE Release 3.1S | |
| EIGRP | TCP/UDP | 88 | Enhanced Interior Gateway Routing Protocol | eigrp | Cisco IOS XE Release 3.1S | |
| ELCSD | TCP/UDP | 704 | errlog copy/server daemon | elcsd | Cisco IOS XE Release 3.1S | |
| EMBL-NDT | TCP/UDP | 394 | EMBL Nucleic Data Transfer | embl-ndt | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| EMCON | TCP/UDP | 14 | EMCON | emcon | Cisco IOS XE Release 3.1S | |
| EMFIS-CNTL | TCP/UDP | 141 | EMFIS Control Service | emfis-cntl | Cisco IOS XE Release 3.1S | |
| EMFIS-Data | TCP/UDP | 140 | EMFIS Data Service | emfis-data | Cisco IOS XE Release 3.1S | |
| Encap | TCP/UDP | 98 | Encapsulation Header | encap | Cisco IOS XE Release 3.1S | |
| Encrypted Bittorrent | TCP | Heuristic | Encrypted Bittorrent | encrypted-bittorrent | Cisco IOS XE Release 3.4S | |
| Entomb | TCP/UDP | 775 | Entomb | entomb | Cisco IOS XE Release 3.1S | |
| Entrust-AAAS | TCP/UDP | 680 | Entrust-aaas | entrust-aaas | Cisco IOS XE Release 3.1S | |
| Entrust-AAMS | TCP/UDP | 681 | Entrust-aams | entrust-aams | Cisco IOS XE Release 3.1S | |
| Entrust-ASH | TCP/UDP | 710 | Entrust Administration Service Handler | entrust-ash | Cisco IOS XE Release 3.1S | |
| Entrust-KMSH | TCP/UDP | 709 | Entrust Key Management Service Handler | entrust-kmsh | Cisco IOS XE Release 3.1S | |
| Entrust-SPS | TCP/UDP | 640 | entrust-sps | entrust-sps | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| ERPC | TCP/UDP | 121 | Encore Expedited Remote Pro.Call | erpc | Cisco IOS XE Release 3.1S | |
| ESCP-IP | TCP/UDP | 621 | escp-ip | escp-ip | Cisco IOS XE Release 3.1S | |
| | ESRO-GEN | TCP/UDP | 259 | Efficient Short Remote Operations | esro-gen | Cisco IOS XE Release 3.1S |
| ESRP-EMSDP | TCP/UDP | 642 | ESRO-EMSDP V1.3 | esro-emsdp | Cisco IOS XE Release 3.1S | |
| EtherIP | TCP/UDP | 97 | Ethernet-within-IP Encapsulation | etherip | Cisco IOS XE Release 3.1S | |
| Eudora-Set | TCP/UDP | 592 | Eudora Set | eudora-set | Cisco IOS XE Release 3.1S | |
| EXEC | TCP/UDP | 512 | remote process execution; | exec | Cisco IOS XE Release 3.1S | |
| Fatserv | TCP/UDP | 347 | Fatmen Server | fatserv | Cisco IOS XE Release 3.1S | |
| FC | TCP/UDP | 133 | Fibre Channel | fc | Cisco IOS XE Release 3.1S | |
| FCP | TCP/UDP | 510 | FirstClass Protocol | fcp | Cisco IOS XE Release 3.1S | |
| Finger | TCP/UDP | 79 | Finger | finger | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| FIRE | TCP/UDP | 125 | FIRE | fire | Cisco IOS XE Release 3.1S | |
| FlexLM | TCP/UDP | 744 | Flexible License Manager | flexlm | Cisco IOS XE Release 3.1S | |
| FLN-SPX | TCP/UDP | 221 | Berkeley rlogind with SPX auth | fln-spx | Cisco IOS XE Release 3.1S | |
| FTP-Agent | TCP/UDP | 574 | FTP Software Agent System | ftp-agent | Cisco IOS XE Release 3.1S | |
| FTP-Data | TCP/UDP | 20 | File Transfer | ftp-data | Cisco IOS XE Release 3.1S | |
| FTPS-Data | TCP/UDP | 989 | ftp protocol, data, over TLS/SSL | ftps-data | Cisco IOS XE Release 3.1S | |
| Fujitsu-Dev | TCP/UDP | 747 | Fujitsu Device Control | fujitsu-dev | Cisco IOS XE Release 3.1S | |
| GACP | TCP/UDP | 190 | Gateway Access Control Protocol | gacp | Cisco IOS XE Release 3.1S | |
| GDOMAP | TCP/UDP | 538 | gdomap | gdomap | Cisco IOS XE Release 3.1S | |
| Genie | TCP/UDP | 402 | Genie Protocol | genie | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| | Genrad-MUX | TCP/UDP | 176 | Genrad-mux | genrad-mux | Cisco IOS XE Release 3.1S |
| | GGF-NCP | TCP/UDP | 678 | GNU Generation Foundation NCP | ggf-ncp | Cisco IOS XE Release 3.1S |
| GGP | TCP/UDP | 3 | Gateway-to-Gateway | ggp | Cisco IOS XE Release 3.1S | |
| Ginad | TCP/UDP | 634 | ginad | ginad | Cisco IOS XE Release 3.1S | |
| GMTP | TCP/UDP | 100 | GMTP | gmtp | Cisco IOS XE Release 3.1S | |
| Go-Login | TCP/UDP | 491 | Go-login | go-login | Cisco IOS XE Release 3.1S | |
| Gopher | TCP/UDP | 70 | Gopher | gopher | Cisco IOS XE Release 3.1S | |
| Graphics | TCP/UDP | 41 | Graphics | graphics | Cisco IOS XE Release 3.1S | |
| GRE | TCP/UDP | 47 | General Routing Encapsulation | gre | Cisco IOS XE Release 3.1S | |
| Groove | TCP/UDP | 2492 | Groove | groove | Cisco IOS XE Release 3.1S | |
| GSS-HTTP | TCP/UDP | 488 | gss-http | gss-http | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| GSS-XLICEN | TCP/UDP | 128 | GNU Generation Foundation NCP | gss-xlicen | Cisco IOS XE Release 3.1S | |
| GTP-User | TCP/UDP | 2152 | GTP-User Plane | gtp-user | Cisco IOS XE Release 3.1S | |
| HA-Cluster | TCP/UDP | 694 | ha-cluster | ha-cluster | Cisco IOS XE Release 3.1S | |
| HAP | TCP/UDP | 661 | hap | hap | Cisco IOS XE Release 3.1S | |
| Hassle | TCP/UDP | 375 | Hassle | hassle | Cisco IOS XE Release 3.1S | |
| HCP-Wismar | TCP/UDP | 686 | Hardware Control Protocol Wismar | hcp-wismar | Cisco IOS XE Release 3.1S | |
| HDAP | TCP/UDP | 263 | hdap | hdap | Cisco IOS XE Release 3.1S | |
| Hello-port | TCP/UDP | 652 | HELLO_PORT | hello-port | Cisco IOS XE Release 3.1S | |
| HEMS | TCP/UDP | 151 | hems | hems | Cisco IOS XE Release 3.1S | |
| | HIP | TCP/UDP | 139 | Host Identity Protocol | hip | Cisco IOS XE Release 3.1S |
| | HL7 | TCP | Dynamically assigned | Health Level Seven | hl7 | 12.2(18)ZYA 12.2(18)ZYA1 |
| HMMP-IND | TCP/UDP | 612 | HMMP Indication | hmmp-ind | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| HMMP-OP | TCP/UDP | 613 | HMMP Operation | hmmp-op | Cisco IOS XE Release 3.1S | |
| HMP | TCP/UDP | 20 | Host Monitoring | hmp | Cisco IOS XE Release 3.1S | |
| HOPOPT | TCP/UDP | 0 | IPv6 Hop-by-Hop Option | hopopt | Cisco IOS XE Release 3.1S | |
| Hostname | TCP/UDP | 101 | NIC Host Name Server | hostname | Cisco IOS XE Release 3.1S | |
| HP-Alarm-Mgr | TCP/UDP | 383 | HP performance data alarm manager | hp-alarm-mgr | Cisco IOS XE Release 3.1S | |
| HP-Collector | TCP/UDP | 381 | HP performance data collector | hp-collector | Cisco IOS XE Release 3.1S | |
| HP-ManagedNode | TCP/UDP | 382 | HP performance data managed node | hp-managed-node | Cisco IOS XE Release 3.1S | |
| HTTP-ALT | TCP/UDP | 8080 | HTTP Alternate | http-alt | Cisco IOS XE Release 3.1S | |
| HTTP-Mgmt | TCP/UDP | 280 | http-mgmt | http-mgmt | Cisco IOS XE Release 3.1S | |
| HTTPRPCEPMAP | TCP/UDP | 593 | HTTP RPC Ep Map | http-rpc-epmap | Cisco IOS XE Release 3.1S | |
| Hybrid-POP | TCP/UDP | 473 | Hybrid-pop | hybrid-pop | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Hyper-G | TCP/UDP | 418 | Hyper-g | hyper-g | Cisco IOS XE Release 3.1S | |
| Hyperwave-ISP | TCP/UDP | 692 | Hyperwave-isp | hyperwave-isp | Cisco IOS XE Release 3.1S | |
| IAFDBase | TCP/UDP | 480 | iafdbase | iafdbase | Cisco IOS XE Release 3.1S | |
| IAFServer | TCP/UDP | 479 | iafserver | iafserver | Cisco IOS XE Release 3.1S | |
| IASD | TCP/UDP | 432 | iasd | iasd | Cisco IOS XE Release 3.1S | |
| IATP | TCP/UDP | 117 | Interactive Agent Transfer Protocol | iatp | Cisco IOS XE Release 3.1S | |
| IBM-App | TCP/UDP | 385 | IBM Application | ibm-app | Cisco IOS XE Release 3.1S | |
| | IBM-DB2 | TCP/UDP | 523 | IBM-DB2 | ibm-db2 | Cisco IOS XE Release 3.1S |
| IBProtocol | TCP/UDP | 6714 | Internet Backplane Protocol | ibprotocol | Cisco IOS XE Release 3.1S | |
| ICLCNet-Locate | TCP/UDP | 886 | ICL coNETion locate server | iclcnet-locate | Cisco IOS XE Release 3.1S | |
| ICLNet_SVInfo | TCP/UDP | 887 | ICL coNETion server info | iclcnet_svinfo | Cisco IOS XE Release 3.1S | |
| ICMP | TCP/UDP | 1 | Internet Control Message | icmp | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| IDFP | TCP/UDP | 549 | idfp | idfp | Cisco IOS XE Release 3.1S | |
| IDPR | TCP/UDP | 35 | Inter-Domain Policy Routing Protocol | idpr | Cisco IOS XE Release 3.1S | |
| IDPRr-CMTP | TCP/UDP | 38 | IDPR Control Message Transport Protocol | idpr-cmtp | Cisco IOS XE Release 3.1S | |
| IDRP | TCP/UDP | 45 | Inter-Domain Routing Protocol | idrp | Cisco IOS XE Release 3.1S | |
| IEEE-MMS | TCP/UDP | 651 | ieee-mms | ieee-mms | Cisco IOS XE Release 3.1S | |
| IEEE-MMS-SSL | TCP/UDP | 695 | ieee-mms-ssl | ieee-mms-ssl | Cisco IOS XE Release 3.1S | |
| IFMP | TCP/UDP | 101 | Ipsilon Flow Management Protocol | ifmp | Cisco IOS XE Release 3.1S | |
| IGRP | TCP/UDP | 9 | Cisco interior gateway | igrp | Cisco IOS XE Release 3.1S | |
| IIOP | TCP/UDP | 535 | iiop | iiop | Cisco IOS XE Release 3.1S | |
| IL | TCP/UDP | 40 | IL Transport Protocol | il | Cisco IOS XE Release 3.1S | |
| IMSP | TCP/UDP | 406 | Interactive Mail Support Protocol | imsp | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| InBusiness | TCP/UDP | 244 | Inbusiness | inbusiness | Cisco IOS XE Release 3.1S | |
| Infoseek | TCP/UDP | 414 | InfoSeek | infoseek | Cisco IOS XE Release 3.1S | |
| Ingres-Net | TCP/UDP | 134 | INGRES-NET Service | ingres-net | Cisco IOS XE Release 3.1S | |
| | I-NLSP | TCP/UDP | 52 | Integrated Net Layer Security TUBA | i-nlsp | Cisco IOS XE Release 3.1S |
| Intecourier | TCP/UDP | 495 | Intecourier | intecourier | Cisco IOS XE Release 3.1S | |
| Integra-SME | TCP/UDP | 484 | Integra Software Management Environment | integra-sme | Cisco IOS XE Release 3.1S | |
| Intrinsia | TCP/UDP | 503 | intrinsa | intrinsa | Cisco IOS XE Release 3.1S | |
| IPCD | TCP/UDP | 576 | ipcd | ipcd | Cisco IOS XE Release 3.1S | |
| IPComp | TCP/UDP | 108 | IP Payload Compression Protocol | ipcomp | Cisco IOS XE Release 3.1S | |
| IPCServer | TCP/UDP | 600 | Sun IPC server | ipcserver | Cisco IOS XE Release 3.1S | |
| IPCV | TCP/UDP | 71 | Internet Packet Core Utility | ipcv | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| IPDD | TCP/UDP | 578 | ipdd | ipdd | Cisco IOS XE Release 3.1S | |
| IPINIP | TCP/UDP | 4 | IP in IP | ipinip | Cisco IOS XE Release 3.1S | |
| IPIP | TCP/UDP | 94 | IP-within-IP Encapsulation Protocol | ipip | Cisco IOS XE Release 3.1S | |
| IPLT | TCP/UDP | 129 | IPLT | iplt | Cisco IOS XE Release 3.1S | |
| IPP | TCP/UDP | 631 | Internet Printing Protocol | ipp | Cisco IOS XE Release 3.1S | |
| IPPC | TCP/UDP | 67 | Internet Pluribus Packet Core | ippc | Cisco IOS XE Release 3.1S | |
| Ipv6-Frag | TCP/UDP | 44 | Fragment Header for IPv6 | ipv6-frag | Cisco IOS XE Release 3.1S | |
| Ipv6-ICMP | TCP/UDP | 58 | ICMP for IPv6 | ipv6-icmp | Cisco IOS XE Release 3.1S | |
| Ipv6INIP | TCP/UDP | 41 | Ipv6 encapsulated | ipv6inip | Cisco IOS XE Release 3.1S | |
| ipv6-NonXT | TCP/UDP | 59 | No Next Header for IPv6 | ipv6-nonxt | Cisco IOS XE Release 3.1S | |
| | Ipv6-OPTS | TCP/UDP | 60 | Destination Options for IPv6 | ipv6-opts | Cisco IOS XE Release 3.1S |
| Ipv6-Route | TCP/UDP | 43 | Routing Header for IPv6 | ipv6-route | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| IRC | TCP/UDP | 194 | Internet Relay Chat | irc | Cisco IOS XE Release 3.1S | |
| IRC-SERV | TCP/UDP | 529 | IRC-SERV | irc-serv | Cisco IOS XE Release 3.1S | |
| IRTP | TCP/UDP | 28 | Internet Reliable Transaction | irtp | Cisco IOS XE Release 3.1S | |
| IS99C | TCP/UDP | 379 | TIA/EIA/IS-99 modem client | is99c | Cisco IOS XE Release 3.1S | |
| IS99S | TCP/UDP | 380 | TIA/EIA/IS-99 modem server | is99s | Cisco IOS XE Release 3.1S | |
| ISAKMP | UDP | 500, 4500 | Internet Security Association & Key Management Protocol | isakmp | Cisco IOS XE Release 3.1S | |
| ISI-GI | TCP/UDP | 55 | ISI Graphics Language | isi-gl | Cisco IOS XE Release 3.1S | |
| ISIS | TCP/UDP | 124 | ISIS over IPv4 | isis | Cisco IOS XE Release 3.1S | |
| ISO-ILL | TCP/UDP | 499 | ISO ILL Protocol | iso-ill | Cisco IOS XE Release 3.1S | |
| ISO-IP | TCP/UDP | 147 | iso-ip | iso-ip | Cisco IOS XE Release 3.1S | |
| ISO-TP0 | TCP/UDP | 146 | iso-tp0 | iso-tp0 | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| ISO-TP4 | TCP/UDP | 29 | ISO Transport Protocol Class 4 | iso-tp4 | Cisco IOS XE Release 3.1S | |
| ISO-TSAP | TCP/UDP | 102 | ISO-TSAP Class 0 | iso-tsap | Cisco IOS XE Release 3.1S | |
| ISO-TSAP-C2 | TCP/UDP | 399 | ISO Transport Class 2 Non-Control | iso-tsap-c2 | Cisco IOS XE Release 3.1S | |
| ITM-MCELL-S | TCP/UDP | 828 | itm-mcell-s | itm-mcell-s | Cisco IOS XE Release 3.1S | |
| IXP-IN-IP | TCP/UDP | 111 | IPX in IP | ixp-in-ip | Cisco IOS XE Release 3.1S | |
| Jargon | TCP/UDP | 148 | Jargon | jargon | Cisco IOS XE Release 3.1S | |
| | Kali | TCP/UDP | 2213 | Kali | kali | Cisco IOS XE Release 3.1S |
| | K-Block | TCP/UDP | 287 | K-block | k-block | Cisco IOS XE Release 3.1S |
| Keyserver | TCP/UDP | 584 | Key Server | keyserver | Cisco IOS XE Release 3.1S | |
| KIS | TCP/UDP | 186 | KIS Protocol | kis | Cisco IOS XE Release 3.1S | |
| Klogin | TCP/UDP | 543 | klogin | klogin | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Knet-CMP | TCP/UDP | 157 | KNET/VM Command Message Protocol | knet-cmp | Cisco IOS XE Release 3.1S | |
| Konspire2b | TCP/UDP | 6085 | Konspire2b p2p network | Konspire2b | Cisco IOS XE Release 3.1S | |
| Kpasswd | TCP/UDP | 464 | Kpasswd | kpasswd | Cisco IOS XE Release 3.1S | |
| Kryptolan | TCP/UDP | 398 | Kryptolan | kryptolan | Cisco IOS XE Release 3.1S | |
| Kshell | TCP/UDP | 544 | Kshell | kshell | Cisco IOS XE Release 3.1S | |
| L2TP | TCP/UDP | 1701 | l2tp | l2tp | Cisco IOS XE Release 3.1S | |
| | | | | | | |
| LA-Maint | TCP/UDP | 51 | IMP Logical Address Maintenance | la-maint | Cisco IOS XE Release 3.1S | |
| LANServer | TCP/UDP | 637 | lanserver | lanserver | Cisco IOS XE Release 3.1S | |
| LARP | TCP/UDP | 91 | Locus Address Resolution Protocol | larp | Cisco IOS XE Release 3.1S | |
| LDAP | TCP/UDP | 389 | Lightweight Directory Access Protocol | ldap | Cisco IOS XE Release 3.1S | |
| LDP | TCP/UDP | 646 | LDP | ldp | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Leaf-1 | TCP/UDP | 25 | Leaf-1 | leaf-1 | Cisco IOS XE Release 3.1S | |
| Leaf-2 | TCP/UDP | 26 | Leaf-2 | leaf-2 | Cisco IOS XE Release 3.1S | |
| Legent-1 | TCP/UDP | 373 | Legent Corporation | legent-1 | Cisco IOS XE Release 3.1S | |
| | Legent-2 | TCP/UDP | 374 | Legent Corporation | legent-2 | Cisco IOS XE Release 3.1S |
| LJK-Login | TCP/UDP | 472 | ljk-login | ljk-login | Cisco IOS XE Release 3.1S | |
| Lockd | TCP/UDP | 4045 | NFS Lock Daemon Manager | lockd | Cisco IOS XE Release 3.1S | |
| Locus-Con | TCP/UDP | 127 | Locus PC-Interface Conn Server | locus-con | Cisco IOS XE Release 3.1S | |
| Locus-Map | TCP/UDP | 125 | Locus PC-Interface Net Map Ser | locus-map | Cisco IOS XE Release 3.1S | |
| MACSRVR-Admin | TCP/UDP | 660 | MacOS Server Admin | mac-srvr-admin | Cisco IOS XE Release 3.1S | |
| Magenta-Logic | TCP/UDP | 313 | Magenta-logic | magenta-logic | Cisco IOS XE Release 3.1S | |
| Mailbox-LM | TCP/UDP | 505 | Mailbox-lm | mailbox-lm | Cisco IOS XE Release 3.1S | |
| Mailq | TCP/UDP | 174 | MAILQ | mailq | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Maitrd | TCP/UDP | 997 | Maitrd | maitrd | Cisco IOS XE Release 3.1S | |
| MANET | TCP/UDP | 138 | MANET Protocols | manet | Cisco IOS XE Release 3.1S | |
| MasqDialer | TCP/UDP | 224 | Masqdialer | masqdialer | Cisco IOS XE Release 3.1S | |
| Matip-Type-A | TCP/UDP | 350 | MATIP Type A | matip-type-a | Cisco IOS XE Release 3.1S | |
| Matip-Type-B | TCP/UDP | 351 | MATIP Type B | matip-type-b | Cisco IOS XE Release 3.1S | |
| MCIDAS | TCP/UDP | 112 | McIDAS Data Transmission Protocol | mcidas | Cisco IOS XE Release 3.1S | |
| MCNS-Sec | TCP/UDP | 638 | mcns-sec | mcns-sec | Cisco IOS XE Release 3.1S | |
| MDC-Portmapper | TCP/UDP | 685 | mdc-portmapper | mdc-portmapper | Cisco IOS XE Release 3.1S | |
| MeComm | TCP/UDP | 668 | MeComm | mecomm | Cisco IOS XE Release 3.1S | |
| | MeRegister | TCP/UDP | 669 | MeRegister | meregister | Cisco IOS XE Release 3.1S |
| Merit-INP | TCP/UDP | 32 | MERIT Internodal Protocol | merit-inp | Cisco IOS XE Release 3.1S | |
| Meta5 | TCP/UDP | 393 | Meta5 | meta5 | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Metagram | TCP/UDP | 99 | Metagram | metagram | Cisco IOS XE Release 3.1S | |
| Meter | TCP/UDP | 570 | Meter | meter | Cisco IOS XE Release 3.1S | |
| Mfcobol | TCP/UDP | 86 | Micro Focus Cobol | mfcobol | Cisco IOS XE Release 3.1S | |
| MFE-NSP | TCP/UDP | 31 | MFE Network Services Protocol | mfe-nsp | Cisco IOS XE Release 3.1S | |
| MFTP | TCP/UDP | 349 | mftp | mftp | Cisco IOS XE Release 3.1S | |
| Micom-PFS | TCP/UDP | 490 | Micom-pfs | micom-pfs | Cisco IOS XE Release 3.1S | |
| MICP | TCP/UDP | 95 | Mobile Internetworking Control Pro. | micp | Cisco IOS XE Release 3.1S | |
| Micromuse-LM | TCP/UDP | 1534 | micromuse-lm | micromuse-lm | Cisco IOS XE Release 3.1S | |
| MIT-DOV | TCP/UDP | 91 | MIT Dover Spooler | mit-dov | Cisco IOS XE Release 3.1S | |
| MIT-ML-Dev | TCP/UDP | 83 | MIT ML Device | mit-ml-dev | Cisco IOS XE Release 3.1S | |
| Mobile | TCP/UDP | 55 | IP Mobility | mobile | Cisco IOS XE Release 3.1S | |
| MobileIP-Agent | TCP/UDP | 434 | mobileip-agent | mobileip-agent | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| MobilIP-MN | TCP/UDP | 435 | mobilip-mn | mobilip-mn | Cisco IOS XE Release 3.1S | |
| Mondex | TCP/UDP | 471 | Mondex | mondex | Cisco IOS XE Release 3.1S | |
| Monitor | TCP/UDP | 561 | Monitor | monitor | Cisco IOS XE Release 3.1S | |
| Mortgageware | TCP/UDP | 367 | Mortgageware | mortgageware | Cisco IOS XE Release 3.1S | |
| | MPLS-IN-IP | TCP/UDP | 137 | MPLS-in-IP | mpls-in-ip | Cisco IOS XE Release 3.1S |
| MPM | TCP/UDP | 45 | Message Processing Module | mpm | Cisco IOS XE Release 3.1S | |
| MPM-Flags | TCP/UDP | 44 | MPM FLAGS Protocol | mpm-flags | Cisco IOS XE Release 3.1S | |
| MPM-SND | TCP/UDP | 46 | MPM [default send] | mpm-snd | Cisco IOS XE Release 3.1S | |
| MPP | TCP/UDP | 218 | Netix Message Posting Protocol | mpp | Cisco IOS XE Release 3.1S | |
| MPTN | TCP/UDP | 397 | Multi Protocol Transport Network | mptn | Cisco IOS XE Release 3.1S | |
| MRM | TCP/UDP | 679 | mrm | mrm | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| MSDP | TCP/UDP | 639 | msdp | msdp | Cisco IOS XE Release 3.1S | |
| MSExch-Routing | TCP/UDP | 691 | MS Exchange Routing | msexch-routing | Cisco IOS XE Release 3.1S | |
| MSFT-GC | TCP/UDP | 3268 | Microsoft Global Catalog | msft-gc | Cisco IOS XE Release 3.1S | |
| MSFT-GC-SSL | TCP/UDP | 3269 | Microsoft Global Catalog with LDAP/SSL | msft-gc-ssl | Cisco IOS XE Release 3.1S | |
| MSG-AUTH | TCP/UDP | 31 | msg-auth | msg-auth | Cisco IOS XE Release 3.1S | |
| MSG-ICP | TCP/UDP | 29 | msg-icp | msg-icp | Cisco IOS XE Release 3.1S | |
| MSNP | TCP/UDP | 1863 | msnp | msnp | Cisco IOS XE Release 3.1S | |
| MS-OLAP | TCP/UDP | 2393 | Microsoft OLAP | ms-olap | Cisco IOS XE Release 3.1S | |
| MSP | TCP/UDP | 18 | Message Send Protocol | msp | Cisco IOS XE Release 3.1S | |
| MS-Rome | TCP/UDP | 569 | Microsoft rome | ms-rome | Cisco IOS XE Release 3.1S | |
| MS-Shuttle | TCP/UDP | 568 | Microsoft shuttle | ms-shuttle | Cisco IOS XE Release 3.1S | |
| MS-SQLl-M | TCP/UDP | 1434 | Microsoft SQL Monitor | ms-sql-m | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| | MS-wbt | TCP | 3389/Heuristic | Microsoft Windows based Terminal Services | ms-wbt | Cisco IOS XE Release 3.4S |
| | MTP | TCP/UDP | 92 | Multicast Transport Protocol | mtp | Cisco IOS XE Release 3.1S |
| Multiling-HTTP | TCP/UDP | 777 | Multiling HTTP | multiling-http | Cisco IOS XE Release 3.1S | |
| Multiplex | TCP/UDP | 171 | Network Innovations Multiplex | multiplex | Cisco IOS XE Release 3.1S | |
| Mumps | TCP/UDP | 188 | Plus Fives MUMPS | mumps | Cisco IOS XE Release 3.1S | |
| MUX | TCP/UDP | 18 | Multiplexing | mux | Cisco IOS XE Release 3.1S | |
| Mylex-MAPD | TCP/UDP | 467 | mylex-mapd | mylex-mapd | Cisco IOS XE Release 3.1S | |
| MySQL | TCP/UDP | 3306 | MySQL | mysql | Cisco IOS XE Release 3.1S | |
| Name | TCP/UDP | 42 | Host Name Server | name | Cisco IOS XE Release 3.1S | |
| NAMP | TCP/UDP | 167 | namp | namp | Cisco IOS XE Release 3.1S | |
| NARP | TCP/UDP | 54 | NBMA Address Resolution Protocol | narp | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| NAS | TCP/UDP | 991 | Netnews Administration System | nas | Cisco IOS XE Release 3.1S | |
| NCED | TCP/UDP | 404 | nced | nced | Cisco IOS XE Release 3.1S | |
| NCLD | TCP/UDP | 405 | ncld | ncld | Cisco IOS XE Release 3.1S | |
| NCP | TCP/UDP | 524 | NCP | ncp | Cisco IOS XE Release 3.1S | |
| NDSAuth | TCP/UDP | 353 | NDSAUTH | ndsauth | Cisco IOS XE Release 3.1S | |
| Nest-Protocol | TCP/UDP | 489 | Nest-protocol | nest-protocol | Cisco IOS XE Release 3.1S | |
| Net8-CMAN | TCP/UDP | 1830 | Oracle Net8 CMan Admin | net8-cman | Cisco IOS XE Release 3.1S | |
| Net-Assistant | TCP/UDP | 3283 | net-assistant | net-assistant | Cisco IOS XE Release 3.1S | |
| Netblt | TCP/UDP | 30 | Bulk Data Transfer Protocol | netblt | Cisco IOS XE Release 3.1S | |
| | NetGW | TCP/UDP | 741 | netgw | netgw | Cisco IOS XE Release 3.1S |
| | NetNews | TCP/UDP | 532 | readnews | netnews | Cisco IOS XE Release 3.1S |
| NetRCS | TCP/UDP | 742 | Network based RCS | netrcs | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| NetRJS-1 | TCP/UDP | 71 | Remote Job Service | netrjs-1 | Cisco IOS XE Release 3.1S | |
| NetRJS-2 | TCP/UDP | 72 | Remote Job Service | netrjs-2 | Cisco IOS XE Release 3.1S | |
| NetRJS-3 | TCP/UDP | 73 | Remote Job Service | netrjs-3 | Cisco IOS XE Release 3.1S | |
| NetRJS-4 | TCP/UDP | 74 | Remote Job Service | netrjs-4 | Cisco IOS XE Release 3.1S | |
| NETSC-Dev | TCP/UDP | 155 | NETSC | netsc-dev | Cisco IOS XE Release 3.1S | |
| NETSC-Prod | TCP/UDP | 154 | NETSC | netsc-prod | Cisco IOS XE Release 3.1S | |
| NetViewDM1 | TCP/UDP | 729 | IBM NetView M | netviewdm1 | Cisco IOS XE Release 3.1S | |
| NetviewDM2 | TCP/UDP | 730 | IBM NetView DM | netviewdm2 | Cisco IOS XE Release 3.1S | |
| NetviewDM3 | TCP/UDP | 731 | IBM NetView DM | netviewdm3 | Cisco IOS XE Release 3.1S | |
| Netwall | TCP/UDP | 533 | for emergency broadcasts | netwall | Cisco IOS XE Release 3.1S | |
| Netware-IP | TCP/UDP | 396 | Novell Netware over IP | netware-ip | Cisco IOS XE Release 3.1S | |
| New-RWHO | TCP/UDP | 550 | new who | new-rwho | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| NextStep | TCP/UDP | 178 | NextStep Window Server | nextstep | Cisco IOS XE Release 3.1S | |
| NFS | TCP/UDP | 2049 | Network File System | nfs | Cisco IOS XE Release 3.1S | |
| NicName | TCP/UDP | 43 | Who Is | nicname | Cisco IOS XE Release 3.1S | |
| NI-FTP | TCP/UDP | 47 | NI FTP | ni-ftp | Cisco IOS XE Release 3.1S | |
| NI-Mail | TCP/UDP | 61 | NI MAIL | ni-mail | Cisco IOS XE Release 3.1S | |
| | Nlogin | TCP/UDP | 758 | nlogin | nlogin | Cisco IOS XE Release 3.1S |
| | NMAP | TCP/UDP | 689 | nmap | nmap | Cisco IOS XE Release 3.1S |
| NMSP | TCP/UDP | 537 | Networked Media Streaming Protocol | nmsp | Cisco IOS XE Release 3.1S | |
| NNSP | TCP/UDP | 433 | nnsp | nnsp | Cisco IOS XE Release 3.1S | |
| Notes | TCP/UDP | 1352 | Lotus Notes(R) | notes | Cisco IOS XE Release 3.1S | |
| NovaStorBakcup | TCP/UDP | 308 | Novastor Backup | novastorbakcup | Cisco IOS XE Release 3.1S | |
| NPMP-GUI | TCP/UDP | 611 | npmp-gui | npmp-gui | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| NPMP-Local | TCP/UDP | 610 | npmp-local | npmp-local | Cisco IOS XE Release 3.1S | |
| NPMP-Trap | TCP/UDP | 609 | npmp-trap | npmp-trap | Cisco IOS XE Release 3.1S | |
| NPP | TCP/UDP | 92 | Network Printing Protocol | npp | Cisco IOS XE Release 3.1S | |
| NQS | TCP/UDP | 607 | nqs | nqs | Cisco IOS XE Release 3.1S | |
| NS | TCP/UDP | 760 | ns | ns | Cisco IOS XE Release 3.1S | |
| NSFNET-IGP | TCP/UDP | 85 | NSFNET-IGP | nsfnet-igp | Cisco IOS XE Release 3.1S | |
| NSIIOPS | TCP/UDP | 261 | IIOP Name Service over TLS/SSL | nsiiops | Cisco IOS XE Release 3.1S | |
| NSRMP | TCP/UDP | 359 | Network Security Risk Management Protocol | nsrmp | Cisco IOS XE Release 3.1S | |
| NSS-Routing | TCP/UDP | 159 | NSS-Routing | nss-routing | Cisco IOS XE Release 3.1S | |
| NSW-FE | TCP/UDP | 27 | NSW User System FE | nsw-fe | Cisco IOS XE Release 3.1S | |
| Ntalk | TCP/UDP | 518 | Ntalk | ntalk | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| NTP | TCP/ UDP | 123 | Network Time Protocol | ntp | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S | |
| | | | | | | |
| | NVP-II | TCP/UDP | 11 | Network Voice Protocol | nvp-ii | Cisco IOS XE Release 3.1S |
| NXEdit | TCP/UDP | 126 | nxedit | nxedit | Cisco IOS XE Release 3.1S | |
| OBCBinder | TCP/UDP | 183 | ocbinder | ocbinder | Cisco IOS XE Release 3.1S | |
| OBEX | TCP/UDP | 650 | obex | obex | Cisco IOS XE Release 3.1S | |
| ObjCall | TCP/UDP | 94 | Tivoli Object Dispatcher | objcall | Cisco IOS XE Release 3.1S | |
| OCS_AMU | TCP/UDP | 429 | ocs_amu | ocs_amu | Cisco IOS XE Release 3.1S | |
| OCS_CMU | TCP/UDP | 428 | ocs_cmu | ocs_cmu | Cisco IOS XE Release 3.1S | |
| OCServer | TCP/UDP | 184 | ocserver | ocserver | Cisco IOS XE Release 3.1S | |
| ODMR | TCP/UDP | 366 | odmr | odmr | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| OHIMSRV | TCP/UDP | 506 | ohimsrv | ohimsrv | Cisco IOS XE Release 3.1S | |
| OLSR | TCP/UDP | 698 | olsr | olsr | Cisco IOS XE Release 3.1S | |
| OMGInitialRefs | TCP/UDP | 900 | omginitialrefs | omginitialrefs | Cisco IOS XE Release 3.1S | |
| OMServ | TCP/UDP | 764 | omserv | omserv | Cisco IOS XE Release 3.1S | |
| ONMUX | TCP/UDP | 417 | onmux | onmux | Cisco IOS XE Release 3.1S | |
| Opalis-RDV | TCP/UDP | 536 | Opalis-rdv | opalis-rdv | Cisco IOS XE Release 3.1S | |
| Opalis-Robot | TCP/UDP | 314 | oOpalis-robot | opalis-robot | Cisco IOS XE Release 3.1S | |
| OPC-Job-Start | TCP/UDP | 423 | IBM Operations Planning and Control Start | opc-job-start | Cisco IOS XE Release 3.1S | |
| OPC-Job-Track | TCP/UDP | 424 | IBM Operations Planning and Control Track | opc-job-track | Cisco IOS XE Release 3.1S | |
| | Openport | TCP/UDP | 260 | Openport | openport | Cisco IOS XE Release 3.1S |
| OpenVMS-Sysipc | TCP/UDP | 557 | Openvms-sysipc | openvms-sysipc | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| OracleNames | TCP/UDP | 1575 | Oraclenames | oraclenames | Cisco IOS XE Release 3.1S | |
| OracleNet8CMAN | TCP/UDP | 1630 | Oracle Net8 Cman | oraclenet8cman | Cisco IOS XE Release 3.1S | |
| ORA-Srv | TCP/UDP | 1525 | Oracle TCP/IP Listener | ora-srv | 12.2(18)ZYA 12.2(18)ZYA Cisco IOS XE Release 3.1S | |
| Orbix-Config | TCP/UDP | 3076 | Orbix 2000 Config | orbix-config | Cisco IOS XE Release 3.1S | |
| Orbix-Locator | TCP/UDP | 3075 | Orbix 2000 Locator | orbix-locator | Cisco IOS XE Release 3.1S | |
| Orbix-Loc-SSL | TCP/UDP | 3077 | Orbix 2000 Locator SSL | orbix-loc-ssl | Cisco IOS XE Release 3.1S | |
| OSPF | TCP/UDP | 89 | Open Shortest Path First | ospf | Cisco IOS XE Release 3.1S | |
| OSU-NMS | TCP/UDP | 192 | OSU Network Monitoring System | osu-nms | Cisco IOS XE Release 3.1S | |
| Parsec-Game | TCP/UDP | 6582 | Parsec Gameserver | parsec-game | Cisco IOS XE Release 3.1S | |
| Passgo | TCP/UDP | 511 | Passgo | passgo | Cisco IOS XE Release 3.1S | |
| Passgo-Tivoli | TCP/UDP | 627 | Passgo-tivoli | passgo-tivoli | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Password-Chg | TCP/UDP | 586 | Password Change | password-chg | Cisco IOS XE Release 3.1S | |
| Pawserv | TCP/UDP | 345 | Perf Analysis Workbench | pawserv | Cisco IOS XE Release 3.1S | |
| PCMail-SRV | TCP/UDP | 158 | PCMail Server | pcmail-srv | Cisco IOS XE Release 3.1S | |
| PDAP | TCP/UDP | 344 | Prospero Data Access Protocol | pdap | Cisco IOS XE Release 3.1S | |
| Personal-link | TCP/UDP | 281 | Personal-link | personal-link | Cisco IOS XE Release 3.1S | |
| PFTP | TCP/UDP | 662 | Parallel File Transfer Protocol | pftp | Cisco IOS XE Release 3.1S | |
| | PGM | TCP/UDP | 113 | PGM Reliable Transport Protocol | pgm | Cisco IOS XE Release 3.1S |
| Philips-VC | TCP/UDP | 583 | Philips VideoConferencing | philips-vc | Cisco IOS XE Release 3.1S | |
| Phonebook | TCP/UDP | 767 | Phone | phonebook | Cisco IOS XE Release 3.1S | |
| Photuris | TCP/UDP | 468 | Photuris | photuris | Cisco IOS XE Release 3.1S | |
| PIM | TCP/UDP | 103 | Protocol Independent Multicast | pim | Cisco IOS XE Release 3.1S | |
| PIM-RP-DISC | TCP/UDP | 496 | PIM-RP-DISC | pim-rp-disc | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| PIP | TCP/UDP | 1321 | pip | pip | Cisco IOS XE Release 3.1S | |
| PIPE | TCP/UDP | 131 | Private IP Encapsulation within IP | pipe | Cisco IOS XE Release 3.1S | |
| PIRP | TCP/UDP | 553 | pirp | pirp | Cisco IOS XE Release 3.1S | |
| PKIX-3-CA-RA | TCP/UDP | 829 | PKIX-3 CA/RA | pkix-3-ca-ra | Cisco IOS XE Release 3.1S | |
| PKIX-Timestamp | TCP/UDP | 318 | pkix-timestamp | pkix-timestamp | Cisco IOS XE Release 3.1S | |
| PNNI | TCP/UDP | 102 | PNNI over IP | pnni | Cisco IOS XE Release 3.1S | |
| Pop2 | TCP/UDP | 109 | Post Office Protocol - Version 2 | pop2 | Cisco IOS XE Release 3.1S | |
| Pop3 | TCP/UDP | 110, Heuristic | Post Office Protocol 3 | pop3 | Cisco IOS XE Release 3.1S | |
| POV-Ray | TCP/UDP | 494 | pov-ray | pov-ray | Cisco IOS XE Release 3.1S | |
| Powerburst | TCP/UDP | 485 | Air Soft Power Burst | powerburst | Cisco IOS XE Release 3.1S | |
| PPStream | TCP/UDP | Heuristic | P2P TV Application | ppstream | Cisco IOS XE Release 3.3S | |
| PPTP | TCP/UDP | 1723 | Point-to-Point Tunneling Protocol | pptp | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| | Printer | TCP/UDP | 515 | spooler | printer | 12.1(2)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S |
| Print-SRV | TCP/UDP | 170 | Network PostScript | print-srv | Cisco IOS XE Release 3.1S | |
| PRM | TCP/UDP | 21 | Packet Radio Measurement | prm | Cisco IOS XE Release 3.1S | |
| PRM-NM | TCP/UDP | 409 | Prospero Resource Manager Node Man | prm-nm | Cisco IOS XE Release 3.1S | |
| PRM-SM | TCP/UDP | 408 | Prospero Resource Manager Sys. Man | prm-sm | Cisco IOS XE Release 3.1S | |
| Profile | TCP/UDP | 136 | PROFILE Naming System | profile | Cisco IOS XE Release 3.1S | |
| Prospero | TCP/UDP | 191 | Prosper Directory Service | prospero | Cisco IOS XE Release 3.1S | |
| PTCNameService | TCP/UDP | 597 | PTC Name Service | ptcnameservice | Cisco IOS XE Release 3.1S | |
| PTP | TCP/UDP | 123 | Performance Transparency Protocol | ptp | Cisco IOS XE Release 3.1S | |
| PTP-Event | TCP/UDP | 319 | PTP Event | ptp-event | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| PTP-General | TCP/UDP | 320 | PTP General | ptp-general | Cisco IOS XE Release 3.1S | |
| Pump | TCP/UDP | 751 | Pump | pump | Cisco IOS XE Release 3.1S | |
| PUP | TCP/UDP | 12 | PUP | pup | Cisco IOS XE Release 3.1S | |
| Purenoise | TCP/UDP | 663 | purenoise | purenoise | Cisco IOS XE Release 3.1S | |
| PVP | TCP/UDP | 75 | Packet Video Protocol | pvp | Cisco IOS XE Release 3.1S | |
| PWDGen | TCP/UDP | 129 | Password Generator Protocol | pwdgen | Cisco IOS XE Release 3.1S | |
| QBIKGDP | TCP/UDP | 368 | qbikgdp | qbikgdp | Cisco IOS XE Release 3.1S | |
| QFT | TCP/UDP | 189 | Queued File Transport | qft | Cisco IOS XE Release 3.1S | |
| QMQP | TCP/UDP | 628 | qmqp | qmqp | Cisco IOS XE Release 3.1S | |
| | QMTP | TCP/UDP | 209 | The Quick Mail Transfer Protocol | qmtp | Cisco IOS XE Release 3.1S |
| | QNX | TCP/UDP | 106 | QNX | qnx | Cisco IOS XE Release 3.1S |
| QoTD | TCP/UDP | 17 | Quote of the Day | qotd | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| QRH | TCP/UDP | 752 | qrh | qrh | Cisco IOS XE Release 3.1S | |
| QUOTD | TCP/UDP | 762 | quotad | quotad | Cisco IOS XE Release 3.1S | |
| r-commands | TCP | Dynamically assigned | rsh, rlogin, rexec | rcmd | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 | |
| RAP | TCP/UDP | 38 | Route Access Protocol | rap | Cisco IOS XE Release 3.1S | |
| RCMD | TCP | 512–514 | BSD r-commands | rcmd | Cisco IOS XE Release 3.3S | |
| RCP | TCP/UDP | 469 | Radio Control Protocol | rcp | 12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S | |
| RDA | TCP/UDP | 630 | rda | rda | Cisco IOS XE Release 3.1S | |
| RDB-DBS-DISP | TCP/UDP | 1571 | Oracle Remote Data Base | rdb-dbs-disp | Cisco IOS XE Release 3.1S | |
| RDP | TCP/UDP | 27 | Reliable Data Protocol | rdp | Cisco IOS XE Release 3.1S | |
| Realm-RUSD | TCP/UDP | 688 | ApplianceWare managment protocol | realm-rusd | Cisco IOS XE Release 3.1S | |
| RE-Mail-CK | TCP/UDP | 50 | Remote Mail Checking Protocol | re-mail-ck | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| RemoteFS | TCP/UDP | 556 | rfs server | remotefs | Cisco IOS XE Release 3.1S | |
| Remote-KIS | TCP/UDP | 185 | Remote-kis | remote-kis | Cisco IOS XE Release 3.1S | |
| REPCMD | TCP/UDP | 641 | repcmd | repcmd | Cisco IOS XE Release 3.1S | |
| REPSCMD | TCP/UDP | 653 | repscmd | repscmd | Cisco IOS XE Release 3.1S | |
| RESCAP | TCP/UDP | 283 | rescap | rescap | Cisco IOS XE Release 3.1S | |
| RIP | TCP/UDP | 520 | Routing Information Protocol | rip | Cisco IOS XE Release 3.1S | |
| | RIPING | TCP/UDP | 521 | ripng | ripng | Cisco IOS XE Release 3.1S |
| | RIS | TCP/UDP | 180 | Intergraph | ris | Cisco IOS XE Release 3.1S |
| RIS-CM | TCP/UDP | 748 | Russell Info Sci Calendar Manager | ris-cm | Cisco IOS XE Release 3.1S | |
| RJE | TCP/UDP | 5 | Remote Job Entry | rje | Cisco IOS XE Release 3.1S | |
| RLP | TCP/UDP | 39 | Resource Location Protocol | rlp | Cisco IOS XE Release 3.1S | |
| RLZDBASE | TCP/UDP | 635 | rlzdbase | rlzdbase | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| RMC | TCP/UDP | 657 | rmc | rmc | Cisco IOS XE Release 3.1S | |
| RMIActivation | TCP/UDP | 1098 | rmiactivation | rmiactivation | Cisco IOS XE Release 3.1S | |
| RMIRegistry | TCP/UDP | 1099 | rmiregistry | rmiregistry | Cisco IOS XE Release 3.1S | |
| RMonitor | TCP/UDP | 560 | Rmonitord | rmonitor | Cisco IOS XE Release 3.1S | |
| RMT | TCP/UDP | 411 | Remote MT Protocol | rmt | Cisco IOS XE Release 3.1S | |
| RPC2Portmap | TCP/UDP | 369 | rpc2portmap | rpc2portmap | Cisco IOS XE Release 3.1S | |
| RRH | TCP/UDP | 753 | rrh | rrh | Cisco IOS XE Release 3.1S | |
| RRP | TCP/UDP | 648 | Registry Registrar Protocol | rrp | Cisco IOS XE Release 3.1S | |
| RSH-SPX | TCP/UDP | 222 | Berkeley rshd with SPX auth | rsh-spx | Cisco IOS XE Release 3.1S | |
| RSVD | TCP/UDP | 168 | rsvd | rsvd | Cisco IOS XE Release 3.1S | |
| RSVP_Tunnel | TCP/UDP | 363 | rsvp_tunnel | rsvp_tunnel | Cisco IOS XE Release 3.1S | |
| RSVP-E2E-Ignore | TCP/UDP | 134 | RSVP-E2E-IGNORE | rsvp-e2e-ignore | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Rsync | TCP/UDP | 873 | Rsync | rsync | Cisco IOS XE Release 3.1S | |
| RTelnet | TCP/UDP | 107 | Remote Telnet Service | rtelnet | 12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S | |
| | RTIP | TCP/UDP | 771 | Real Time Streaming Protocol | rtip | Cisco IOS XE Release 3.1S |
| RTMP | TCP | Heuristic | Real Time Messaging Protocol | rtmp | Cisco IOS XE Release 3.4S | |
| RTSPS | TCP/UDP | 322 | RTSPS | rtsps | Cisco IOS XE Release 3.1S | |
| Rushd | TCP/UDP | 696 | Rushd | rushd | Cisco IOS XE Release 3.1S | |
| RVD | TCP/UDP | 66 | MIT Remote Virtual Disk Protocol | rvd | Cisco IOS XE Release 3.1S | |
| RXE | TCP/UDP | 761 | rxe | rxe | Cisco IOS XE Release 3.1S | |
| SAFT | TCP/UDP | 487 | saft Simple Asynchronous File Transfer | saft | Cisco IOS XE Release 3.1S | |
| Sanity | TCP/UDP | 643 | Sanity | sanity | Cisco IOS XE Release 3.1S | |
| SAT-EXPAK | TCP/UDP | 64 | SATNET and Backroom EXPAK | sat-expak | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| SAT-Mon | TCP/UDP | 69 | SATNET Monitoring | sat-mon | Cisco IOS XE Release 3.1S | |
| SCC-Security | TCP/UDP | 582 | scc-security | scc-security | Cisco IOS XE Release 3.1S | |
| SCC-SP | TCP/UDP | 96 | Semaphore Communications Sec. Pro. | scc-sp | Cisco IOS XE Release 3.1S | |
| SCO-DTMgr | TCP/UDP | 617 | SCO Desktop Administration Server | sco-dtmgr | Cisco IOS XE Release 3.1S | |
| SCOHELP | TCP/UDP | 457 | scohelp | scohelp | Cisco IOS XE Release 3.1S | |
| SCOI2ODialog | TCP/UDP | 360 | scoi2odialog | scoi2odialog | Cisco IOS XE Release 3.1S | |
| SCO-Inetmgr | TCP/UDP | 615 | Internet Configuration Manager | sco-inetmgr | Cisco IOS XE Release 3.1S | |
| SCO-SysMgr | TCP/UDP | 616 | SCO System Administration Server | sco-sysmgr | Cisco IOS XE Release 3.1S | |
| SCO-Websrvmg3 | TCP/UDP | 598 | SCO Web Server Manager 3 | sco-websrvmg3 | Cisco IOS XE Release 3.1S | |
| SCO-Websrvmgr | TCP/UDP | 620 | SCO WebServer Manager | sco-websrvmgr | Cisco IOS XE Release 3.1S | |
| | SCPS | TCP/UDP | 105 | SCPS | scps | Cisco IOS XE Release 3.1S |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| SCTP | TCP/UDP | 132 | Stream Control Transmission Protocol | sctp | Cisco IOS XE Release 3.1S | |
| SCX-Proxy | TCP/UDP | 470 | scx-proxy | scx-proxy | Cisco IOS XE Release 3.1S | |
| SDNSKMP | TCP/UDP | 558 | SDNSKMP | sdnskmp | Cisco IOS XE Release 3.1S | |
| SDRP | TCP/UDP | 42 | Source Demand Routing Protocol | sdrp | Cisco IOS XE Release 3.1S | |
| Secure-ftp | TCP/UDP | 990 | ftp protocol, control, over TLS/SSL | secure-ftp | Cisco IOS XE Release 3.1S | |
| Secure-IRC | TCP/UDP | 994 | irc protocol over TLS | secure-irc | Cisco IOS XE Release 3.1S | |
| Secure-LDAP | TCP/UDP | 636 | ldap protocol over TLS | secure-ldap | Cisco IOS XE Release 3.1S | |
| Secure-NNTP | TCP/UDP | 563 | nntp protocol over TLS | secure-nntp | Cisco IOS XE Release 3.1S | |
| Secure-Pop3 | TCP/UDP | 995 | pop3 protocol over TLS | secure-pop3 | Cisco IOS XE Release 3.1S | |
| Secure-Telnet | TCP/UDP | 992 | telnet protocol over TLS | secure-telnet | Cisco IOS XE Release 3.1S | |
| Secure-VMTP | TCP/UDP | 82 | SECURE-VMTP | secure-vmtp | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Semantix | TCP/UDP | 361 | Semantix | semantix | Cisco IOS XE Release 3.1S | |
| Send | TCP/UDP | 169 | SEND | send | Cisco IOS XE Release 3.1S | |
| Server-IPX | TCP/UDP | 213 | Internetwork Packet Exchange Protocol | server-ipx | Cisco IOS XE Release 3.1S | |
| Servstat | TCP/UDP | 633 | Service Status update | servstat | Cisco IOS XE Release 3.1S | |
| SET | TCP/UDP | 257 | Secure Electronic Transaction | set | Cisco IOS XE Release 3.1S | |
| SFS-Config | TCP/UDP | 452 | Cray SFS config server | sfs-config | Cisco IOS XE Release 3.1S | |
| | SFS-SMP-Net | TCP/UDP | 451 | Cray Network Semaphore server | sfs-smp-net | Cisco IOS XE Release 3.1S |
| SFTP | TCP/UDP | 115 | Simple File Transfer Protocol | sftp | Cisco IOS XE Release 3.1S | |
| SGCP | TCP/UDP | 440 | sgcp | sgcp | Cisco IOS XE Release 3.1S | |
| SGMP | TCP/UDP | 153 | sgmp | sgmp | Cisco IOS XE Release 3.1S | |
| SGMP-Traps | TCP/UDP | 160 | sgmp-traps | sgmp-traps | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Shockwave | TCP/UDP | 1626 | Shockwave | shockwave | Cisco IOS XE Release 3.1S | |
| Shrinkwrap | TCP/UDP | 358 | Shrinkwrap | shrinkwrap | Cisco IOS XE Release 3.1S | |
| SIAM | TCP/UDP | 498 | siam | siam | Cisco IOS XE Release 3.1S | |
| SIFT-UFT | TCP/UDP | 608 | Sender-Initiated/Unsolicited File Transfer | sift-uft | Cisco IOS XE Release 3.1S | |
| SILC | TCP/UDP | 706 | silc | silc | Cisco IOS XE Release 3.1S | |
| SitaraDir | TCP/UDP | 2631 | Sitaradir | sitaradir | Cisco IOS XE Release 3.1S | |
| SitaraMgmt | TCP/UDP | 2630 | Sitaramgmt | sitaramgmt | Cisco IOS XE Release 3.1S | |
| Sitaraserver | TCP/UDP | 2629 | sitaraserver | sitaraserver | Cisco IOS XE Release 3.1S | |
| SKIP | TCP/UDP | 57 | SKIP | skip | Cisco IOS XE Release 3.1S | |
| SKRONK | TCP/UDP | 460 | skronk | skronk | Cisco IOS XE Release 3.1S | |
| SM | TCP/UDP | 122 | SM | sm | Cisco IOS XE Release 3.1S | |
| Smakynet | TCP/UDP | 122 | Smakynet | smakynet | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| SmartSDP | TCP/UDP | 426 | Smartsdp | smartsdp | Cisco IOS XE Release 3.1S | |
| SMP | TCP/UDP | 121 | Simple Message Protocol | smp | Cisco IOS XE Release 3.1S | |
| | SMPNameRes | TCP/UDP | 901 | smpnameres | smpnameres | Cisco IOS XE Release 3.1S |
| | SMSD | TCP/UDP | 596 | smsd | smsd | Cisco IOS XE Release 3.1S |
| SMSP | TCP/UDP | 413 | Storage Management Services Protocol | smsp | Cisco IOS XE Release 3.1S | |
| SMUX | TCP/UDP | 199 | SMUX | smux | Cisco IOS XE Release 3.1S | |
| SNAGas | TCP/UDP | 108 | SNA Gateway Access Server | snagas | Cisco IOS XE Release 3.1S | |
| Snare | TCP/UDP | 509 | Snare | snare | Cisco IOS XE Release 3.1S | |
| S-Net | TCP/UDP | 166 | Sirius Systems | s-net | Cisco IOS XE Release 3.1S | |
| SNP | TCP/UDP | 109 | Sitara Networks Protocol | snp | Cisco IOS XE Release 3.1S | |
| SNPP | TCP/UDP | 444 | Simple Network Paging Protocol | snpp | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| SNTP-Heartbeat | TCP/UDP | 580 | SNTP HEARTBEAT | sntp-heartbeat | Cisco IOS XE Release 3.1S | |
| SoftPC | TCP/UDP | 215 | Insignia Solutions | softpc | Cisco IOS XE Release 3.1S | |
| Sonar | TCP/UDP | 572 | Sonar | sonar | Cisco IOS XE Release 3.1S | |
| SPMP | TCP/UDP | 656 | spmp | spmp | Cisco IOS XE Release 3.1S | |
| Sprite-RPC | TCP/UDP | 90 | Sprite RPC Protocol | sprite-rpc | Cisco IOS XE Release 3.1S | |
| SPS | TCP/UDP | 130 | Secure Packet Shield | sps | Cisco IOS XE Release 3.1S | |
| SPSC | TCP/UDP | 478 | spsc | spsc | Cisco IOS XE Release 3.1S | |
| SQL*Net | TCP/UDP | 66 | Oracle SQL*NET | sql*net | Cisco IOS XE Release 3.1S | |
| SQLExec | TCP/UDP | 9088 | SQL Informix | sqlexec | 12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.1S | |
| SQL-Net | TCP/UDP | 150 | SQL-NET | sql-net | Cisco IOS XE Release 3.1S | |
| | | | | | | |
| | SQLServ | TCP/UDP | 118 | SQL Services | sqlserv | Cisco IOS XE Release 3.1S |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| SQLServer | TCP/UDP | 1433 | Microsoft SQL Server | sqlserver | Cisco IOS XE Release 3.1S | |
| SRC | TCP/UDP | 200 | IBM System Resource Controller | src | Cisco IOS XE Release 3.1S | |
| SRMP | TCP/UDP | 193 | Spider Remote Monitoring Protocol | srmp | Cisco IOS XE Release 3.1S | |
| SRP | TCP/UDP | 119 | SpectraLink Radio Protocol | srp | Cisco IOS XE Release 3.1S | |
| SRSSend | TCP/UDP | 362 | srssend | srssend | Cisco IOS XE Release 3.1S | |
| SS7NS | TCP/UDP | 477 | ss7ns | ss7ns | Cisco IOS XE Release 3.1S | |
| SSCOPMCE | TCP/UDP | 128 | SSCOPMCE | sscopmce | Cisco IOS XE Release 3.1S | |
| SSH | TCP/UDP | 22 | Secure Shell Protocol | ssh | Cisco IOS XE Release 3.1S | |
| Sshell | TCP/UDP | 614 | SSLshell | sshell | Cisco IOS XE Release 3.1S | |
| SST | TCP/UDP | 266 | SCSI on ST | sst | Cisco IOS XE Release 3.1S | |
| ST | TCP/UDP | 5 | Stream | st | Cisco IOS XE Release 3.1S | |
| StatSRV | TCP/UDP | 133 | Statistics Service | statsrv | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| STMF | TCP/UDP | 501 | stmf | stmf | Cisco IOS XE Release 3.1S | |
| STP | TCP/UDP | 118 | Schedule Transfer Protocol | stp | Cisco IOS XE Release 3.1S | |
| StreetTalk | TCP/UDP | 566 | Streettalk | streettalk | Cisco IOS XE Release 3.1S | |
| Stun-NAT | TCP/UDP | 3478 | STUN | stun-nat | Cisco IOS XE Release 3.1S | |
| STX | TCP/UDP | 527 | Stock IXChange | stx | Cisco IOS XE Release 3.1S | |
| Submission | TCP/UDP | 587 | Submission | submission | Cisco IOS XE Release 3.1S | |
| | Subntbcst_TFTP | TCP/UDP | 247 | subntbcst_tftp | subntbcst_tftp | Cisco IOS XE Release 3.1S |
| SU-MIT-TG | TCP/UDP | 89 | SU/MIT Telnet Gateway | su-mit-tg | Cisco IOS XE Release 3.1S | |
| Sun-DR | TCP/UDP | 665 | sun-dr | sun-dr | Cisco IOS XE Release 3.1S | |
| Sun-ND | TCP/UDP | 77 | SUN ND PROTOCOL-Temporary | sun-nd | Cisco IOS XE Release 3.1S | |
| SupDup | TCP/UDP | 95 | SUPDUP | supdup | Cisco IOS XE Release 3.1S | |
| Surf | TCP/UDP | 1010 | Surf | surf | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Sur-Meas | TCP/UDP | 243 | Survey Measurement | sur-meas | Cisco IOS XE Release 3.1S | |
| Svrloc | TCP/UDP | 427 | Server Location | svrloc | Cisco IOS XE Release 3.1S | |
| Swift-RVF | TCP/UDP | 97 | Swift Remote Virtural File Protocol | swift-rvf | Cisco IOS XE Release 3.1S | |
| Swipe | TCP/UDP | 53 | IP with Encryption | swipe | Cisco IOS XE Release 3.1S | |
| Synoptics-Trap | TCP/UDP | 412 | Trap Convention Port | synoptics-trap | Cisco IOS XE Release 3.1S | |
| Synotics-Broker | TCP/UDP | 392 | SynOptics Port Broker Port | synotics-broker | Cisco IOS XE Release 3.1S | |
| Synotics-Relay | TCP/UDP | 391 | SynOptics SNMP Relay Port | synotics-relay | Cisco IOS XE Release 3.1S | |
| Systat | TCP/UDP | 11 | Active Users | systat | 12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S | |
| TACACS | TCP/UDP | 49, 65 | Terminal Access Controller Access Control System | tacacs | 12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S | |
| TAC News | TCP/UDP | 98 | TAC News | tacnews | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Talk | TCP/UDP | 517 | Talk | talk | Cisco IOS XE Release 3.1S | |
| | | TCF | TCP/UDP | 87 | TCF | tcf | Cisco IOS XE Release 3.1S |
| TD-Replica | TCP/UDP | 268 | Tobit David Replica | td-replica | Cisco IOS XE Release 3.1S | |
| TD-Service | TCP/UDP | 267 | Tobit David Service Layer | td-service | Cisco IOS XE Release 3.1S | |
| Teedtap | TCP/UDP | 559 | Teedtap | teedtap | Cisco IOS XE Release 3.1S | |
| Tell | TCP/UDP | 754 | Send | tell | Cisco IOS XE Release 3.1S | |
| Telnet | TCP/UDP | 23 | Telnet | telnet | Cisco IOS XE Release 3.1S | |
| Tempo | TCP/UDP | 526 | newdate | tempo | Cisco IOS XE Release 3.1S | |
| Tenfold | TCP/UDP | 658 | Tenfold | tenfold | Cisco IOS XE Release 3.1S | |
| Texar | TCP/UDP | 333 | Texar Security Port | texar | Cisco IOS XE Release 3.1S | |
| TICF-1 | TCP/UDP | 492 | Transport Independent Convergence for FNA | ticf-1 | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| TICF-2 | TCP/UDP | 493 | Transport Independent Convergence for FNA | ticf-2 | Cisco IOS XE Release 3.1S | |
| Timbuktu | TCP/UDP | 407 | Timbuktu | timbuktu | Cisco IOS XE Release 3.1S | |
| Time | TCP/UDP | 37 | Time | time | 12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S | |
| Timed | TCP/UDP | 525 | Timeserver | timed | Cisco IOS XE Release 3.1S | |
| TINC | TCP/UDP | 655 | tinc | tinc | Cisco IOS XE Release 3.1S | |
| TLISRV | TCP/UDP | 1527 | Oracle | tlisrv | Cisco IOS XE Release 3.1S | |
| TLSP | TCP/UDP | 56 | Transport Layer Security Protocol | tlsp | Cisco IOS XE Release 3.1S | |
| TNETOS | TCP/UDP | 377 | NEC Corporation | tnETOS | Cisco IOS XE Release 3.1S | |
| TNS-CML | TCP/UDP | 590 | tns-cml | tns-cml | Cisco IOS XE Release 3.1S | |
| | | | | | | |
| TN-TL-FD1 | TCP/UDP | 476 | tn-tl-fd1 | tn-tl-fd1 | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| TP++ | TCP/UDP | 39 | TP++ Transport Protocol | tp++ | Cisco IOS XE Release 3.1S | |
| TPIP | TCP/UDP | 594 | tpip | tpip | Cisco IOS XE Release 3.1S | |
| Trunk-1 | TCP/UDP | 23 | Trunk-1 | trunk-1 | Cisco IOS XE Release 3.1S | |
| Trunk-2 | TCP/UDP | 24 | Trunk-2 | trunk-2 | Cisco IOS XE Release 3.1S | |
| TServer | TCP/UDP | 450 | Computer Supported Telecomunication Applications | tserver | Cisco IOS XE Release 3.1S | |
| TTP | TCP/UDP | 84 | TTP | ttp | Cisco IOS XE Release 3.1S | |
| UAAC | TCP/UDP | 145 | UAAC Protocol | uaac | Cisco IOS XE Release 3.1S | |
| UARPs | TCP/UDP | 219 | Unisys ARPs | uarps | Cisco IOS XE Release 3.1S | |
| UDPLite | TCP/UDP | 136 | UDPLite | udplite | Cisco IOS XE Release 3.1S | |
| UIS | TCP/UDP | 390 | uis | uis | Cisco IOS XE Release 3.1S | |
| uLISTProc | TCP/UDP | 372 | List Processor | ulistproc | Cisco IOS XE Release 3.1S | |
| ULP | TCP/UDP | 522 | ulp | ulp | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| ULPNet | TCP/UDP | 483 | ulpnet | ulpnet | Cisco IOS XE Release 3.1S | |
| Unidata-LDM | TCP/UDP | 388 | Unidata LDM | unidata-ldm | Cisco IOS XE Release 3.1S | |
| Unify | TCP/UDP | 181 | Unify | unify | Cisco IOS XE Release 3.1S | |
| UPS | TCP/UDP | 401 | Uninterruptible Power Supply | ups | Cisco IOS XE Release 3.1S | |
| | URM | TCP/UDP | 606 | Cray Unified Resource Manager | urm | Cisco IOS XE Release 3.1S |
| | UTI | TCP/UDP | 120 | UTI | uti | Cisco IOS XE Release 3.1S |
| Utime | TCP/UDP | 519 | Unixtime | utime | Cisco IOS XE Release 3.1S | |
| UTMPCD | TCP/UDP | 431 | utmpcd | utmpcd | Cisco IOS XE Release 3.1S | |
| UTMPSD | TCP/UDP | 430 | utmpsd | utmpsd | Cisco IOS XE Release 3.1S | |
| UUCP | TCP/UDP | 540 | uucpd | uucp | Cisco IOS XE Release 3.1S | |
| UUCP-Path | TCP/UDP | 117 | UUCP Path Service | uucp-path | Cisco IOS XE Release 3.1S | |
| UUCP-rLogin | TCP/UDP | 541 | uucp-rlogin | uucp-rlogin | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| UUIDGEN | TCP/UDP | 697 | UUIDGEN | uuidgen | Cisco IOS XE Release 3.1S | |
| VACDSM-App | TCP/UDP | 671 | VACDSM-APP | vacdsm-app | Cisco IOS XE Release 3.1S | |
| VACDSM-SWS | TCP/UDP | 670 | VACDSM-SWS | vacdsm-sws | Cisco IOS XE Release 3.1S | |
| VATP | TCP/UDP | 690 | Velazquez Application Transfer Protocol | vatp | Cisco IOS XE Release 3.1S | |
| VEMMI | TCP/UDP | 575 | vemmi | vemmi | Cisco IOS XE Release 3.1S | |
| VID | TCP/UDP | 769 | vid | vid | Cisco IOS XE Release 3.1S | |
| Videotex | TCP/UDP | 516 | videotex | videotex | Cisco IOS XE Release 3.1S | |
| VISA | TCP/UDP | 70 | VISA Protocol | visa | Cisco IOS XE Release 3.1S | |
| VNC | TCP/UDP | 5800, 5900, 5901 | Virtual Network Computing | vnc | 12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 | |
| VMNet | TCP/UDP | 175 | vmnet | vmnet | Cisco IOS XE Release 3.1S | |
| VMPWSCS | TCP/UDP | 214 | vmpwscs | vmpwscs | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| VMTP | TCP/UDP | 81 | VMTP | vmtp | Cisco IOS XE Release 3.1S | |
| | VNAS | TCP/UDP | 577 | vnas | vnas | Cisco IOS XE Release 3.1S |
| VPP | TCP/UDP | 677 | Virtual Presence Protocol | vpp | Cisco IOS XE Release 3.1S | |
| VPPS-QUA | TCP/UDP | 672 | vpps-qua | vpps-qua | Cisco IOS XE Release 3.1S | |
| VPPS-VIA | TCP/UDP | 676 | vpps-via | vpps-via | Cisco IOS XE Release 3.1S | |
| VRRP | TCP/UDP | 112 | Virtual Router Redundancy Protocol | vrrp | Cisco IOS XE Release 3.1S | |
| VSINet | TCP/UDP | 996 | vsinet | vsinet | Cisco IOS XE Release 3.1S | |
| VSLMP | TCP/UDP | 312 | vslmp | vslmp | Cisco IOS XE Release 3.1S | |
| WAP-Push | TCP/UDP | 2948 | WAP PUSH | wap-push | Cisco IOS XE Release 3.1S | |
| WAP-Push-HTTP | TCP/UDP | 4035 | WAP Push OTA-HTTP port | wap-push-http | Cisco IOS XE Release 3.1S | |
| WAP-Push-HTTPS | TCP/UDP | 4036 | WAP Push OTA-HTTP secure | wap-push-https | Cisco IOS XE Release 3.1S | |
| WAP-Pushsecure | TCP/UDP | 2949 | WAP PUSH SECURE | wap-pushsecure | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| WAP-VACL-S | TCP/UDP | 9207 | WAP vCal Secure | wap-vcal-s | Cisco IOS XE Release 3.1S | |
| WAP-VCAL | TCP/UDP | 9205 | WAP vCal | wap-vcal | Cisco IOS XE Release 3.1S | |
| WAP-VCARD | TCP/UDP | 9204 | WAP vCard | wap-vcard | Cisco IOS XE Release 3.1S | |
| WAP-VCARD-S | TCP/UDP | 9206 | WAP vCard Secure | wap-vcard-s | Cisco IOS XE Release 3.1S | |
| WAP-WSP | TCP/UDP | 9200 | WAP connectionless session service | wap-wsp | Cisco IOS XE Release 3.1S | |
| WAP-WSP-S | TCP/UDP | 9202 | WAP secure connectionless session service | wap-wsp-s | Cisco IOS XE Release 3.1S | |
| WAP-WSP-WTP | TCP/UDP | 9201 | WAP session service | wap-wsp-wtp | Cisco IOS XE Release 3.1S | |
| WAP-WSP-WTP-S | TCP/UDP | 9203 | WAP secure session service | wap-wsp-wtp-s | Cisco IOS XE Release 3.1S | |
| | WB-Expak | TCP/UDP | 79 | WIDEBAND EXPAK | wb-expak | Cisco IOS XE Release 3.1S |
| WB-Mon | TCP/UDP | 78 | WIDEBAND Monitoring | wb-mon | Cisco IOS XE Release 3.1S | |
| Webster | TCP/UDP | 765 | Webster | webster | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Webex Meeting | TCP | Heuristic | Webex Meeting | webex-meeting | Cisco IOS XE Release 3.4S | |
| WhoAmI | TCP/UDP | 565 | whoami | whoami | Cisco IOS XE Release 3.1S | |
| Whois++ | TCP/UDP | 63 | whois++ Service | whois++ | 12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S | |
| Windows Update | TCP | 80, 443, Heuristic | Windows Update | windows-update | Cisco IOS XE Release 3.4S | |
| WorldFusion | TCP/UDP | 2595 | World Fusion | worldfusion | Cisco IOS XE Release 3.1S | |
| WPGS | TCP/UDP | 780 | wpgs | wpgs | Cisco IOS XE Release 3.1S | |
| WSN | TCP/UDP | 74 | Wang Span Network | wsn | Cisco IOS XE Release 3.1S | |
| XAct-Backup | TCP/UDP | 911 | Xact-backup | xact-backup | Cisco IOS XE Release 3.1S | |
| X-Bone-CTL | TCP/UDP | 265 | Xbone CTL | x-bone-ctl | Cisco IOS XE Release 3.1S | |
| XDMCP | TCP/UDP | 177 | X Display Manager Control Protocol | xdmcp | 12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| XDTP | TCP/UDP | 3088 | eXtensible Data Transfer Protocol | xdtp | Cisco IOS XE Release 3.1S | |
| XFER | TCP/UDP | 82 | XFER Utility | xfer | Cisco IOS XE Release 3.1S | |
| XNET | TCP/UDP | 15 | Cross Net Debugger | xnet | Cisco IOS XE Release 3.1S | |
| XNS-Auth | TCP/UDP | 56 | XNS Authentication | xns-auth | Cisco IOS XE Release 3.1S | |
| XNS-CH | TCP/UDP | 54 | XNS Clearinghouse | xns-ch | Cisco IOS XE Release 3.1S | |
| | | | | | | |
| | XNS-Courier | TCP/UDP | 165 | Xerox | xns-courier | Cisco IOS XE Release 3.1S |
| XNS-IDP | TCP/UDP | 22 | XEROX NS IDP | xns-idp | Cisco IOS XE Release 3.1S | |
| XNS-Mail | TCP/UDP | 58 | XNS mail | xns-mail | Cisco IOS XE Release 3.1S | |
| XNS-Time | TCP/UDP | 52 | XNS Time Protocol | xns-time | Cisco IOS XE Release 3.1S | |
| XTP | TCP/UDP | 36 | XTP | xtp | Cisco IOS XE Release 3.1S | |
| XVTTP | TCP/UDP | 508 | xvttp | xvttp | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| XYPlex-Mux | TCP/UDP | 173 | Xyplex | xyplex-mux | Cisco IOS XE Release 3.1S | |
| X Windows | TCP | 6000-6003 | X Window System | xwindows | 12.0(5)XE2 12.1(1)E 12.1(5)T 12.2(18)ZYA1 Cisco IOS XE Release 2.3 Cisco IOS XE Release 3.1S | |
| z39.50 | TCP/UDP | 210 | ANSI Z39.50 | z39.50 | Cisco IOS XE Release 3.1S | |
| Zannet | TCP/UDP | 317 | Zannet | zannet | Cisco IOS XE Release 3.1S | |
| ZServ | TCP/UDP | 346 | Zebra server | zserv | Cisco IOS XE Release 3.1S | |
| AN | IP | 107 | Active Networks | an | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| | | | | | | |
| AOL-Protocol[8] | | TCP | 5190 | America OnLine Protocol | aol-protocol | Cisco IOS XE Release 3.3S |
| ARGUS | | IP | 13 | ARGUS | argus | Cisco IOS XE Release 3.1S |
| ARIS | | IP | 104 | ARIS | aris | Cisco IOS XE Release 3.1S |
| AX25 | | IP | 93 | AX.25 Frames | ax25 | Cisco IOS XE Release 3.1S |
| BBNR RCC Mon | | IP | 10 | BBN RCC Monitoring | bbnrccmon | Cisco IOS XE Release 3.1S |
| BLIZWOW | | TCp, UDP | 3724 | World of Warcraft Gaming Protocol | blizwow | Cisco IOS XE Release 3.3S |
| BNA | | IP | 49 | BNA | bna | Cisco IOS XE Release 3.1S |
| | BR-SAT-Mon | IP | 76 | Backroom SATNET Monitoring | br-sat-mon | Cisco IOS XE Release 3.1S |
| | CBT | IP | 7 | CBT | cbt | Cisco IOS XE Release 3.1S |
| CFTP | IP | 62 | CFTP | cftp | Cisco IOS XE Release 3.1S | |
| Choas | IP | 16 | Chaos | chaos | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Compaq-Peer | IP | 110 | Compaq Peer Protocol | compaq-peer | Cisco IOS XE Release 3.1S | |
| CPHB | IP | 73 | Computer Protocol Heart Beat | cphb | Cisco IOS XE Release 3.1S | |
| CPNX | IP | 72 | Computer Protocol Network Executive | cpnx | Cisco IOS XE Release 3.1S | |
| CRTP | IP | 126 | Combat Radio Transport Protocol | crtp | Cisco IOS XE Release 3.1S | |
| CRUDP | IP | 127 | Combat Radio User Datagram | crudp | Cisco IOS XE Release 3.1S | |
| DCCP | IP | 33 | Datagram Congestion Control Protocol | dccp | Cisco IOS XE Release 3.1S | |
| DCN-Meas | IP | 19 | DCN Measurement Subsystems | dcn-meas | Cisco IOS XE Release 3.1S | |
| DDP | IP | 37 | Datagram Delivery Protocol | ddp | Cisco IOS XE Release 3.1S | |
| DDX | IP | 116 | D-II Data Exchange | ddx | Cisco IOS XE Release 3.1S | |
| DGP | IP | 86 | Dissimilar Gateway Protocol | dgp | Cisco IOS XE Release 3.1S | |
| DSR | IP | 48 | Dynamic Source Routing Protocol | dsr | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| EGP | IP | 8 | Exterior Gateway Protocol | egp | Cisco IOS XE Release 3.1S | |
| EIGRP | IP | 88 | Enhanced Interior Gateway Routing Protocol | eigrp | Cisco IOS XE Release 3.1S | |
| EMCON | IP | 14 | EMCON | emcon | Cisco IOS XE Release 3.1S | |
| Encap | IP | 98 | Encapsulation Header | encap | 15.1(3)T | |
| EtherIP | IP | 97 | Ethernet-within-IP Encapsulation | etherip | Cisco IOS XE Release 3.1S | |
| | FC | IP | 133 | Fibre Channel | fc | Cisco IOS XE Release 3.1S |
| FIRE | IP | 125 | FIRE | fire | Cisco IOS XE Release 3.1S | |
| GGP | IP | 3 | Gateway-to-Gateway | ggp | Cisco IOS XE Release 3.1S | |
| GMTP | IP | 100 | GMTP | gmtp | Cisco IOS XE Release 3.1S | |
| GRE | IP | 47 | General Routing Encapsulation | gre | Cisco IOS XE Release 3.1S | |
| HIP | IP | 139 | Host Identity Protocol | hip | Cisco IOS XE Release 3.1S | |
| HMP | IP | 20 | Host Monitoring | hmp | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| HopOpt | IP | 0 | IPv6 Hop-by-Hop Option | hopopt | Cisco IOS XE Release 3.1S | |
| ICQ | TCP | 80, Heuristic | I seek you Instant Messaging Protocol | icq | Cisco IOS XE Release 3.3S | |
| IATP | IP | 117 | Interactive Agent Transfer Protocol | iatp | Cisco IOS XE Release 3.1S | |
| ICMP | IP | 1 | Internet Control Message | icmp | Cisco IOS XE Release 3.1S | |
| IDPR | IP | 35 | Inter-Domain Policy Routing Protocol | idpr | Cisco IOS XE Release 3.1S | |
| IDPR-CMTP | IP | 38 | IDPR Control Message Transport Protocol | idpr-cmtp | Cisco IOS XE Release 3.1S | |
| IDRP | IP | 45 | Inter-Domain Routing Protocol | idrp | Cisco IOS XE Release 3.1S | |
| IFMP | IP | 101 | Ipsilon Flow Management Protocol | ifmp | Cisco IOS XE Release 3.1S | |
| IGRP | IP | 9 | Cisco interior gateway | igrp | Cisco IOS XE Release 3.1S | |
| IL | IP | 40 | IL Transport Protocol | il | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| I-NLSP | IP | 52 | Integrated Net Layer Security TUBA | i-nlsp | Cisco IOS XE Release 3.1S | |
| IMPCOMP | IP | 108 | IP Payload Compression Protocol | ipcomp | Cisco IOS XE Release 3.1S | |
| | IPCU | IP | 71 | Internet Packet Core Utility | ipcv | Cisco IOS XE Release 3.1S |
| IPinIP | IP | 4 | IP in IP | ipinip | Cisco IOS XE Release 3.1S | |
| IPIP | IP | 94 | IP-within-IP Encapsulation Protocol | ipip | Cisco IOS XE Release 3.1S | |
| IPLT | IP | 129 | IPLT | iplt | Cisco IOS XE Release 3.1S | |
| IPPC | IP | 67 | Internet Pluribus Packet Core | ippc | Cisco IOS XE Release 3.1S | |
| IPv6-Frag | IP | 44 | Fragment Header for IPv6 | ipv6-frag | Cisco IOS XE Release 3.1S | |
| IPv6-ICMP | IP | 58 | ICMP for IPv6 | ipv6-icmp | Cisco IOS XE Release 3.1S | |
| IPv6INIP | IP | 41 | Ipv6 encapsulated | ipv6inip | Cisco IOS XE Release 3.1S | |
| IPv6-NONXT | IP | 59 | No Next Header for IPv6 | ipv6-nonxt | Cisco IOS XE Release 3.1S | |
| IPv6-Opts | IP | 60 | Destination Options for IPv6 | ipv6-opts | Cisco IOS XE Release 3.1S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| IPv6-Route | IP | 43 | Routing Header for IPv6 | ipv6-route | Cisco IOS XE Release 3.1S | |
| IRTP | IP | 28 | Internet Reliable Transaction | irtp | Cisco IOS XE Release 3.1S | |
| ISIS | IP | 124 | ISIS over IPv4 | isis | Cisco IOS XE Release 3.1S | |
| ISO-TP4 | IP | 29 | ISO Transport Protocol Class 4 | iso-tp4 | Cisco IOS XE Release 3.1S | |
| IXP-in-IP | IP | 111 | IPX in IP | ixp-in-ip | Cisco IOS XE Release 3.1S | |
| LARP | IP | 91 | Locus Address Resolution Protocol | larp | Cisco IOS XE Release 3.1S | |
| Leaf-1 | IP | 25 | Leaf-1 | leaf-1 | Cisco IOS XE Release 3.1S | |
| 6to4 IPv6 Tunneled | L3 Protocol | -- | 6to4 IPv6 Tunneled | 6to4 IPv6 Tunneled | Cisco IOS XE Release 3.2S | |
| | AYIYA IPv6 Tunneled | UDP | 5072 | IPv6 Tunneled based on AYIYA traffic | AYIYA IPv6 Tunneled | Cisco IOS XE Release 3.2S |
| | BabelGum | TCP, UDP | 80 + Heuristic | BabelGum | BabelGum | Cisco IOS XE Release 3.2S |
| Baidu Movie | TCP, UDP | 80 + Heuristic | Baidu Movie | Baidu Movie | Cisco IOS XE Release 3.2S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| DHCP | UDP | 67,68 | Dynamic Host Configuration Protocol | dhcp | Cisco IOS XE Release 3.2S | |
| DHT | UDP | Heuristic | Distributed sloppy Hash Table Protocol | DHT | Cisco IOS XE Release 3.2S | |
| Filetopia | TCP | Heuristic | Filetopia P2P file sharing | filetopia | Cisco IOS XE Release 3.2S | |
| Fring-VoIP | UDP | Heuristic | Fring VoIP | fring-voip | Cisco IOS XE Release 3.3S | |
| GoogleEarth | TCP | 80 + Heuristic | GoogleEarth | GoogleEarth | Cisco IOS XE Release 3.2S | |
| Guruguru | TCP | Heuristic | Guruguru | guruguru | Cisco IOS XE Release 3.2S | |
| IMAP | TCP | 143,220 | Internet Mail Access Protocol | imap | Cisco IOS XE Release 3.2S | |
| IRC | TCP | 80 + Heuristic | IRC | IRC | Cisco IOS XE Release 3.2S | |
| ISATAP IPv6 Tunneled | L3 Protocol | | Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) IPv6 Tunneled | ISATAP IPv6 Tunneled | Cisco IOS XE Release 3.2S | |
| iTunes | TCP | 80 + Heuristic | iTunes | iTunes | Cisco IOS XE Release 3.2S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Kuro | TCP | Heuristic | Kuro | kuro | Cisco IOS XE Release 3.3S | |
| Manolito | TCP, UDP | TCP - Heuristic port, UDP - 41170 | Manolito P2P music sharing protocol | manolito | Cisco IOS XE Release 3.2S | |
| MapleStory | TCP | Heuristic | Maple Story Gaming Protocol | MapleStory | Cisco IOS XE Release 3.2S | |
| SIP | TCP, UDP | TCP/UDP - 5060 + Heuristic | Session Initiation Protocol | sip | Cisco IOS XE Release 3.2S | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | MGCP | TCP, UDP | UDP 2427/2727 - TCP 2427/2428/2727 + Heuristic | Media Gateway Control Protocol | MGCP | 12.2(18)ZYA1 12.3(7)T Cisco IOS XE Release 3.2S |
| Microsoft-DS | TCP, UDP | 445 | Microsoft-ds | microsoftds | 12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.3S | |
| MSN Messenger | TCP | 1080,1863, 80, Hueristic | MSN Messenger | msn-messenger | 12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.3S | |
| MyJabber File Transfer | TCP | Heuristic | MyJabber File Transfer | MyJabber File Transfer | Cisco IOS XE Release 3.2S | |
| Napster | TCP | 80 + Heuristic | Napster | napster | Cisco IOS XE Release 3.2S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Netshow | TCP | 1755 + Heuristic | Netshow | netshow | 12.0(5)XE2<br>12.1(1)E<br>12.1(5)T<br>12.2(18)ZYA1 | |
| NNTP | TCP | TCP - 119 + Heuristic, UDP -119 | Network News Transfer Protocol | NNTP | Cisco IOS XE Release 3.2S | |
| NTP | UDP | 123 | Network Time Protocol | NTP | Cisco IOS XE Release 3.2S | |
| Pando | TCP,UDP | TCP - 80 + Heuristic, UDP - Heuristic | Pando | Pando | Cisco IOS XE Release 3.2S | |
| POCO | TCP, UDP | Heuristic | POCO File-Sharing Application | POCO | Cisco IOS XE Release 3.2S | |
| POP3 | TCP | 110, Heuristic | POP3 | POP3 | Cisco IOS XE Release 3.2S | |
| PPTP | TCP | 1723 | Point-to-Point Tunneling Protocol | pptp | Cisco IOS XE Release 3.2S | |
| RADIUS | UDP | 1812, 1813 | Remote Authentication Dial In User Service protocol | radius | Cisco IOS XE Release 3.3S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| | | | | | | |
| | SCCP/Skinny | TCP | 2000-2002 | Skinny Call Control Protocol | skinny | Cisco IOS XE Release 3.3S |
| | Soribada | TCP | TCP - 80 + Heuristic, UDP - Heuristic | Soribada, Korean P2P music sharing Protocol | soribada | Cisco IOS XE Release 3.2S |
| | Soulseek | TCP | Heuristic | SoulSeek internet download manager Protocol | soulseek | Cisco IOS XE Release 3.3S |
| | TeamSpeak | UDP | Heuristic | TeamSpeak internet based voice-conferencing Protocol | TeamSpeak | Cisco IOS XE Release 3.2S |
| TelePresence | TCP/UDP | Dynamically assigned | Cisco TelePresence System | telepresence-media | 12.2(18)ZYA2 | |
| Telepresence-control | TCP,UDP | TCP- 5060, UDP- Heuristic | Telepresence-control | telepresence-control | Cisco IOS XE Release 3.2S | |
| Teredo IPv6 Tunneled | TCP,UDP | TCP- Heuristic, UDP - 3544 + Heuristic | Teredo IPv6 Tunneled | teredo-ipv6-tunneled | Cisco IOS XE Release 3.2S | |
| TFTP | UDP | 69 | Trivial File Transfer Protocol | tftp | Cisco IOS XE Release 3.2S | |
| TomatoPang | TCP | Heuristic | TomatoPang P2P Sharing Protocol | TomatoPang | Cisco IOS XE Release 3.2S | |
| Tunnel-HTTP | TCP | 80 + Heuristic | HTTP Tunneling | tunnel-http | Cisco IOS XE Release 3.2S | |

| Category | Protocol | Type | WKP/IP Protocol | Description | Syntax | Cisco IOS XE Release |
|---|---|---|---|---|---|---|
| Ventrilo | TCP, UDP | Heuristic | Ventrilo VoIP Protocol | Ventrilo | Cisco IOS XE Release 3.2S | |
| Waste | TCP/UDP | Heuristic | Waste | waste | Cisco IOS XE Release 3.3S | |
| WebThunder | TCP, UDP | TCP-80, UDP-Heuristic | WebThunder Peer-to-Peer File Sharing | WebThunder | Cisco IOS XE Release 3.2S | |
| Yahoo-Messenger | TCP | TCP-5050/1080/1190 /Heuristic | Yahoo Messenger | yahoo-messenger | 12.2(18)ZYA 12.2(18)ZYA1 Cisco IOS XE Release 3.3S | |
| Yahoo-Messenger-VoIP | TCP/UDP | Heuristic | Yahoo Messenger VoIP | yahoo-voip-messenger | Cisco IOS XE Release 3.3S | |
| Yahoo VoIP over SIP | TCP/UDP | 5060/Heuristic | Yahoo VoIP over SIP | yahoo-voip-over-sip | Cisco IOS XE Release 3.4S | |
| | | | | | | |

1 For Release 12.2(18)ZYA and Cisco IOS XE Release 2.5 Cisco supports Exchange 03 and 07 only. MS client access is recognized, but web client access is not recognized.

2 In Release 12.3(4)T, the NBAR Extended Inspection for HTTP Traffic feature was introduced. This feature allows NBAR to scan TCP ports that are not well known and to identify HTTP traffic that is traversing these ports. For Cisco IOS XE Release 2.1, classification of HTTP traffic by URL or hostname is not supported. Cisco IOS XE Release 2.5 supports classification of HTTP traffic by URL or hostname.

3 Skype was introduced in Cisco IOS Release 12.4(4)T. As a result of this introduction, Skype is native in (included with) the Cisco IOS software and uses the NBAR infrastructure new to Cisco IOS Release 12.4(4)T. Cisco software supports Skype 1.0, 2.5, and 3.0. For Cisco IOS XE Release 2.1, Skype is supported in the TCP type only. Note that certain hardware platforms do not support Skype. For instance, Skype is not supported on the Catalyst 6500 series switch that is equipped with a Supervisor/PISA engine. Cisco IOS XE Release 2.5 supports Skype in the TCP and UDP type.

4 For Release 12.2(18)ZYA, access to YouTube via HTTP only is recognized.

5 BitTorrent classifies only unencrypted traffic.

6 eDonkey classifies only unencrypted traffic.

7 For Release 12.2(18)ZYA, only SIP and Skinny telephone connections (cisco-phone traffic connections) are recognized. H.323 telephone connections are not recognized.

8 AOL-Protocol classifies traffic shared between ICQ and AOL clients.

### Custom Protocols Created with the ip nbar custom Command

The *variable-field-name* argumentis used in conjunction with the **variable***field-namefield-length* options that are entered when you create a custom protocol using the **ipnbarcustom**command. The variable option allows NBAR to match traffic on the basis of a specific value of a custom protocol. For instance, if **ipnbarcustomftdd125variablescid2tcprange50015005** is entered to create a custom protocol, and then a

class map using the**matchprotocolftddscid804**is created, the created class map will match all traffic that has the value “804” at byte 125 entering or leaving TCP ports 5001 to 5000.

Up to 24 variable values per custom protocol can be expressed in class maps. For instance, in the following configuration, 4 variables are used and 20 more “scid” values could be used.

```
Router(config)# ip nbar custom ftdd field scid 125 variable 1 tcp range 5001 5005
Router(config)# class-map active-craft
Router(config-cmap)# match protocol ftdd scid 0x15
Router(config-cmap)# match protocol ftdd scid 0x21
Router(config)# class-map passive-craft
Router(config-cmap)# match protocol ftdd scid 0x11
Router(config-cmap)# match protocol ftdd scid 0x22
```

**match protocol Command Restrictions (Catalyst 6500 Series Switches Only)**

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) on the basis of a protocol type or application. You can create as many traffic classes as needed.

Cisco IOS Release 12.2(18)ZY includes software intended for use on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine. For this release and platform, note the following restrictions for using policy maps and **matchprotocol** commands:

- A single traffic class can be configured to match a maximum of eight protocols or applications.
- Multiple traffic classes can be configured to match a cumulative maximum of 95 protocols or applications.

## Examples

The following example configures NBAR to match FTP traffic:

```
Router(config-cmap)# match protocol ftp
```

In the following example, custom protocol ftdd is created by using a variable. A class map matching this custom protocol based on the variable is also created. In this example, class map matchscidinftdd will match all traffic that has the value “804” at byte 125 entering or leaving TCP ports 5001 to 5005. The variable scid is 2 bytes in length:

```
Router(config)# ip nbar custom ftdd 125 variable scid 2 tcp range 5001 5005
Router(config)# class-map matchscidinftdd
Router(config-cmap)# match protocol ftdd scid 804
```

The following example show the command can also be written using hexadecimal values in the class map as follows:

```
Router(config)#
ip nbar custom ftdd 125 variable scid 2 tcp range 5001 5005
Router(config)# class-map matchscidinftdd
Router(config-cmap)# match protocol ftdd scid 0x324
```

In the following example, the **variable** keyword is used while you create a custom protocol, and class maps are configured to classify different values within the variable field into different traffic classes. Specifically, in the following example, variable scid values 0x15, 0x21, and 0x27 will be classified into class map active-craft, while scid values 0x11, 0x22, and 0x25 will be classified into class map passive-craft.

```
Router(config)# ip nbar custom ftdd field scid 125 variable 1 tcp range 5001 5005
Router(config)# class-map active-craft
Router(config-cmap)# match protocol ftdd scid 0x15
Router(config-cmap)# match protocol ftdd scid 0x21
Router(config-cmap)# match protocol ftdd scid 0x27
Router(config)# class-map passive-craft
Router(config-cmap)# match protocol ftdd scid 0x11
```

```
Router(config-cmap)# match protocol ftdd scid 0x22
Router(config-cmap)# match protocol ftdd scid 0x25
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **ip nbar custom** | Extends the capability of NBAR Protocol Discovery to classify and monitor additional static port applications, or allows NBAR to classify nonsupported static port traffic. |

# match protocol citrix

To configure network-based application recognition (NBAR) to match Citrix traffic, use the **matchprotocolcitrix** command in class-map configuration mode. To disable NBAR from matching Citrix traffic, use the **no** form of this command.

**match protocol citrix** [**app** *application-name-string*] [**ica-tag** *ica-tag-value*]

**no match protocol citrix** [**app** *application-name-string*] [**ica-tag** *ica-tag-value*]

## Syntax Description

| | |
|---|---|
| **app** | (Optional) Specifies matching of an application name string. |
| *application-name-string* | (Optional) Specifies the string to be used as the subprotocol parameter. |
| **ica-tag** | (Optional) Specifies tagging of Independent Computing Architecture (ICA) packets. |
| *ica-tag-value* | (Optional) Specifies the priority tag of ICA packets. Priority tag values can be in the range of 0 to 3. |

## Command Default

No match criteria are specified.

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(2)E | This command was introduced. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.1(13)E | This command was implemented on Catalyst 6000 family switches without FlexWAN modules. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(17a)SX1 | This command was integrated into Cisco IOS Release 12.2(17a)SX1. |
| 12.4(2)T | This command was modified to include the ica-tag keyword and the *ica-tag-value* argument. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

Entering the **matchprotocolcitrix** command without the **app** keyword establishes all Citrix traffic as successful match criteria.

Entering the**matchprotocolcitrix** command with the ica-tag keyword prioritizes Citrix ICA traffic. The priority tag values can be a number from 0 to 3, with 0 having the highest priority and 3 the lowest.

## Examples

The following example configures NBAR to match all Citrix traffic:

```
match protocol citrix
```

The following example configures NBAR to match Citrix traffic with the application name of packet1:

```
match protocol citrix app packet1
```

The following example configures NBAR to give Citrix ICA traffic a priority of 1:

```
match protocol citrix ica-tag-1
```

# match protocol fasttrack

To configure network-based application recognition (NBAR) to match FastTrack peer-to-peer traffic, use the **matchprotocolfasttrack** command in class-map configuration mode. To disable NBAR from matching FastTrack traffic, use the **no** form of this command.

**match protocol fasttrack file-transfer** *"regular-expression"*

**no match protocol fasttrack file-transfer** *"regular-expression"*

## Syntax Description

| | |
|---|---|
| **file-transfer** | Indicates that a regular expression will be used to identify specific FastTrack traffic. |
| " *regular-expression* " | Regular expression used to identify specific FastTrack traffic. For instance, entering "cisco" as the regular expression would classify the FastTrack traffic containing the string "cisco" as matches for the traffic policy.<br>To specify that all FastTrack traffic be identified by the traffic class, use "*" as the regular expression. |

## Command Default

NBAR is not configured to match FastTrack peer-to-peer traffic

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)E | This command was introduced. |
| 12.1(13)E | This command became available on Catalyst 6000 family switches without FlexWAN modules. |
| 12.2(2)T | This command was integrated into Cisco IOS Release 12.2(2)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(17a)SX1 | This command was integrated into Cisco IOS Release 12.2(17a)SX1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

To specify that all FastTrack traffic be identified by the traffic class, use "*" as the regular expression.

Applications that use FastTrack include KaZaA, Grokster, and Morpheus (although newer versions of Morpheus use Gnutella).

## Examples

The following example configures NBAR to match all FastTrack traffic:

```
match protocol fasttrack file-transfer “*”
```

In the following example, all FastTrack files that have the “.mpeg” extension will be classified into class map nbar:

```
class-map match-all nbar
 match protocol fasttrack file-transfer "*.mpeg"
```

The following example configures NBAR to match FastTrack traffic that contains the string “cisco”:

```
match protocol fasttrack file-transfer “*cisco*”
```

# match protocol gnutella

To configure network-based application recognition (NBAR) to match Gnutella peer-to-peer traffic, use the **matchprotocolgnutella** command in class-map configuration mode. To disable NBAR from matching Gnutella traffic, use the **no** form of this command.

**match protocol gnutella file-transfer** *"regular-expression"*

**no match protocol gnutella file-transfer** *"regular-expression"*

## Syntax Description

| | |
|---|---|
| **file-transfer** | Indicates that a regular expression will be used to identify specific Gnutella traffic. |
| " *regular-expression* " | The regular expression used to identify specific Gnutella traffic. For instance, entering "cisco" as the regular expression would classify the Gnutella traffic containing the string "cisco" as matches for the traffic policy.<br>To specify that all Gnutella traffic be identified by the traffic class, use "*" as the regular expression. |

## Command Default

No behavior or values are predefined.

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(12c)E | This command was introduced. |
| 12.1(13)E | This command became available on Catalyst 6000 family switches without FlexWAN modules. |
| 12.2(2)T | This command was integrated into Cisco IOS Release 12.2(2)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(17a)SX1 | This command was integrated into Cisco IOS Release 12.2(17a)SX1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

To specify that all Gnutella traffic be identified by the traffic class, use "*" as the regular expression.

Applications that use Gnutella include the following:

- BearShare
- Gnewtellium
- Gnucleus
- Gtk-Gnutella
- JTella
- LimeWire
- Morpheus
- Mutella
- Phex
- Qtella
- Swapper
- XoloX
- XCache

## Examples

The following example configures NBAR to match all Gnutella traffic:

```
match protocol gnutella file-transfer “*”
```

In the following example, all Gnutella files that have the “.mpeg” extension will be classified into class map nbar:

```
class-map match-all nbar
 match protocol gnutella file-transfer "*.mpeg"
```

In the following example, only Gnutella traffic that contains the characters “cisco” is classified:

```
class-map match-all nbar
 match protocol gnutella file-transfer “*cisco*”
```

# match protocol http

To configure Network-Based Application Recognition (NBAR) to match HTTP traffic by URL, host, Multipurpose Internet Mail Extension (MIME) type, or fields in HTTP packet headers, use the **matchprotocolhttp** command in class-map configuration mode. To disable NBAR from matching HTTP traffic by URL, host, or MIME type, or fields in HTTP packet headers, use the **no** form of this command.

**match protocol http** [**url** *url-string*| **host** *hostname-string*| **mime** *MIME-type*| **c-header-field** *c-header-field-string*| **s-header-field** *s-header-field-string*]

**no match protocol http** [**url** *url-string*| **host** *hostname-string*| **mime** *MIME-type*| **c-header-field** *c-header-field-string*| **s-header-field** *s-header-field-string*]

**match protocol http** [**content-encoding** *content-encoding-name-string*| **from** *from-address-string*| **host** *hostname-string*| **location** *location-name-string*| **mime** *MIME-type*| **referer** *referer-address-string*| **server** *server-software-name-string*| **url** *url-string*| **user-agent** *user-agent-software-name-string*]

**no match protocol http** [**content-encoding** *content-encoding-name-string*| **from** *from-address-string*| **host** *hostname-string*| **location** *location-name-string*| **mime** *MIME-type*| **referer** *referer-address-string*| **server** *server-software-name-string*| **url** *url-string*| **user-agent** *user-agent-software-name-string*]

## Syntax Description

| | |
|---|---|
| **url** | (Optional) Specifies matching by a URL. |
| *url-string* | (Optional) User-specified URL of HTTP traffic to be matched. |
| **host** | (Optional) Specifies matching by a hostname. |
| *hostname-string* | (Optional) User-specified hostname to be matched. |
| **mime** | (Optional) Specifies matching by a MIME text string. |
| *MIME-type* | (Optional) User-specified MIME text string to be matched. |
| **c-header-field** | (Optional) Specifies matching by a string in the header field in HTTP client messages.<br>**Note** HTTP client messages are often called HTTP request messages. |
| c-header-field-string | (Optional) User-specified text string within the HTTP client message (HTTP request message) to be matched. |
| **s-header-field** | (Optional) Specifies matching by a string in the header field in the HTTP server messages<br>**Note** HTTP server messages are often called HTTP response messages. |

| | |
|---|---|
| s-header-field-string | (Optional) User-specified text within the HTTP server message (HTTP response message) to be matched. |
| Cisco IOS 15.1(2)T and Later Releases and Catalyst 6500 Series Switch Equipped with the Supervisor 32/PISA Engine | |
| **content-encoding** | (Optional) Specifies matching by the encoding mechanism used to package the entity body. |
| *content-encoding-name-string* | (Optional) User-specified content-encoding name. |
| **from** | (Optional) Specifies matching by the e-mail address of the person controlling the user agent. |
| *from-address-string* | (Optional) User-specified e-mail address. |
| **location** | (Optional) Specifies matching by the exact location of the resource from request. |
| *location-name-string* | (Optional) User-specified location of the resource. |
| **referer** | (Optional) Specifies matching by the address from which the resource request was obtained. |
| *referer-address-name-string* | (Optional) User-specified address of the referer resource. |
| **server** | (Optional) Specifies matching by the software used by the origin server handling the request. |
| *server-software-name-string* | (Optional) User-specified software name. |
| **user-agent** | (Optional) Specifies matching by the software used by the agent sending the request. |
| *user-agent-software-name-string* | (Optional) User-specified name of the software used by the agent sending the request. |

**Command Default** NBAR does not match HTTP traffic by URL, host, MIME type, or fields in HTTP packet headers.

**Command Modes** Class-map configuration (config-cmap)

**Command History**

| Release | Modification |
|---|---|
| 12.0(5)XE2 | This command was introduced. |

| Release | Modification |
|---|---|
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(2)E | This command was modified to include the *hostname-string* argument. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.1(13)E | This command became available on Catalyst 6000 family switches without FlexWAN modules. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(17a)SX1 | This command was integrated into Cisco IOS Release 12.2(17a)SX1. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T, and the NBAR Extended Inspection for HTTP Traffic feature was introduced. This feature allows NBAR to scan TCP ports that are not well known and to identify HTTP traffic traversing these ports. |
| 12.4(2)T | The command was integrated into Cisco IOS Release 12.4(2)T and was modified to include the **c-header-field***c-header-field-string* and **s-header-field***s-header-field-string* keywords and arguments. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(18)ZY2 | This command was integrated into Cisco IOS Release 12.2(18)ZY2, and support was provided for the Catalyst 6500 series switch that is equipped with the Supervisor 32/PISA engine.<br>**Note** For this Cisco IOS release and this platform, the **c-header-field***c-header-field-string* and **s-header-field***s-header-field-string* keywords and arguments are not available. To achieve the same functionality, use the individual keywords and arguments as shown in the syntax for the Catalyst 6500 series switch. |
| 15.1(2)T | This command was modified. Support for the **c-header-field***c-header-field-string* and **s-header-field***s-header-field-string* keywords and arguments was removed. The **content-encoding**, **from**, **location**, **referrer**, and **user-agent** keywords and respective arguments were added. |
| Cisco IOS XE Release 3.1S | This command was integrated into Cisco IOS XE Release 3.1S. |

## Usage Guidelines

Classification of HTTP Traffic by Host, URL, or MIME

In Cisco IOS Release 12.3(4)T, the NBAR Extended Inspection for HTTP Traffic feature was introduced. This feature allows NBAR to scan TCP ports that are not well-known and that identify HTTP traffic traversing these ports. This feature is enabled automatically when a service policy containing the **matchprotocolhttp** command is attached to an interface.

When matching by MIME type, the MIME type can contain any user-specified text string. See the following web page for the IANA-registered MIME types:

http://www.iana.org/assignments/media-types/

When matching by MIME type, NBAR matches a packet containing the MIME type and all subsequent packets until the next HTTP transaction.

When matching by host, NBAR performs a regular expression match on the host field contents inside the HTTP packet and classifies all packets from that host.

HTTP client request matching supports GET, PUT, HEAD, POST, DELETE, OPTIONS, CONNECT, and TRACE. When matching by URL, NBAR recognizes the HTTP packets containing the URL and then matches all packets that are part of the HTTP request. When specifying a URL for classification, include only the portion of the URL that follows the www.*hostname .domain* in the **match** statement. For example, for the URL www.cisco.com/latest/whatsnew.html, include only /latest/whatsnew.html with the **match** statement (for instance, **matchprotocolhttpurl/latest/whatsnew.html**).

**Note** For Cisco IOS Release 12.2(18)ZY2 (and later releases) on the Cisco Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA, up to 56 parameters or subclassifications per protocol per router can be specified with the **matchprotocolhttp** command. These parameters or subclassifications can be a combination of any of the available match choices, such as host matches, MIME matches, server matches, and URL matches. For other Cisco IOS releases and platforms, the maximum is 24 parameters or subclassifications per protocol per router.

To match the www.*anydomain* .com portion, use the hostname matching feature. The parameter specification strings can take the form of a regular expression with the following options.

| Option | Description |
|---|---|
| | Match any zero or more characters in this position. |
| | Match any one character in this position. |
| | Match one of a choice of characters. |
| (\|) | Match one of a choice of characters in a range. For example cisco.(gif \| jpg) matches either cisco.gif or cisco.jpg. |
| [ ] | Match any character in the range specified, or one of the special characters. For example, [0-9] is all of the digits. [*] is the "*" character and [[] is the "[" character. |

Classification of HTTP Header Fields

In Cisco IOS Release 12.3(11)T, NBAR introduced expanded ability for users to classify HTTP traffic using information in the HTTP Header Fields.

HTTP works using a client/server model: HTTP clients open connections by sending a request message to an HTTP server. The HTTP server then returns a response message to the HTTP client (this response message

is typically the resource requested in the request message from the HTTP client). After delivering the response, the HTTP server closes the connection and the transaction is complete.

HTTP header fields are used to provide information about HTTP request and response messages. HTTP has numerous header fields. For additional information on HTTP headers, see section 14 of RFC 2616: Hypertext Transfer Protocol--HTTP/1.1. This document can be read at the following URL:

http://www.w3.org/Protocols/rfc2616/rfc2616-sec14.html

For request messages (client to server), the following HTTP header fields can be identified by using NBAR:

- User-Agent
- Referer

For response messages (server to client), the following header fields can be identified by using NBAR:

- Server
- Location
- Content-Encoding
- Content-Base

**Note** Use of the Content-Base field has not been implemented by the HTTP community. (See RFC 2616 for details.) Therefore, the Content-Base field is not identified by NBAR on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine.

Within NBAR, the **matchprotocolhttpc-header-field** command is used to specify request messages (the “c” in the **c-header-field** portion of the command is for client). The **matchprotocolhttps-header-field** command is used to specify response messages (the “s” in the **s-header-field**portion of the command is for server).

It is important to note that combinations of URL, host, MIME type, and HTTP headers can be used during NBAR configuration. These combinations provide customers with more flexibility to classify specific HTTP traffic based on their network requirements.

**Note** For Cisco IOS Release 12.2(18)ZY2 and later releases on the Cisco Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA, and for Cisco IOS Release 15.1(2)T and later releases, the **c-header-field** and **s-header-field** keywords and associated arguments in the **matchprotocolhttp** command are not available.

## Examples

The following example classifies, within class map class1, HTTP packets based on any URL containing the string whatsnew/latest followed by zero or more characters:

```
class-map class1
 match protocol http url whatsnew/latest*
```

The following example classifies, within class map class2, packets based on any hostname containing the string cisco followed by zero or more characters:

```
class-map class2
 match protocol http host cisco*
```

The following example classifies, within class map class3, packets based on the JPEG MIME type:

```
class-map class3
 match protocol http mime “*jpeg”
```

In the following example, any response message that contains “ gzip” in the Content-Base (if available), Content-Encoding, Location, or Server header fields will be classified by NBAR. Typically, the term “gzip” would be found in the Content-Encoding header field of the response message.

```
class-map class4
 match protocol http s-header-field “gzip”
```

In the following example, HTTP header fields are combined with a URL to classify traffic. In this example, traffic with a User-Agent field of “CERN-LineMode/3.0” and a Server field of “CERN/3.0”, along with URL “www.cisco.com/routers”, will be classified using NBAR.

```
class-map match-all c-http
 match protocol http c-header-field “CERN-LineMode/3.0”
 match protocol http s-header-field “CERN/3.0”
 match protocol http url “www.cisco.com/routers”
```

## Examples

In the following two examples, the individual keywords and associated arguments are used to specify traffic (instead of the **c-header-field** and the **s-header-field** keywords).

In the first example, the**user-agent**, **referrer**, and **from** keywords are specified. In the second example, the server, location, content-encoding keywords are specified.

```
class-map match-all test1
 match protocol http user-agent Mozilla
 match protocol http referrer *10.0.10.50”
 match protocol http from *example.com”
class-map match-all test2
 match protocol http server Apache
 match protocol http location *example.com”
 match protocol http content-encoding compress
 match protocol http match protocol http content-base *exmaple.com”
```

## Related Commands

| Command | Description |
|---|---|
| **show ip nbar protocol-discovery** | Displays the statistics gathered by the NBAR Protocol Discovery feature. |

# match protocol pppoe-discovery

To match and classify PPP over Ethernet (PPPoE) control-plane packets that are sent to the control plane, use the **match protocol pppoe-discovery** command in QoS class-map configuration mode. To remove this match criterion, use the **no** form of this command.

**match protocol pppoe-discovery**

**no match protocol pppoe-discovery**

## Syntax Description

This command has no arguments or keywords.

## Command Default

PPPoE control packets sent to the control plane are not matched or classified.

## Command Modes

QoS class-map configuration (config-cmap)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 2.3 | This command was introduced on Cisco ASR 1000 Series Aggregation Routers. |

## Usage Guidelines

The **match pppoe-discovery** command is associated with control-plane-related features such as Control Plane Policing (CoPP).

When used in a class map, the **match protocol pppoe-discovery** command can classify either ingress PPPoE control-plane packets or egress PPPoE control-plane packets and include them in a specified traffic class. That class can then be configured in a policy map and can receive the desired quality of service (QoS) feature (such as traffic policing).

**Note** With CSCts20715, the **match protocol pppoe-discovery** command matches PPPoE Active Discovery Initiation (PADI) packets received over Automatic Virtual Circuits (AutoVC) configured on an ATM subinterface. Each ATM cell of PADI packets is punted as a separate packet and is counted towards the PPPOE_DISCOVERY packet count.

## Examples

The following is an example of the **match protocol pppoe-discovery** command configured in a class-map called copplass-pppoe-discovery. PPPoE control-plane traffic identified as meeting the match criterion is placed in a class called coppclass-pppoe-discovery.

The coppclass-pppoe-discovery class is then configured in a policy map called copp-policy-pppoe-discovery, and the QoS traffic policing feature is applied using the **police** command.

```
Router> enable
```

```
Router# configure terminal
Router(config)# class-map match-all coppclass-pppoe-discovery
Router(config-cmap)# match protocol pppoe-discovery
Router(config-cmap)# exit
Router(config)# policy-map copp-policy-pppoe-discovery
Router(config-pmap)# class coppclass-pppoe-discovery
Router(config-pmap-c)# police rate 8000 bps conform-action transmit exceed-action drop
Router(config-pmap-c-police)# end
```

## Related Commands

| Command | Description |
|---|---|
| **control-plane** | Enters control-plane configuration mode, which allows users to associate or modify attributes or parameters (such as a service policy) that are associated with the control plane of the device. |
| **match protocol** | Configures the match criterion for a class map on the basis of the specified protocol. |
| **police rate** | Configures traffic policing for traffic that is destined for the control plane. |
| **show policy-map control-plane** | Displays the configuration and statistics for a traffic class or all traffic classes in the policy maps attached to the control plane for aggregate or distributed control-plane services. |
| **show pppoe session** | Displays information about currently active PPPoE sessions. |

# match protocol rtp

To configure network-based application recognition (NBAR) to match Real-Time Transfer Protocol (RTP) traffic, use the **matchprotocolrtp** command in class-map configuration mode. To disable NBAR from matching RTP traffic, use the no form of this command.

**match protocol rtp** [**audio**| **video**| **payload-type** *payload-string*]

**no match protocol rtp** [**audio**| **video**| **payload-type** *payload-string*]

## Syntax Description

| | |
|---|---|
| **audio** | (Optional) Specifies matching by audio payload-type values in the range of 0 to 23. These payload-type values are reserved for audio traffic. |
| **video** | (Optional) Specifies matching by video payload-type values in the range of 24 to 33. These payload-type values are reserved for video traffic. |
| **payload-type** | (Optional) Specifies matching by a specific payload-type value, providing more granularity than is available with the **audio** or **video** keywords. |
| *payload-string* | (Optional) User-specified string that contains the specific payload-type values.<br>A *payload-string* argument can contain commas to separate payload-type values and hyphens to indicate a range of payload-type values. A *payload-string* argument can be specified in hexadecimal (prepend 0x to the value) and binary (prepend b to the value) notation in addition to standard number values. |

## Command Default

No match criteria are specified.

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(8)T | This command was introduced. |
| 12.1(11b)E | This command was integrated into Cisco IOS Release 12.1(11b)E. |
| 12.1(13)E | This command was implemented on Catalyst 6000 family switches without FlexWAN modules. |

| Release | Modification |
|---|---|
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(17a)SX1 | This command was integrated into Cisco IOS Release 12.2(17a)SX1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

Entering the **matchprotocolrtp** command without any other keywords establishes all RTP traffic as successful match criteria.

RTP is a packet format for multimedia data streams. It can be used for media-on-demand as well as interactive services such as Internet telephony. RTP consists of a data and a control part. The control part is called Real-Time Transport Control Protocol (RTCP). It is important to note that the NBAR RTP Payload Classification feature does not identify RTCP packets and that RTCP packets run on odd-numbered ports while RTP packets run on even-numbered ports.

The payload type field of an RTP packet identifies the format of the RTP payload and is represented by a number. NBAR matches RTP traffic on the basis of this field in the RTP packet. A working knowledge of RTP and RTP payload types is helpful if you want to configure NBAR to match RTP traffic. For more information about RTP and RTP payload types, refer to RFC 1889, *RTP: A Transport Protocol for Real-Time Applications.*

## Examples

The following example configures NBAR to match all RTP traffic:

```
class-map class1
 match protocol rtp
```

The following example configures NBAR to match RTP traffic with the payload-types 0, 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, and 64:

```
class-map class2
 match protocol rtp payload-type "0, 1, 4-0x10, 10001b-10010b, 64"
```

# match qos-group

To identify a specific quality of service (QoS) group value as a match criterion, use the **matchqos-group**command in class-map configuration or policy inline configuration mode. To remove a specific QoS group value from a class map, use the **no** form of this command.

**match qos-group** *qos-group-value*

**no match qos-group** *qos-group-value*

## Syntax Description

| | |
|---|---|
| *qos-group-value* | The exact value from 0 to 99 used to identify a QoS group value. |

## Command Default

No match criterion is specified.

## Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

## Command History

| Release | Modification |
|---|---|
| 11.1CC | This command was introduced. |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 Series Routers. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode. |
| 12.2(58)SE | This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor. |

## Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

The **matchqos-group** command is used by the class map to identify a specific QoS group value marking on a packet. This command can also be used to convey the received Multiprotocol Label Switching (MPLS) experimental (EXP) field value to the output interface.

The *qos-group-value* argument is used as a marking only. The QoS group values have no mathematical significance. For instance, the *qos-group-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *qos-group-value* of 2 is different than a packet marked with the *qos-group-value* of 1. The treatment of these packets is defined by the user through the setting of QoS policies in QoS policy-map class configuration mode.

The QoS group value is local to the router, meaning that the QoS group value that is marked on a packet does not leave the router when the packet leaves the router. If you need a marking that resides in the packet, use IP precedence setting, IP differentiated services code point (DSCP) setting, or another method of packet marking.

This command can be used with the **random-detectdiscard-class-based**command.

**Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE**

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

## Examples

The following example shows how to configure the service policy named priority50 and attach service policy priority50 to an interface. In this example, the class map named qosgroup5 will evaluate all packets entering Fast Ethernet interface 1/0/0 for a QoS group value of 5. If the incoming packet has been marked with the QoS group value of 5, the packet will be treated with a priority level of 50.

```
Router(config)#

class-map qosgroup5
Router(config-cmap)
#
 match qos-group 5
Router(config)#

exit
Router(config)#

policy-map priority50
Router(config-pmap)#

class qosgroup5
Router(config-pmap-c)#

priority 50
Router(config-pmap-c)#

exit
Router(config-pmap)#

exit
Router(config)#

interface fastethernet1/0/0
Router(config-if)#

service-policy output priority50
```

## Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the criteria of a QoS value of 4 will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match qosgroup 4
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **service-policy type performance-monitor** | Associates a Performance Monitor policy with an interface. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **random-detect discard-class-based** | Bases WRED on the discard class value of a packet. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **set precedence** | Specifies an IP precedence value for packets within a traffic class. |
| **set qos-group** | Sets a group ID that can be used later to classify packets. |

# match source-address mac

To use the source MAC address as a match criterion, use the **matchsource-addressmac**command in class-map configuration or policy inline configuration mode. To remove a previously specified source MAC address as a match criterion, use the **no**form of this command.

**match source-address mac** *address-source*

**no match source-address mac** *address-source*

## Syntax Description

| | |
|---|---|
| *address-source* | The source source MAC address to be used as a match criterion. |

## Command Default

No match criterion is configured.

## Command Modes

Class-map configuration (config-cmap) Policy inline configuration (config-if-spolicy-inline)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)XE | This command was introduced. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode. |
| 12.2(58)SE | This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor. |

## Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

This command can be used only on an input interface with a MAC address; for example, Fast Ethernet and Ethernet interfaces.

This command cannot be used on output interfaces with no MAC address, such as serial and ATM interfaces.

**Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE**

You must first enter the s**ervice-policytypeperformance-monitorinline**command.

## Examples

The following example uses the MAC address mac 0.0.0 as a match criterion:

```
Router(config)# class-map matchsrcmac
Router(config-cmap)
#
match source-address mac 0.0.0
```

## Examples

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the specified MAC source address will be monitored based on the parameters specified in the flow monitor configuration named**fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match source-address mac 0.0.0
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **service-policy type performance-monitor** | Associates a Performance Monitor policy with an interface. |

# match start

**Note** Effective with Cisco IOS Release 15.2(4)M, the **match start** command is not available in Cisco IOS software.

To configure the match criteria for a class map on the basis of the datagram header (Layer 2 ) or the network header (Layer 3), use the **match start** command in class-map configuration mode. To remove the specified match criteria, use the **no** form of this command.

**match start** {**l2-start**| **l3-start**} **offset** *number* **size** *number* {**eq**| **neq**| **gt**| **lt**| **range** *range*| **regex** *string*} {*value* [ *value2* ]| [ *string* ]}

**no match start** {**l2-start**| **l3-start**} **offset** *number* **size** *number* {**eq**| **neq**| **gt**| **lt**| **range** *range*| **regex** *string*} {*value* [ *value2* ]| [ *string* ]}

## Syntax Description

| | |
|---|---|
| **l2-start** | Match criterion starts from the datagram header. |
| **l3-start** | Match criterion starts from the network header. |
| **offset** *number* | Match criterion can be made according to any aribitrary offset. |
| **size** *number* | Number of bytes in which to match. |
| eq | *Match criteria is met if the* packet is equal to the specified value or mask. |
| neq | *Match criteria is met if the* packet is not equal to the specified value or mask. |
| *mask* | (Optional) Can be used when the **eq** or the **neq** keywords are issued. |
| gt | *Match criteria is met if the* packet is greater than the specified value. |
| lt | *Match criteria is met if the* packet is less than the specified value. |
| range *range* | Match critera is based upon a lower and upper boundary protocol field range. |
| regex *string* | Match critera is based upon a string that is to be matched. |

| | |
|---|---|
| *value* | Value for which the packet must be in accordance with. |

**Command Default** No match criteria are configured.

**Command Modes** Class-map configuration

**Command History**

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |
| 12.2(18)ZY | This command was integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA). |
| Cisco IOS XE 2.2 | This command was integrated into Cisco IOS XE Release 2.2. |

**Usage Guidelines** To the match criteria that is to be used for flexible packet matching, you must first enter the**class-map** command to specify the name of the class whose match criteria you want to establish. Thereafter, you can enter one of the following commands:

- **match field** (which configures the match criteria for a class map on the basis of the fields defined in the protocol header description files [PHDFs])
- **match start** (which can be used if a PHDF is not loaded onto the router)

**Examples** The following example shows how to configure FPM for blaster packets. The class map contains the following match criteria: TCP port 135, 4444 or UDP port 69; and pattern 0x0030 at 3 bytes from start of IP header.

```
load protocol disk2:ip.phdf
load protocol disk2:tcp.phdf
load protocol disk2:udp.phdf
class-map type stack match-all ip-tcp
 match field ip protocol eq 0x6 next tcp
class-map type stack match-all ip-udp
 match field ip protocol eq 0x11 next udp
class-map type access-control match-all blaster1
 match field tcp dest-port eq 135
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster2
 match field tcp dest-port eq 4444
 match start 13-start offset 3 size 2 eq 0x0030
class-map type access-control match-all blaster3
 match field udp dest-port eq 69
 match start 13-start offset 3 size 2 eq 0x0030
policy-map type access-control fpm-tcp-policy
 class blaster1
 drop
 class blaster2
```

```
 drop
policy-map type access-control fpm-udp-policy
 class blaster3
 drop
policy-map type access-control fpm-policy
 class ip-tcp
 service-policy fpm-tcp-policy
 class ip-udp
 service-policy fpm-udp-policy
interface gigabitEthernet 0/1
 service-policy type access-control input fpm-policy
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **load protocol** | Loads a PHDF onto a router. |
| **match field** | Configures the match criteria for a class map on the basis of the fields defined in the PHDFs. |

# match tag (class-map)

To specify the tag to be matched for a tag type of class map, use the **matchtag** command in class-map configuration mode. To delete the tag, use the **no** form of this command.

**match tag** *tag-name*

**no match tag** *tag-name*

## Syntax Description

| | |
|---|---|
| *tag-name* | Name of the tag. |

## Command Default

No match tags are defined.

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |

## Usage Guidelines

The access control server (ACS) sends the tag attribute to the network access device (NAD) using the Cisco attribute-value (AV) pair. (The tag attribute can also be sent to the NAD using the IETF attribute 88.)

## Examples

The following example shows that the tag to be matched is named “healthy”:

```
Router(config)# class-map type tag healthy_class
Router(config-cmap)# match tag healthy
Router(config-cmap)# end
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |

# match vlan (QoS)

To match and classify traffic on the basis of the virtual local-area network (VLAN) identification number, use the **matchvlan** command in class-map configuration mode. To remove a previously specified VLAN identification number as a match criterion, use the **no** form of this command.

**match vlan** *vlan-id-number*

**no match vlan** *vlan-id-number*

## Syntax Description

| | |
|---|---|
| *vlan-id-number* | VLAN identification number, numbers, or range of numbers. Valid VLAN identification numbers must be in the range of 1 to 4095. |

## Command Default

Traffic is not matched on the basis of the VLAN identification number.

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SB2 | This command was introduced for use on Cisco 10000 series routers only. . |
| 15.1(1)T | This command was modified. Support for this command is no longer limited to the Cisco 10000 series routers. |
| Cisco IOS XE Release 2.1 | This command was modifed. Support for this command was introduced on the Cisco ASR 1000 series routers. |

## Usage Guidelines

### Specifying VLAN Identification Numbers

You can specify a single VLAN identification number, multiple VLAN identification numbers separated by spaces (for example, 2 5 7), or a range of VLAN identification numbers separated by a hyphen (for example, 25-35).

### Support Restrictions

The following restrictions apply to the **matchvlan** command:

- The **matchvlan** command is supported for IEEE 802.1q and Inter-Switch Link (ISL) VLAN encapsulations only.
- As of Cisco IOS Release 12.2(31)SB2, the **matchvlan** command is supported on Cisco 10000 series routers only.

## Examples

In the following sample configuration, the **matchvlan** command is enabled to classify and match traffic on the basis of a range of VLAN identification numbers. Packets with VLAN identification numbers in the range of 25 to 50 are placed in the class called class1.

```
Router> enable
Router# configure terminal
Router(config)# class-map class1
Router(config-cmap)# match vlan 25-50
Router(config-cmap)# end
```

**Note** Typically, the next step would be to configure class1 in a policy map, enable a quality of service (QoS) feature (for example, class-based weighted fair queueing [CBWFQ]) in the policy map, and attach the policy map to an interface. To configure a policy map, use the **policy-map** command. To enable CBWFQ, use the **bandwidth** command (or use the command for the QoS feature that you want to enable). To attach the policy map to an interface, use the**service-policy**command. For more information about classifying network traffic on the basis of a match criterion, see the "Classification" part of the Cisco IOS Quality of Service Solutions Configuration Guide , Release 12.4T.

## Related Commands

| Command | Description |
|---|---|
| **bandwidth (policy-map class)** | Specify or modifies the bandwidth allocated for a class belonging to a policy map. |
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces. |
| **service-policy** | Attached a policy map to an interface. |

# match vlan inner

To configure a class map to match the innermost VLAN ID in an 802.1q tagged frame, use the **matchvlaninner**command in ATM interface configuration mode. To remove matching on the innermost VLAN ID of an 802.1q tagged frame, use the **no** form of this command.

**match vlan inner** *vlan-ids*

**no match vlan inner** *vlan-ids*

## Syntax Description

| | |
|---|---|
| *vlan-ids* | One or more VLAN IDs to be matched. The valid range for VLAN IDs is from 1 to 4095, and the list of VLAN IDs can include one or all of the following:<br>• Single VLAN IDs, separated by spaces. For example: 100 200 300<br>• One or more ranges of VLAN IDs, separated by spaces. For example: 1-1024 2000-2499 |

## Command Default

Packets are not matched on the basis of incoming dot1q VLAN inner IDs.

## Command Modes

Class map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(18)SXF | This command was implemented on Cisco 7600 series routers. |

## Examples

The following example creates a class map that matches packets with a VLAN IDs of 100 to 300.

```
Router(config)#
cclass-map match-all vlan100
Router(config-cmap)# match vlan inner 100
Router(config-cmap)# exit
Router(config)# class-map match-all vlan200
Router(config-cmap)# match vlan inner 200
Router(config-cmap)# exit
Router(config)# class-map match-all vlan300
Router(config-cmap)# match vlan inner 300
```

## Related Commands

| Command | Description |
|---|---|
| **clear cef linecard** | Clears Cisco Express Forwarding (CEF) information on one or more line cards, but does not clear the CEF information on the main route processor (RP). This forces the line cards to synchronize their CEF information with the information that is on the RP. |
| **match qos-group** | Identifies a specified QoS group value as a match criterion. |
| **mls qos trust** | Sets the trusted state of an interface to determine which incoming QoS field on a packet, if any, should be preserved. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |
| **show platform qos policy-map** | Displays the type and number of policy maps that are configured on the router. |

# maximum (local policy)

To set the limits for Resource Reservation Protocol (RSVP) resources, use the **maximum** command in local policy configuration mode. To delete the limits, use the **no** form of this command.

**maximum** [**bandwidth** [**group**| **single**] *bandwidth*| **senders** *maximum-senders*]

**no maximum** [**bandwidth** [**group**| **single**]| **senders**]

## Syntax Description

| | |
|---|---|
| **bandwidth** | (Optional) Indicates bandwidth limits for RSVP reservations. |
| **group** | (Optional) Specifies the amount of bandwidth, in kbps, that can be requested by all the reservations covered by a local policy. |
| single | (Optional) Specifies the maximum bandwidth, in kbps, that can be requested by any specific RSVP reservation covered by a local policy. |
| *bandwidth* | Maximum limit for the requested bandwidth, in kbps. Range is from 1 to 10000000. |
| **senders** | (Optional) Limits the number of RSVP senders affected by a local policy that can be active at the same time on a router. |
| *maximum-senders* | Maximum number of senders the specified policy allows. Range is from 1 to 50000; the default is 1000. |

## Command Default

No maximum bandwidth limit is set and no RSVP senders are configured.

## Command Modes

Local policy configuration (config-rsvp-local-if-policy)

## Command History

| Release | Modification |
|---|---|
| 12.0(29)S | This command was introduced. |
| 12.4(6)T | This command was modified to apply to RESV messages. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

As part of the application ID enhancement, the **maximumbandwidth** command applies to RESV messages. This change has the following benefits:

- Allows the local policy bandwidth limit to be used by RSVP's admission control process for both shared and nonshared reservations. Releases that performed group bandwidth checks on PATH messages could not account for bandwidth sharing and, as a result, you had to account for sharing by creating a larger maximum group bandwidth for the policy.
- Allows a local policy to trigger preemption during the admission control function if there is insufficient policy bandwidth to meet the needs of an incoming RESV message.

## Examples

The following example specifies the maximum bandwidth for a group of reservations and for a single reservation, respectively:

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet 1/0
Router(config-if)# ip rsvp policy local identity video
Router(config-rsvp-local-policy)# maximum bandwidth group 500
Router(config-rsvp-local-policy)# maximum bandwidth single 50
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp policy local** | Determines how to perform authorization on RSVP requests. |

# maximum bandwidth ingress

To configure the bandwidth parameters for the ingress policy pool, use the **maximumbandwidthingress** command in local policy configuration mode or local policy interface configuration mode. To disable the bandwidth configuration for the ingress policy pool, use the **no** form of this command.

### Command Syntax in Local Policy Configuration Mode

**maximum bandwidth ingress** {**group**| **single**} *bandwidth*

**no maximum bandwidth ingress** {**group**| **single**}

### Command Syntax in Local Policy Interface Configuration Mode

**maximum bandwidth ingress** {**group** *bandwidth*| **percent** {**group**| **single**} *percent*| **single** *bandwidth*}

**no maximum bandwidth ingress** {**group**| **percent** {**group**| **single**}| **single**}

## Syntax Description

| | |
|---|---|
| **group** | Specifies the maximum ingress bandwidth, in kb/s, that can be requested by all the reservations covered by a local policy. |
| single | Specifies the maximum ingress bandwidth, in kb/s, that can be requested by any specific RSVP reservation covered by a local policy. |
| *bandwidth* | Maximum limit for the requested ingress bandwidth, in kb/s. |
| **percent** {**group** \| **single**} | Specifies a percentage of the ingress bandwidth of an interface as the maximum bandwidth available to a group of flows or a single flow. |
| *percent* | Maximum limit for the requested bandwidth, in percent. |

## Command Default

RSVP is disabled by default; therefore, maximum bandwidth limit is not set.

## Command Modes

Local policy configuration (config-rsvp-local-policy) Local policy interface configuration (config-rsvp-local-if-policy)

## Command History

| Release | Modification |
|---|---|
| 15.1(3)T | This command was introduced. |

| Release | Modification |
|---|---|
| 15.1(1)S | This command was integrated into Cisco IOS Release 15.1(1)S. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |

## Usage Guidelines

You can use the **maximumbandwidthingress**command to configure the maximum bandwidth for a given policy. You can also configure a percentage of the RSVP ingress bandwidth of an interface as the maximum bandwidth available to a group of flows, or a single flow matching the policy. The percentages of the RSVP bandwidth to be configured as the maximum bandwidth are not available for global-based RSVP policies, but are available for interface RSVP policies.

The **maximumbandwidthingresspercent** command is mutually exclusive with the **maximumbandwidthingressgroup** and **maximumbandwidthingresssingle** commands. That is, if you configure the maximum percentage of RSVP ingress bandwidth using the **maximumbandwidthingresspercent** command, any configurations made using the **maximumbandwidthingressgroup** and **maximumbandwidthingresssingle** commands are removed.

## Examples

The following example shows how to configure the maximum ingress bandwidth for a group of reservations and for a single reservation respectively, in a global-based RSVP policy:

```
Device> enable
Device# configure terminal
Device(config)# ip rsvp policy local identity rsvp-video
Device(config-rsvp-local-policy)# maximum bandwidth ingress group
 200
Device(config-rsvp-local-policy)# maximum bandwidth ingress single 100
The following example shows how to configure the maximum percentage of RSVP ingress bandwidth
 of an interface for a group of reservations and for a single reservation, respectively:
Device> enable
Device# configure terminal
Device(config)# interface tunnel 0
Device(config-if)# ip rsvp policy local identity rsvp-video
Device(config-rsvp-local-if-policy)# maximum bandwidth ingress percent group 50
Device(config-rsvp-local-if-policy)# maximum bandwidth ingress single 50
```

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp ingress** | Displays information about the RSVP ingress bandwidth configured on interfaces. |

# maximum bandwidth percent

To configure the percentage of the Resource Reservation Protocol (RSVP) bandwidth of an interface as the maximum bandwidth available to a group of flows or a single flow, use the **maximumbandiwidthpercent**command in local policy configuration mode. To disable this configuration, use the **no** form of this command.

**maximum bandwidth percent** {**group**| **single**} *bandwidth-percentage*

**no maximum bandwidth percent** {**group**| **single**}

## Syntax Description

| | |
|---|---|
| **group** | Specifies the amount of bandwidth, in kb/s, that can be requested by all the reservations covered by a local policy. |
| **single** | Specifies the maximum bandwidth, in kb/s, that can be requested by any specific RSVP reservation covered by a local policy. |
| *bandwidth-percentage* | Maximum limit for the requested bandwidth, in kb/s. |

## Command Default

RSVP is disabled by default; therefore, no percentage bandwidth is set.

## Command Modes

Local policy configuration (config-rsvp-local-if-policy)

## Command History

| Release | Modification |
|---|---|
| 15.1(2)T | This command was introduced. |

## Usage Guidelines

The **maximumbandwidthpercent** command is mutually exclusive with the **maximumbandwidthgroup** and **maximumbandwidthsingle** commands. That is, if you configure the maximum percentage of RSVP using the **maximumbandwidthpercent** command, any configurations made using the **maximumbandwidthgroup** and **maximumbandwidthsingle** commands are removed. The **maximumbandwidthpercent** command is not present in the global RSVP policy.

This maximum percentage of RSVP bandwidth configured for a group of flows is used to do RSVP Call Admission Control (CAC) for the flows matching with the policy. The **maximumbandiwidthpercent** command allows oversubscription. That is, you can configure more than 100 percent of the RSVP bandwidth as the maximum bandwidth for group reservations or as the maximum bandwidth for a single reservation.

## Examples

The following example shows how to conifgure the maximum percentage of RSVP bandwidth of an interface for a group of reservations and for a single reservation, respectively:

```
Router> enable
Router# configure terminal
Router(config)# interface fastethernet 1/0
Router(config-if)# ip rsvp policy local identity video
Router(config-rsvp-local-policy)# maximum bandwidth percent group 50
Router(config-rsvp-local-policy)# maximum bandwidth single 50
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp policy local** | Determines how to perform authorization on RSVP requests. |
| **maximum** (local policy) | Sets the limits for RSVP resources. |

# maximum header

To specify the maximum size of the compressed IP header, use the **maximumheader** command in IPHC-profile configuration mode. To return the maximum size of the compressed IP header to the default size, use the **no** form of this command.

**maximum header** *number-of-bytes*

**no maximum header**

## Syntax Description

| | |
|---|---|
| *number-of-bytes* | The maximum header size, in bytes. Valid entries are numbers from 20 to 168. Default is 168. |

## Command Default

The maximum size of the compressed IP header is 168 bytes.

## Command Modes

IPHC-profile configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

The **maximumheader** command allows you to define the maximum size of the IP header of a packet to be compressed. Any packet with an IP header that exceeds the maximum size is sent uncompressed.

Use the *number-of-bytes* argument of the **maximumheader** command to restrict the size of the IP header to be compressed.

**Intended for Use with IPHC Profiles**

The **maximumheader** command is intended for use as part of an IPHC profile. An IPHC profile is used to enable and configure header compression on your network. For more information about using IPHC profiles to configure header compression, see the "Header Compression" module and the "Configuring Header Compression Using IPHC Profiles" module of the *Cisco IOS Quality of Service Solutions Configuration Guide* , Release 12.4T.

**Prerequisite**

Before using the **maximumheader**command, you must enable either TCP header compression or non-TCP header compression. To enable TCP header compression, use the **tcp** command. To enable non-TCP header compression, use the **non-tcp** command.

## Examples

The following is an example of an IPHC profile called profile2. In this example, the maximum size of the compressed IP header is set to 75 bytes.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp
Router(config-iphcp)# maximum header 75
Router(config-iphcp)# end
```

## Related Commands

| Command | Description |
|---|---|
| **iphc-profile** | Creates an IPHC profile. |
| **non-tcp** | Enables non-TCP header compression within an IPHC profile. |
| **tcp** | Enables TCP header compression within an IPHC profile. |

# max-reserved-bandwidth

**Note** Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **max-reservedbandwidth**command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

**Note** Effective with Cisco IOS XE Release 3.2S, the **max-reservedbandwidth**command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To change the percent of interface bandwidth allocated for Resource Reservation Protocol (RSVP), class-based weighted fair queueing (CBWFQ), low latency queueing (LLQ), IP RTP Priority, Frame Relay IP RTP Priority, Frame Relay PVC Interface Priority Queueing (PIPQ), or hierarchical queueing framework (HQF), use the **max-reservedbandwidth** command in interface configuration mode. To restore the default value, use the **no** form of this command.

**max-reserved-bandwidth** *percent*

**no max-reserved-bandwidth**

## Syntax Description

| | |
|---|---|
| *percent* | Amount of interface bandwidth allocated for RSVP, CBWFQ, LLQ, IP RTP Priority, Frame Relay IP RTP Priority, Frame Relay PIPQ, and HQF. |

## Command Default

75 percent on all supported platforms except the Cisco 7500 series routers, which do not have this restriction.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |

| Release | Modification |
|---|---|
| 12.4(20)T | Support was added for HQF using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC).<br>**Note** This is the last T release in which the command is supported. |
| Cisco IOS XE Release 2.6 | This command was modified. This command was hidden. |
| 15.0(1)S | This command was modified. This command was hidden. |
| 15.1(3)T | This command was modified. This command was hidden. |
| Cisco IOS XE Release 3.2S | This command was replaced by an MQC command (or sequence of MQC commands). |

## Usage Guidelines

The **max-reserved-bandwidth** command is not supported in Cisco IOS Release 12.2SR or in 12.2SX. It is supported in 12.4T, but only up to the 12.4(20)T release in which HQF functionality was integrated.

The sum of all bandwidth allocation on an interface should not exceed 75 percent of the available bandwidth on an interface. The remaining 25 percent of bandwidth is used for overhead, including Layer 2 overhead, control traffic, and best-effort traffic.

If you need to allocate more than 75 percent for RSVP, CBWFQ, LLQ, IP RTP Priority, Frame Relay IP RTP Priority, Frame Relay PIPQ, or HQF, you can use the **max-reserved-bandwidth** command. The *percent* argument specifies the maximum percentage of the total interface bandwidth that can be used.

If you do use the **max-reserved-bandwidth** command, make sure that not too much bandwidth is taken away from best-effort and control traffic.

## Examples

In the following example, the policy map called policy1 is configured for three classes with a total of 8 Mbps configured bandwidth, as shown in the output from the **showpolicy-map** command:

```
Router# show policy-map policy1
 Policy Map policy1
  Weighted Fair Queueing
    Class class1
      Bandwidth 2500 (kbps) Max Threshold 64 (packets)
    Class class2
      Bandwidth 2500 (kbps) Max Threshold 64 (packets)
    Class class3
      Bandwidth 3000 (kbps) Max Threshold 64 (packets)
```

When you enter the **service-policy**command in an attempt to attach the policy map on a 10-Mbps Ethernet interface, an error message such as the following is produced:

```
I/f Ethernet1/1 class class3 requested bandwidth 3000 (kbps) Available only 2500 (kbps)
```

The error message is produced because the default maximum configurable bandwidth is 75 percent of the available interface bandwidth, which in this example is 7.5 Mbps. To change the maximum configurable bandwidth to 80 percent, use the **max-reserved-bandwidth** command in interface configuration mode, as follows:

```
max-reserved-bandwidth 80
service output policy1
end
```

To verify that the policy map was attached, enter the **showpolicy-mapinterface** command:

```
Router# show policy-map interface e1/1
 Ethernet1/1  output :policy1
  Weighted Fair Queueing
    Class class1
      Output Queue:Conversation 265
        Bandwidth 2500 (kbps) Packets Matched 0 Max Threshold 64 (packets)
        (discards/tail drops) 0/0
    Class class2
      Output Queue:Conversation 266
        Bandwidth 2500 (kbps) Packets Matched 0 Max Threshold 64 (packets)
        (discards/tail drops) 0/0
    Class class3
      Output Queue:Conversation 267
        Bandwidth 3000 (kbps) Packets Matched 0 Max Threshold 64 (packets)
        (discards/tail drops) 0/0
```

## Examples

The following example configures a strict priority queue in a virtual template configuration with CBWFQ. The **max-reserved-bandwidth** command changes the maximum bandwidth allocated between CBWFQ and IP RTP Priority from the default (75 percent) to 80 percent.

```
multilink virtual-template 1
interface virtual-template 1
 ip address 172.16.1.1 255.255.255.0
 no ip directed-broadcast
 ip rtp priority 16384 16383 25
 service-policy output policy1
 ppp multilink
 ppp multilink fragment-delay 20
 ppp multilink interleave
 max-reserved-bandwidth 80
 end
interface Serial0/1
 bandwidth 64
 ip address 10.1.1.2 255.255.255.0
 no ip directed-broadcast
 encapsulation ppp
 ppp multilink
 end
```

**Note** To make the virtual access interface function properly, do not configure the **bandwidth** command on the virtual template. Configure it on the actual interface, as shown in the example.

## Related Commands

| Command | Description |
|---|---|
| **bandwidth (policy-map class)** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map. |
| **ip rtp priority** | Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |

| Command | Description |
|---|---|
| **show policy-map** | Displays the configuration of all classes comprising the specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

# metadata application-params

To enter metadata application entry configuration mode and create new metadata application parameters, use the **metadata application-params** command in global configuration mode. To remove previously configured metadata application parameters, use the **no** form of this command.

**metadata application-params** *app-param-name*

**no metadata application-params** *app-param-name*

## Syntax Description

| | |
|---|---|
| *app-param-name* | Metadata application name that can be used as the match criterion for provisioning control plane classification. |

## Command Default

The application parameters for metadata-based classification are not created.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T | This command was introduced. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |

## Usage Guidelines

To create new metadata application parameters that can be used as match criteria for provisioning control plane classification, use the **metadata application-params** command. The **metadata application-params** command places the device in metadata application entry configuration mode. Use the following commands in metadata application entry configuration mode to configure the properties of the application. Configuring the name and ID is mandatory.

- **default—**Default properties for the name, description, and ID for the specified application.
- **description** *description-text***—**Description of the application. Supports up to 55 characters.
- **identifier** *id-value***—**Application ID. Internally maps to the application name. The range is from 1 to 16777215.
- **name** *name***—**Name of the application. Supports up to 24 characters.

Use the **show metadata application table** command to display the details of all metadata applications.

## Examples

The following example shows how to create a new metadata application with appropriate parameters:

```
Device(config)# metadata application-params app1
Device(config-md-app-entry)# name instant-messaging-audio
Device(config-md-app-entry)# identifier 243
Device(config-md-app-entry)# description instant messaging audio recordings
```

The following output of the **show metadata application table** command shows the name and ID of all the metadata applications configured on a specific endpoint:

```
Device# show metadata application table

ID     Name                  Vendor                Vendor id
-------------------------------------------------------------------------------
113    telepresence-media    -                     -
114    telepresence-contr$   -                     -
478    telepresence-data     -                     -
414    webex-meeting         -                     -
56     citrix                -                     -
81     cisco-phone           -                     -
472    vmware-view           -                     -
473    wyze-zero-client      -                     -
61     rtp                   -                     -
64     h323                  -                     -
5060   sip                   -                     -
554    rtsp                  -                     -
496    jabber                -                     -
5222   xmpp-client           -                     -
```

The table below describes the significant fields shown in the display.

***Table 15: show metadata application table Field Descriptions***

| Field | Description |
|---|---|
| ID | Application ID. Internally maps to the application name. |
| Name | Name of the application. |

## Related Commands

| Command | Description |
|---|---|
| **debug metadata** | Enables debugging for metadata flow. |
| **default** | Displays default properties for the name, description, and ID for the specified application. |
| **description** | Displays the description of the application. |
| **identifier** | Displays the Application ID. |
| **name** | Displays the name of the application. |

| Command | Description |
|---|---|
| **show metadata application table** | Displays a list of metadata applications defined on a device. |
| **show metadata flow** | Displays metadata flow information. |
| **name** | Displays the name of the application. |

# metadata flow

To enable metadata on all interfaces or on a specific interface, use the **metadata flow** command in global configuration mode or interface configuration mode. To disable metadata, use the **no** form of this command.

**metadata flow**

**no metadata flow**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Metadata is disabled on an interface.

## Command Modes

Global configuration (config)

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T | This command was introduced. |
| Cisco IOS XE Release 3.7S | This command was integrated into Cisco IOS XE Release 3.7S. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |

## Usage Guidelines

If you use the **metadata flow** command in global configuration mode, metadata is enabled at the device level. That is, metadata is enabled on all the interfaces configured on the device. If you use the **metadata flow** command in interface configuration mode, metadata is enabled on the specified interface only. You can use the **no metadata flow** command in interface configuration mode to disable metadata on any one interface. However, metadata flows that enter from other interfaces will not be able to pass through an interface on which metadata has been disabled. In such instances, the flow table will not be populated and classification will not complete successfully. When you explicitly enable or disable metadata on an interface, configuration details are retrieved using the nonvolatile generation (NVGEN) method and are displayed in the configuration.

## Examples

The following example shows how to enable metadata at the device level:

```
Device(config)# metadata flow
```

The following example shows how to enable metadata at the per-interface level:

```
Device(config)# interface gigabitethernet 0/0
Device(config-if)# metadata flow
```

## Related Commands

| Command | Description |
|---|---|
| **metadata flow (troubleshooting)** | Creates flow entries for testing and troubleshooting the metadata flow. |

# metadata flow (troubleshooting)

To simulate the creation of flows for testing and troubleshooting metadata, use the **metadata flow** command in global configuration mode. To remove the flows created for testing and troubleshooting, use the **no** form of this command.

### Cisco IOS Release 15.1(1)SY and Later Releases

**metadata flow**

**no metadata flow**

### Releases Prior to Cisco IOS Release 15.1(1)SY

**metadata flow** [**entry** *entry-name*| **flow-specifier** *flow-specifier-name* | **session-params** *session-name*]

**no metadata flow** [**entry** *entry-name*| **flow-specifier** *flow-specifier-name* | **session-params** *session-name*]

## Syntax Description

| | |
|---|---|
| **entry** *entry-name* | Creates a flow entry with the specified name. |
| **flow-specifier** *flow-specifier-name* | Configures source and destination information. |
| **session-params** *session-name* | Configures session parameters for the flow. |

## Command Default

Static metadata flow entries are not created.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T | This command was introduced. |
| 15.1(1)SY | The command was modified. The **entry** *entry-name*, **flow-specifier** *flow-specifier-name*, and **session-params** *session-name* keyword-argument pairs were removed. |

## Usage Guidelines

You can use the **metadata flow** command along with the associated keywords when you need to simulate an environment consisting of virtual endpoints for testing or troubleshooting purposes.

Use the **metadata flow entry** *entry-name* command to create a flow. To create a successful flow, specify the flow specifier and session parameters.

Using the **flow-specifier** *flow-specifier-name* keyword and argument pair creates a flow specifier and places the device in metadata configuration flow specifier mode. Use the following commands in metadata configuration flow specifier mode to configure the flow tuple for the flow:

- **dest-ip** *ip-address* **dest-port** *port-number*—Specifies the destination IPv4 address and destination port number for the endpoint.
- **source-ip** *ip-address* **source-port** *port-number*—Specifies the source IPv4 address and source port number for the endpoint.

Using the **session-params** *session-name* keyword and argument pair places the command in metadata session parameters configuration mode. Use the following related command in metadata session parameters configuration mode to configure the session parameters for the flow:

- **application name** *application-name*—Associates the specified application name to the session.

Using the **entry** *entry-name* keyword and argument pair places the command in metadata entry configuration mode. In metadata entry configuration mode, use the **flow-specifier** keyword with the previously defined flow specifier and the **session-params** keyword with the previously defined session parameter name to associate with the specified flow entry.

## Examples

The following examples show how to create a flow entry, a flow specifier, and session parameters, and how to associate the flow specifier and session parameters with the flow entry.

The following configuration shows how to create a flow entry:

```
Device(config)# metadata flow entry e1
```

The following example shows how to create a flow specifier with the source IP address, destination IP address, and source and destination port numbers:

```
Device(config)# metadata flow flow-specifier flow1
Device(config-md-flowspec)# source 209.165.201.3 source-port 1000
Device(config-md-flowspec)# destination 209.165.201.20 dest-port 1000
```

The following example shows how to create a session parameter and the associated parameters:

```
Device(config)# metadata flow session-params session1
Device(config-md-session-params)# application name webex-meeting
```

The following example shows how to associate the flow specifier and session parameters with the flow entry:

```
Device(config)# metadata flow entry e1
Device(config-md-entry)# flow-specifier flow1
Device(config-md-entry)# session-params session1
```

## Related Commands

| Command | Description |
|---|---|
| **debug metadata** | Enables debugging for metadata flow. |
| **show metadata application table** | Displays a list of metadata applications defined on a device. |
| **show metadata flow** | Displays metadata flow information. |

# mls ip pbr

To enable the multilayer switching (MLS) support for policy-routed packets, use the **mlsippbr**command in global configuration mode. To disable the MLS support for policy-routed packets, use the **no** form of this command.

**mls ip pbr [null0]**

**no mls ip pbr**

## Syntax Description

| | |
|---|---|
| **null0** | (Optional) Enables the hardware support for the interface null0 in the route-maps. |

## Command Default

MLS support for policy-routed packets is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(17d)SXB | This command was introduced on the Supervisor Engine 2 and introduced into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(18)SXE | This command was changed to support the **null0** keyword. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

**Note** Do not enable PBR and SLB on the same interface; PBR-based packets are not forwarded correctly.

When you enable the hardware-policy routing by entering the **mlsippbr** command, all policy routing occurs in the hardware and is applied to all interfaces, regardless of which interface was configured for policy routing.

Use the **null0** keyword when you have routed traffic only to enable the hardware support for the **setinterfacenull0** in the route-maps.

## Examples

This example shows how to enable the MLS support for policy-routed packets:

```
Router(config)#
mls ip pbr
```

## Related Commands

| Command | Description |
|---|---|
| **show tcam interface vlan acl** | Displays information about the interface-based TCAM. |

# mls qos global configuration mode through mpls experimental


- mls qos (global configuration mode), page 701
- mls qos (interface configuration mode), page 703
- mls qos 10g-only, page 704
- mls qos aggregate-policer, page 706
- mls qos bridged, page 710
- mls qos channel-consistency, page 711
- mls qos cos, page 712
- mls qos cos-mutation, page 715
- mls qos dscp-mutation, page 716
- mls qos exp-mutation, page 717
- mls qos loopback, page 718
- mls qos map, page 719
- mls qos map cos-dscp, page 722
- mls qos map cos-mutation, page 724
- mls qos map dscp-cos, page 726
- mls qos map dscp-exp, page 728
- mls qos map dscp-mutation, page 730
- mls qos map exp-dscp, page 732
- mls qos map exp-mutation, page 734
- mls qos map ip-prec-dscp, page 736
- mls qos map policed-dscp, page 738
- mls qos marking ignore port-trust, page 740
- mls qos marking statistics, page 741

- mls qos mpls trust experimental, page 742
- mls qos police redirected, page 744
- mls qos police serial, page 745
- mls qos protocol, page 746
- mls qos queueing-only, page 749
- mls qos queue-mode mode-dscp, page 751
- mls qos rewrite ip dscp, page 752
- mls qos statistics-export (global configuration), page 754
- mls qos statistics-export (interface configuration), page 755
- mls qos statistics-export aggregate-policer, page 757
- mls qos statistics-export class-map, page 759
- mls qos statistics-export delimiter, page 762
- mls qos statistics-export destination, page 763
- mls qos statistics-export interval, page 766
- mls qos supervisor 10g-only, page 768
- mls qos trust, page 770
- mls qos trust extend, page 773
- mls qos tunnel gre input uniform-mode, page 775
- mls qos vlan-based, page 776
- monitor pids, page 778
- mpls experimental, page 779

# mls qos (global configuration mode)

To enable the quality of service (QoS) functionality globally, use the **mlsqos**command in global configuration mode. To disable the QoS functionality globally, use the **no** form of this command.

**mls qos**

**no mls qos**

## Syntax Description

This command has no arguments or keywords.

## Command Default

QoS is globally disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

If you enable QoS globally, QoS is enabled on all interfaces with the exception of the interfaces where you disabled QoS. If you disable QoS globally, all traffic is passed in QoS pass-through mode.

In port-queueing mode, Policy Feature Card (PFC) QoS (marking and policing) is disabled, and packet type of service (ToS) and class of service (CoS) are not changed by the PFC. All queueing on rcv and xmt is based on a QoS tag in the incoming packet, which is based on the incoming CoS.

For 802.1Q or Inter-Switch Link (ISL)-encapsulated port links, queueing is based on the packet 802.1Q or ISL CoS.

For the router main interfaces or access ports, queueing is based on the configured per-port CoS (the default CoS is 0).

This command enables or disables ternary content addressable memory (TCAM) QoS on all interfaces that are set in the OFF state.

## Examples

This example shows how to enable QoS globally:

```
Router(config)# mls qos
Router(config)#
```

This example shows how to disable QoS globally on the Cisco 7600 series routers:

```
Router(config)# no mls qos
Router(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos (interface configuration mode)** | Enables the QoS functionality on an interface. |
| **show mls qos** | Displays MLS QoS information. |

# mls qos (interface configuration mode)

To enable the quality of service (QoS) functionality on an interface, use the **mlsqos**command in interface configuration command mode. To disable QoS functionality on an interface, use the **no** form of this command.

**mls qos**

**no mls qos**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Enabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is deprecated on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Although the CLI allows you to configure PFC-based QoS on the WAN ports on the OC-12 ATM OSMs and on the WAN ports on the channelized OSMs, PFC-based QoS is not supported on the WAN ports on these OSMs.

If you disable QoS globally, it is also disabled on all interfaces.

This command enables or disables TCAM QoS (classification, marking, and policing) for the interface.

## Examples

This example shows how to enable QoS on an interface:

```
Router(config-if)# mls qos
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos (global configuration mode)** | Enables the QoS functionality globally. |
| **show mls qos** | Displays MLS QoS information. |

# mls qos 10g-only

To enable quality of service (QoS) in 10g-only mode, in which only the supervisor engine's 10-Gigabit Ethernet uplink ports are used, use the **mls qos 10g-only** command in global configuration mode. To allow the use of all uplink ports, including the 1-Gigabit Ethernet ports, use the **no** form of this command.

**mls qos 10g-only**

**no mls qos 10g-only**

## Syntax Description

This command has no arguments or keywords.

## Command Default

All ports are active on the supervisor engine.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXH | This command was introduced on the Supervisor Engine 720 -10GE. |
| 15.1(1)SY | This command was modified. The mode switching requirements were changed. |

## Usage Guidelines

When you enter the **mls qos 10g-only** command, a supervisor engine with both 1-Gigabit and 10-Gigabit Ethernet uplink ports reallocates the interface queue capacity to improve the performance of its 10-Gigabit Ethernet ports. The reallocation is possible only in 10g-only mode, in which the supervisor engine's 1-Gigabit Ethernet ports are not used. In the normal mode, when all supervisor engine ports are active, the queue structure is 2q4t on receive and 1p3q4t on transmit. In 10g-only mode, the queue structure is 8q4t on receive and 1p7q4t on transmit.

**Note** To display detailed information about the queues, use the **show queueing interface** command.

When you switch between normal and 10g-only modes, any existing QoS configuration on the uplink ports is lost, and you must reconfigure QoS. In addition, service will be temporarily lost on the ports during the transition.

You must shut down the 1-Gigabit Ethernet ports before entering the **mls qos 10g-only** command. If you do not shut down the ports, the mode change will not occur.

When you switch from 10g-only mode to normal mode, you must enter the **no shutdown** command on each of the 1-Gigabit Ethernet ports to resume QoS service on those ports.

With CSCty37687, when you switch from 10g-only mode to normal mode, you must remove the trust state and the default class of service (CoS) value on the 1-Gigabit supervisor engine uplink ports.

In 10g-only mode, the 1-Gigabit Ethernet ports are visible, but they remain in an administratively down state.

The **mls qos 10g-only** command affects only active and standby supervisors, but if you have four supervisors, you must apply it to the in-chassis standby supervisors.

## Examples

The following example shows how to place the supervisor engine in the 10g-only mode:

```
Router# configure terminal
Router(config)# mls qos 10g-only
```

## Related Commands

| Command | Description |
|---|---|
| **show mls qos interface** | Displays QoS information. |
| **show queueing interface** | Displays the queueing statistics of an interface. |

# mls qos aggregate-policer

To define a named aggregate policer for use in policy maps, use the **mlsqosaggregate-policer**command in global configuration mode. To delete a named aggregate policer, use the **no** form of this command.

**mls qos aggregate-policer** *name rate-bps* [**normal-burst-bytes** [**maximum-burst-bytes**| **pir peak-rate-bps**| **action-type action**]]

**no mls qos aggregate-policer** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of the aggregate policer. See the “Usage Guidelines” section for naming conventions. |
| *rate-bps* | Maximum bits per second. Range is 32000 to 10000000000. |
| *normal-burst-bytes* | (Optional) Normal burst bytes. Range is 1000 to 31250000. |
| *maximum-burst-bytes* | (Optional) Maximum burst bytes. Range is 1000 to 31250000 (if entered, this value must be set equal to normal-burst-bytes). |
| pir peak-rate-bps | (Optional) Keyword and argument that set the peak information rate (PIR). Range is 32000 to 10000000000. Default is equal to the normal (**cir**) rate. |

| | |
|---|---|
| *action-type action* | (Optional) Action type keyword. This command may include multiple *action types* and corresponding *actions* to set several actions simultaneously. Valid values are:<br>• **conform-action** -- Keyword that specifies the action to be taken when the rate is not exceeded. Valid actions are:<br>  • **drop**-- Drops the packet.<br>  • **set-dscp-transmit***value* -- Sets the DSCP value and sends the packet. Valid entries are: 0 to 63 (differentiated code point value), af11 to af43 (match packets with specified AF DSCP), cs1 to cs7 (match packets with specified CS DSCP), default, or ef (match packets with the EF DSCP).<br>  • **set-mpls-exp-imposition-transmit***number* --Sets experimental (exp) bits at the tag imposition. Valid range is 0 to 7.<br>  • **set-prec-transmit**-- Rewrites packet precedence and sends the packet.<br>  • **transmit**--Transmits the packet. This is the default.<br>• **exceed-action** -- Keyword that specifies the action to be taken when QoS values are exceeded. Valid actions are:<br>  • **drop**-- Drops the packet. This is the default.<br>  • **policed-dscp-transmit**--Changes the DSCP value according to the policed-dscp map and sends the packet.<br>  • **transmit**--Transmits the packet.<br>• **violate-action** -- Keyword that specifies the action to be taken when QoS values are violated. Valid actions are:<br>  • **drop**-- Drops the packet.<br>  • **policed-dscp-transmit**--Changes the DSCP value according to the policed-dscp map and sends the packet.<br>  • **transmit**--Transmits the packet. |

**Command Default**

The defaults are as follows:

- **conform-action** is **transmit**
- **exceed-action** is **drop**
- **violate-action** is equal to the **exceed-action**
- **pir** *peak-rate-bps* is equal to the normal (**cir**) rate.

**Command Modes**

Global configuration

**Command History**

| Release | Modification |
|---|---|
| 12.2(14)SX | This command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.3 | This command was implemented on the Cisco 6500 and Cisco 7600. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

**Usage Guidelines**

This policer can be shared by different policy map classes and on different interfaces. The Cisco 7600 series routers supports up to 1023 aggregates and 1023 policing rules.

The **mlsqosaggregate-policer** command allows you to configure an aggregate flow and a policing rule for that aggregate. When you enter the rate and burst parameters, the range for the average rate is 32 kbps to 10 Gbps (entered as 32000 and 10000000000) and the range for the burst size is 1 KB (entered as 1000) to 31.25 MB (entered as 31250000). Modifying an existing aggregate rate limit entry causes that entry to be modified in NVRAM and in the Cisco 7600 series routers if that entry is currently being used.

**Note** Because of hardware granularity, the rate value is limited, so the burst that you configure may not be the value that is used.

Modifying an existing microflow or aggregate rate limit modifies that entry in NVRAM as well as in the Cisco 7600 series routers if it is currently being used.

When you enter the aggregate policer name, follow these naming conventions:

- Maximum of 31 characters and may include a-z, A-Z, 0-9, the dash character (-), the underscore character (_), and the period character (.).
- Must start with an alphabetic character and must be unique across all ACLs of all types.
- Case sensitive.
- Cannot be a number.

- Must not be a keyword; keywords to avoid are **all**, **default-action**, **map**, **help**, and **editbuffer.**

Aggregate policing works independently on each DFC-equipped switching module and independently on the PFC2, which supports any non-DFC-equipped switching modules. Aggregate policing does not combine flow statistics from different DFC-equipped switching modules. You can display aggregate policing statistics for each DFC-equipped switching module, PFC2, and any non-DFC-equipped switching modules that are supported by the PFC2 by entering the **showmlsqosaggregatepolicer** command.

## Examples

The following example shows how to configure a QoS aggregate policer to allow a maximum of 100000 bits per second with a normal burst byte size of 10000, to set DSCP to 48 when these rates are not exceeded, and to drop packets when these rates are exceeded:

```
Router(config)# mls qos aggregate-policer micro-one 100000 10000 conform-action
set-dscp-transmit 48 exceed-action drop
```

## Related Commands

| Command | Description |
|---|---|
| police (policy map) | Creates a per-interface policer and configures the policy-map class to use it. |
| **set ip dscp (policy-map configuration)** | Marks a packet by setting the IP DSCP in the ToS byte. |
| **show mls qos aggregate policer** | Displays information about the aggregate policer for MLS QoS. |

# mls qos bridged

To enable the microflow policing for bridged traffic on Layer 3 LAN interfaces, use the **mlsqosbridged**command in interface configuration mode. To disable microflow policing for bridged traffic, use the **no** form of this command.

**mls qos bridged**

**no mls qos bridged**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is supported on SVIs only.

On Cisco 7600 series routers that are configured with a Supervisor Engine 2, you must enable the **mlsqosbridged** command on an SVI for the microflow policing of IPv4 multicast packets if the user policy is attached to an SVI.

## Examples

This example shows how to enable the microflow policing for bridged traffic on a VLAN interface:

```
Router(config-if)# mls qos bridged
```

## Related Commands

| Command | Description |
|---|---|
| **show mls qos** | Displays MLS QoS information. |

# mls qos channel-consistency

To enable the quality of service (QoS)-port attribute checks on EtherChannel bundling, use the **mlsqoschannel-consistency** command in interface configuration mode. To disable the QoS-port attribute checks on EtherChannel bundling, use the **no** form of this command.

**mls qos channel-consistency**

**no mls qos channel-consistency**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Enabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

The **mlsqoschannel-consistency** command is supported on port channels only.

## Examples

This example shows how to enable the QoS-port attribute checks on the EtherChannel bundling:

```
Router(config-if)# mls qos channel-consistency
```

This example shows how to disable the QoS-port attribute checks on the EtherChannel bundling:

```
Router(config-if)# no mls qos channel-consistency
```

# mls qos cos

To define the default multilayer switching (MLS) class of service (CoS) value of a port or to assign the default CoS value to all incoming packets on the port, use the **mlsqoscos** command in interface configuration mode. To return to the default CoS setting, use the no form of this command.

### Cisco 3660, 3845, 6500, 7200, 7400, and 7500 Series Routers

**mls qos cos** {*cos-value*| **override**}

**no mls qos cos** {*cos-value*| **override**}

### Cisco 7600 Series Routers

**mls qos cos** *cos-value*

**no mls qos cos** *cos-value*

## Syntax Description

| | |
|---|---|
| *cos-value* | Assigns a default CoS value to a port. If the port is CoS trusted and packets are untagged, the default CoS value is used to select one output queue as an index into the CoS-to-DSCP map. The CoS range is 0 to 7. The default is 0. |
| **override** | Overrides the CoS of the incoming packets and applies the default CoS value on the port to all incoming packets. |

## Command Default

The defaults are as follows:

- Default CoS value (*cos-value)* value for a port is **0**
- CoS override is not configured .

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(6)EA2 | This command was introduced. It replaced the **switchportpriority**command. |
| 12.2(14)SX | Support for this command was introduced on the Cisco 7600 series router. |
| 12.2(15)ZJ | This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |

| Release | Modification |
|---|---|
| 12.2(17d)SXB | This command was implemented on the Cisco 7600 series router and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

**Cisco 3660, 3845, 6500, 7200, 7400, and 7500 Series Routers**

You can assign the default CoS and differentiated services code point (DSCP) value to all packets entering a port if the port has been configured by use of the **override** keyword.

Use the **override** keyword when all incoming packets on certain ports deserve a higher or lower priority than packets the enter from other ports. Even if a port was previously set to trust DSCP or CoS, this command overrides that trust state, and all the CoS values on the incoming packets are changed to the default CoS value that is configured with the **mlsqoscos**command. If an incoming packet is tagged, the CoS value of the packet is modified at the ingress port. It is changed to the default CoS of that port.

Use the **showmlsqosinterface**privileged EXEC command to verify your settings.

**Cisco 7600 Series Routers**

CoS values are configurable on physical LAN ports only.

On Cisco 7600 series routers that are configured with a Supervisor Engine 2, the following restrictions apply:

- This command is not supported on any WAN interface on the Optical Service Modules (OSMs).
- This command is not supported on 4-port Gigabit Ethernet WAN ports.

## Examples

Cisco 3660, 3845, 6500, 7200, 7400, and 7500 Series Routers

The following example shows how to assign 4 as the default port CoS:

```
Router(config)# interface gigabitethernet
0/1
Router(config-if)# mls qos trust cos
Router(config-if)# mls qos cos 4
```

The following example shows how to assign 4 as the default port CoS value for all packets the enter the port:

```
Router(config)# interface gigabitethernet
0/1
Router(config-if)# mls qos cos 4
Router(config-if)# mls qos cos override
```

## Examples

The following example shows how to configure the default QoS CoS value as 6:

```
Router(config)# interface gigabitethernet
0/1
Router(config-if)# mls qos cos 6
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos map** | Defines the CoS-to-DSCP map or the DSCP-to-CoS map. |
| **mls qos trust** | Configures the port trust state. |
| **show interface fax/y switchport** | Displays switch port interfaces. |
| **show mls qos** | Displays MLS QoS information. |
| **show mls qos interface** | Displays QoS information. |

# mls qos cos-mutation

To attach an ingress-class-of-service (CoS) mutation map to the interface, use the **mlsqoscos-mutation**command in interface configuration mode. To remove the ingress-CoS mutation map from the interface, use the **no** form of this command.

**mls qos cos-mutation** *cos-mutation-table-name*

**no mls qos cos-mutation**

## Syntax Description

| | |
|---|---|
| *cos-mutation-table-name* | Name of the ingress-CoS mutation table. |

## Command Default

No ingress-CoS mutation table is defined.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(17b)SXA | This command was introduced on the Supervisor Engine 720. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

## Examples

This example shows how to attach the ingress-CoS mutation map named mutemap2:

```
Router(config-if)# mls qos cos-mutation mutemap2
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos map cos-mutation** | Maps a packet's CoS to a new CoS value. |
| **show mls qos** | Displays MLS QoS information. |

# mls qos dscp-mutation

To attach an egress-differentiated-services-code-point (DSCP) mutation map to the interface, use the **mlsqosdscp-mutation**command in interface configuration mode. To remove the egress-DSCP mutation map from the interface, use the **no** form of this command.

**mls qos dscp-mutation** *dscp-mutation-table-name*

**no mls qos dscp-mutation**

## Syntax Description

| | |
|---|---|
| *dscp-mutation-table-name* | Name of the egress-DSCP mutation table. |

## Command Default

No table is defined.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

## Examples

This example shows how to attach the egress-DSCP mutation map named mutemap1:

```
Router(config-if)# mls qos dscp-mutation mutemap1
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos map dscp-mutation** | Defines a named DSCP mutation map. |
| **show mls qos** | Displays MLS QoS information. |

# mls qos exp-mutation

To attach an egress-EXP mutation map to the interface in the interface configuration command mode, use the **mlsqosexp-mutation**command. Use the **no** form of this command to remove the egress-EXP mutation map from the interface.

**mls qos exp-mutation** *exp-mutation-table-name*

**no mls qos exp-mutation**

## Syntax Description

| | |
|---|---|
| *exp-mutation-table-name* | Name of the egress-EXP mutation table. |

## Command Default

No table is defined.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(17a)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is supported in PFC3BXL or PFC3B mode only.

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

## Examples

This example shows how to attach the egress-exp mutation map named mutemap2:

```
Router(config-if)# mls qos exp-mutation mutemap2
Router(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos map dscp-mutation** | Defines a named DSCP mutation map. |
| **show mls qos mpls** | Displays an interface summary for MPLS QoS classes in the policy maps. |

# mls qos loopback

To remove a router port from the Switched Virtual Interface (SVI) flood for VLANs that are carried through by the loopback cable, use the**mlsqosloopback** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

**mls qos loopback**

**no mls qos loopback**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(17a)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

With **mlsqosloopback** applied at the interface, the packets are not forwarded to the destination.

Before you enter the **mlsqosloopback** command, you must specify a MAC address for the Optical Services Modules (OSM) interface. The MAC address must be different from the LAN router MAC address that is used in PFC2 hardware switching.

## Examples

This example shows how to prevent packets from being forwarded to the destination:

```
Router(config-if)# mls qos loopback
```

# mls qos map

To define the multilayer switching (MLS) class of service (CoS)-to-differentiated services code point (DSCP) map or DSCP-to-CoS map, use the **mlsqosmap** command in global configuration mode. To return to the default map, use the no form of this command.

**mls qos map** {**cos-dscp** *dscp1...dscp8*| **dscp-cos** *dscp-list* **to** *cos*}

**no mls qos map** {**cos-dscp**| **dscp-cos**}

## Syntax Description

| | |
|---|---|
| **cos-dscp** *dscp1...dscp8* | Defines the CoS-to-DSCP map.<br>For *dscp1...dscp8*, enter eight DSCP values that correspond to CoS values 0 to 7. Separate consecutive DSCP values from each other with a space.<br>The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56. |
| **dscp-cos** *dscp-list* **to** *cos* | Defines the DSCP-to-CoS map.<br>For *dscp-list*, enter up to 13 DSCP values separated by spaces. Then enter the **to** keyword. The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56.<br>For *cos*, enter the CoS value to which the DSCP value or values correspond. Range: 0 to 7. |

## Command Default

The table below shows the default CoS-to-DSCP map.

***Table 16: Default CoS-to-DSCP Map***

| **CoS Value** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
|---|---|---|---|---|---|---|---|---|
| **DSCP Value** | 0 | 8 | 16 | 26 | 32 | 46 | 48 | 56 |

The table below shows the default DSCP-to-CoS map.

*Table 17: Default DSCP-to-CoS Map*

| DSCP Values | 0 | 8, 10 | 16, 18 | 24, 26 | 32, 34 | 40, 46 | 48 | 56 |
|---|---|---|---|---|---|---|---|---|
| CoS Value | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.1(6)EA2 | This command was introduced. |
| 12.2(15)ZJ | This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

All of the CoS-to-DSCP and DSCP-to-CoS maps are globally defined. You apply all maps to all ports.

If you enter the **mlsqostrustcos**command, the default CoS-to-DSCP map is applied.

If you enter the **mlsqostrustdscp** command, the default DSCP-to-CoS map is applied.

After a default map is applied, you can define the CoS-to-DSCP or DSCP-to-CoS map by entering consecutive **mlsqosmap** commands.

If the **mlsqostrustdscp**command is entered and a packet with an untrusted DSCP value is at an ingress port, the packet CoS value is set to 0.

Use the **showmlsqosmaps**privileged EXEC command to verify your settings.

## Examples

The following example shows how to define the DSCP-to-CoS map. DSCP values 16, 18, 24, and 26 are mapped to CoS 1. DSCP values 0, 8, and 10 are mapped to CoS 0.

```
Router# configure terminal
Router(config)# mls qos map dscp-cos 16 18 24 26 to 1
Router(config)# mls qos map dscp-cos 0 8 10 to 0
```

The following example shows how to define the CoS-to-DSCP map. CoS values 0 to 7 are mapped to DSCP values 8, 8, 8, 8, 24, 32, 56, and 56.

```
R
outer# configure terminal
Router(config)# mls qos map cos-dscp 8 8 8 8 24 32 56 56
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos cos** | Defines the default CoS value of a port or assigns the default CoS to all incoming packets on the port. |
| **mls qos trust** | Configures the port trust state. |
| **show mls qos maps** | Displays QoS mapping information. |

# mls qos map cos-dscp

To define the ingress Class of Service (CoS)-to-differentiated services code point (DSCP) map for trusted interfaces, use the **mlsqosmapcos-dscp**command in global configuration mode. Use the **no** form of this command to remove a prior entry.

**mls qos map cos-dscp** *dscp1 ...dscp8*

**no mls qos map cos-dscp**

## Syntax Description

| | |
|---|---|
| *dscp1...dscp8* | Defines the CoS-to-DSCP map.<br>For *dscp1...dscp8*, enter eight DSCP values that correspond to CoS values 0 to 7. Separate consecutive DSCP values from each other with a space.<br>The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56. |

## Command Default

The default CoS-to-DSCP configuration is listed in the table below.

***Table 18: CoS-to-DSCP Default Map***

| CoS | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| DSCP | 0 | 8 | 16 | 24 | 32 | 40 | 48 | 56 |

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(6)EA2 | This command was introduced. |
| 12.2(15)ZJ | This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

All of the CoS-to-DSCP and DSCP-to-CoS maps are globally defined. You apply all maps to all ports.

If you enter the **mlsqostrustcos**command, the default CoS-to-DSCP map is applied.

If you enter the **mlsqostrustdscp** command, the default DSCP-to-CoS map is applied.

After a default map is applied, you can define the CoS-to-DSCP or DSCP-to-CoS map by entering consecutive **mlsqosmap** commands.

If the **mlsqostrustdscp**command is entered and a packet with an untrusted DSCP value is at an ingress port, the packet CoS value is set to 0.

Use the **showmlsqosmaps**privileged EXEC command to verify your settings.

## Examples

The following example shows how to define the CoS-to-DSCP map. CoS values 0 to 7 are mapped to DSCP values 8, 8, 8, 8, 24, 32, 56, and 56.

```
Router#
 configure terminal
Router(config)# mls qos map cos-dscp 8 8 8 8 24 32 56 56
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos map dscp-cos** | Defines an egress DSCP-to-CoS map. |
| **mls qos map ip-prec-dscp** | Defines an ingress-IP precedence-to-DSCP map for trusted interfaces. |
| **mls qos map policed-dscp** | Sets the mapping of policed DSCP values to marked-down DSCP values. |
| **show mls qos maps** | Displays information about the QoS-map configuration and runtime-version. |

# mls qos map cos-mutation

To map a class of service (CoS) value to a new CoS value for a packet, use the **mlsqosmapcos-mutation**command in the global configuration mode. To remove the map, use the **no** form of this command

**mls qos map cos-mutation** *name mutated-cos1 mutated-cos2 mutated-cos3 mutated-cos4 mutated-cos5 mutated-cos6 mutated-cos7 mutated-cos8*

**no mls qos map cos-mutation** *name*

## Syntax Description

| | |
|---|---|
| *name* | Name of the CoS map. |
| *mutated-cos1 ... mutated-cos8* | Eight CoS out values, separated by spaces; valid values are from 0 to 7. See the "Usage Guidelines" section for additional information. |

## Command Default

If the CoS-to-CoS mutation map is not configured, the default CoS-to-CoS mutation mapping is listed in the table below.

***Table 19: CoS-to-CoS Default Map***

| **CoS-in** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
|---|---|---|---|---|---|---|---|---|
| **CoS-out** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(17b)SXA | This command was introduced on the Supervisor Engine 720. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command is not supported on the Catalyst 6500 series switches and the Cisco 7600 series routers that are configured with a Supervisor Engine 2.

This command is supported on the Catalyst 6500 series switches and the Cisco 7600 series routers that are configured with the following modules only:

- WS-X6704-10GE
- WS-X6724-SFP
- WS-X6748-GE-TX

CoS mutation is not supported on non-802.1Q tunnel ports.

When you enter the **mlsqosmapcos-mutation**command, you are configuring the mutated-CoS values map to sequential ingress-CoS numbers. For example, by entering the **mlsqosmapcos-mutation23456701** command, you configure this map:

| **CoS-in** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
|---|---|---|---|---|---|---|---|---|
| **CoS-out** | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 |

Separate the eight CoS values by a space.

After you define the map in global configuration mode, you can attach the map to a port.

If QoS is disabled, the port is not in a trust CoS mode, and the port is not in 802.1Q tunneling mode. The changes appear once you put the port into trust CoS mode and the port is configured as an 802.1Q tunnel port.

Release 12.2(17b)SXA and later releases support ingress-CoS mutation on 802.1Q tunnel ports and is on a per-port group basis only.

To avoid ingress-CoS mutation configuration failures, only create EtherChannels where all member ports support ingress-CoS mutation or where no member ports support ingress-CoS mutation. Do not create EtherChannels with mixed support for ingress-CoS mutation.

If you configure ingress-CoS mutation on a port that is a member of an EtherChannel, the ingress-CoS mutation is applied to the port-channel interface.

You can configure ingress-CoS mutation on port-channel interfaces.

## Examples

This example shows how to define a CoS-to-CoS map:

```
Router(config)# mls qos map cos-mutation test-map 1 2 3 4 5 6 7 1
```

## Related Commands

| Command | Description |
|---|---|
| **show mls qos maps** | Displays information about the QoS-map configuration and runtime-version. |

# mls qos map dscp-cos

To define an egress differentiated services code point (DSCP)-to-class of service (CoS) map, use the **mlsqosmapdscp-cos** command in global configuration mode. To remove a prior entry, use the **no** form of this command.

**mls qos map dscp-cos** *dscp-values* **to** *cos-values*

**no mls qos map dscp-cos**

## Syntax Description

| | |
|---|---|
| *dscp-values* **to** *cos-values* | Defines the DSCP-to-CoS map.<br>For *dscp-list*, enter up to 13 DSCP values separated by spaces. Then enter the **to** keyword. The supported DSCP values are 0, 8, 10, 16, 18, 24, 26, 32, 34, 40, 46, 48, and 56.<br>For *cos*, enter the CoS value to which the DSCP value or values correspond. Range: 0 to 7. |

## Command Default

The default DSCP-to-CoS map is listed in the table below.

***Table 20: DSCP-to-CoS Default Map***

| DSCP | 0-7 | 8-15 | 16-23 | 24-31 | 32-39 | 40-47 | 48-55 | 56-63 |
|---|---|---|---|---|---|---|---|---|
| CoS | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(6)EA2 | This command was introduced. |
| 12.2(15)ZJ | This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |

| Release | Modification |
|---|---|
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

The DSCP-to-CoS map is used to map the final DSCP classification to a final CoS. This final map determines the output queue and threshold to which the packet is assigned. The CoS map is written into the Inter-Switch Link (ISL) header or 802.1Q tag of the transmitted packet on trunk interfaces and contains a table of 64 DSCP values and the corresponding CoS values. The Catalyst 6500 series switch and the Cisco 7600 series router have one map.

All of the CoS-to-DSCP and DSCP-to-CoS maps are globally defined. You apply all maps to all ports.

If you enter the **mlsqostrustcos**command, the default CoS-to-DSCP map is applied.

If you enter the **mlsqostrustdscp** command, the default DSCP-to-CoS map is applied.

After a default map is applied, you can define the CoS-to-DSCP or DSCP-to-CoS map by entering consecutive **mlsqosmap** commands.

If the **mlsqostrustdscp**command is entered and a packet with an untrusted DSCP value is at an ingress port, the packet CoS value is set to 0.

Use the **showmlsqosmaps**privileged EXEC command to verify your settings.

## Examples

The following example shows how to define the DSCP-to-CoS map. DSCP values 16, 18, 24, and 26 are mapped to CoS 1. DSCP values 0, 8, and 10 are mapped to CoS 0.

```
Router# configure terminal
Router(config)# mls qos map dscp-cos 16 18 24 26 to 1
Router(config)# mls qos map dscp-cos 0 8 10 to 0
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos map cos-dscp** | Defines the ingress CoS-to-DSCP map for trusted interfaces. |
| **show mls qos maps** | Displays information about the QoS-map configuration and runtime-version. |

# mls qos map dscp-exp

To map the final differentiated services code point (DSCP) value to the final experimental (EXP) value, use the **mlsqosmapdscp-exp** command in global configuration mode. To remove a prior entry, use the **no** form of this command.

**mls qos map dscp-exp** *dscp-values* **to** *exp-values*

**no mls qos map dscp-exp**

## Syntax Description

| | |
|---|---|
| *dscp-values* | DSCP values; valid values are from 0 to 63. |
| **to** | Defines mapping. |
| *exp-values* | EXP values; valid values are from 0 to 7. |

## Command Default

The default DSCP-to-EXP map is listed in the table below.

***Table 21: DSCP-to-EXP Default Map***

| DSCP | 0-7 | 8-15 | 16-23 | 24-31 | 32-39 | 40-47 | 48-55 | 56-63 |
|---|---|---|---|---|---|---|---|---|
| EXP | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.2(17a)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is supported in PFC3BXL or PFC3B mode only.

The DSCP-to-EXP map is used to map the final DSCP value to a final EXP value. This final map determines the output queue and threshold to which the packet is assigned. The EXP map contains a table of 64 DSCP values and the corresponding EXP values. The Catalyst 6500 series switch and the Cisco 7600 series router have one map.

You can enter up to eight DSCP values separated by a space. You can enter up to eight EXP values separated by a space.

## Examples

This example shows how to configure the final DSCP value to a final EXP value:

```
Router(config)# mls qos map dscp-exp 20 25 to 3
```

## Related Commands

| Command | Description |
|---|---|
| **show mls qos maps** | Displays information about the QoS-map configuration and runtime-version. |

# mls qos map dscp-mutation

To define a named differentiated services code point (DSCP) mutation map, use the **mlsqosmapdscp-mutation** command in global configuration mode. To return to the default mapping, use the **no** form of this command.

**mls qos map dscp-mutation** *map-name input-dscp1* [*input-dscp2* [*input-dscp3* [**i** *nput-dscp4* [*input-dscp5* [*input-dscp6* [*input-dscp7* [ *input-dscp8* ]]]]]]] **to** *output-dscp*

**no mls qos map dscp-mutation** *map-name*

## Syntax Description

| | |
|---|---|
| *map-name* | Name of the DSCP mutation map . |
| *input-dscp#* | Internal DSCP value; valid values are from 0 to 63. See the “Usage Guidelines” section for additional information. |
| **to** | Defines mapping. |
| *output-dscp* | Egress DSCP value; valid values are from 0 to 63. |

## Command Default

*output-dscp* equals *input-dscp*.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is not supported on the Catalyst 6500 series switches and the Cisco 7600 series routers that are configured with a Supervisor Engine 2.

When configuring a named DSCP mutation map, note the following:

- You can enter up to eight input DSCP values that map to a mutated DSCP value.
- You can enter multiple commands to map additional DSCP values to a mutated DSCP value.

- You can enter a separate command for each mutated DSCP value.

You can configure 15 egress-DSCP mutation maps to mutate the internal DSCP value before it is written as the egress-DSCP value. You can attach egress-DSCP mutation maps to any interface that Policy Feature Card (PFC) QoS supports.

PFC QoS derives the egress-class-of-service (CoS) value from the internal DSCP value. If you configure egress-DSCP mutation, PFC QoS does not derive the egress-CoS value from the mutated DSCP value.

## Examples

**This example shows how to map DSCP 30 to mutated DSCP value 8:**

```
Router(config)# mls qos map dscp-mutation mutemap1 30 to 8
```

## Related Commands

| Command | Description |
|---|---|
| **show mls qos maps** | Displays information about the QoS-map configuration and runtime-version. |

# mls qos map exp-dscp

To define the ingress Experimental (EXP) value to the internal differentiated services code point (DSCP) map, use the **mlsqosmapexp-dscp** command in global configuration mode. To return to the default mapping, use the **no** form of this command.

**mls qos map exp-dscp** *dscp-values*

**no mls qos map exp-dscp**

## Syntax Description

| | |
|---|---|
| *dscp-values* | D efines the ingress EXP value to the internal DSCP map . Range: 0 to 63. |

## Command Default

The default EXP-to-DSCP map is listed in the table below.

***Table 22: EXP-to-DSCP Default Map***

| **EXP** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
|---|---|---|---|---|---|---|---|---|
| **DSCP** | 0 | 8 | 16 | 24 | 32 | 40 | 48 | 56 |

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.2(17a)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is supported in PFC3BXL or PFC3B mode only.

The DSCP in these maps refers to the internal DSCP, not the packet DSCP.

The EXP-to-DSCP map is used to map the received EXP value to the internal DSCP map. This final map determines the output queue and threshold to which the packet is assigned. The EXP map contains a table of

64 DSCP values and the corresponding EXP values. The Catalyst 6500 series switch and the Cisco 7600 series router have one map.

You can enter up to eight DSCP values separated by a space.

## Examples

This example shows how to configure the received EXP value to an internal DSCP value:

```
Router(config)# mls qos map exp-dscp 20 25 30 31 32 32 33 34
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos map exp-mutation** | Maps a packet's EXP to a new EXP value. |
| **show mls qos mpls** | Displays an interface summary for MPLS QoS classes in the policy maps. |

# mls qos map exp-mutation

To map the Experimental (EXP) value of a packet to a new EXP value, use the **mlsqosmapexp-mutation** command in global configuration mode. To return to the default mapping, use the **no** form of this command.

**mls qos map exp-mutation** *map-name mutated-exp1 mutated-exp2 mutated-exp3 mutated-exp4 mutated-exp5 mutated-exp6 mutated-exp7 mutated-exp8*

**no mls qos map exp-mutation** *map-name*

## Syntax Description

| | |
|---|---|
| *map-name* | Name of the EXP-mutation map . |
| *mutated-exp#* | Eight EXP values, separated by spaces ; valid values are from 0 to 7. See the “Usage Guidelines” section for additional information. |

## Command Default

If the EXP-to-EXP mutation map is not configured, the default EXP-to-EXP mutation mapping is listed in the table below.

***Table 23: EXP-to-EXP Mutation Default Map***

| **EXP-in** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
|---|---|---|---|---|---|---|---|---|
| **EXP-out** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.2(17a)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is not supported on the Catalyst 6500 series switch and the Cisco 7600 series router that are configured with a Supervisor Engine 2.

This command is supported in PFC3BXL or PFC3B mode only.

When you enter the**mlsqosmapexp-mutation**command, you are configuring the mutated EXP values map to the sequential EXP numbers. For example, by entering the **mlsqosmapexp-mutation23456701** command, you configure the map as shown in the table below:

***Table 24: Mutated EXP Values Mapped to Sequential EXP Values***

| **EXP-in** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
|---|---|---|---|---|---|---|---|---|
| **EXP-out** | 2 | 3 | 4 | 5 | 6 | 7 | 0 | 1 |

Separate the eight EXP values by a space.

After you define the map in global configuration mode, you can attach the map to a port.

You can configure 15 ingress-EXP mutation maps to mutate the internal EXP value before it is written as the ingress-EXP value. You can attach ingress-EXP mutation maps to any interface that Policy Feature Card (PFC) quality of service (QoS) supports.

The PFC QoS derives the egress EXP value from the internal differentiated services code point (DSCP) value. If you configure ingress-EXP mutation, PFC QoS does not derive the ingress-EXP value from the mutated EXP value.

## Examples

**This example shows how to map** the EXP value of a packet to a new EXP value**:**

```
Router(config)# mls qos map exp-mutation mutemap1 1 2 3 4 5 6 7 0
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos map exp-dscp** | Defines the ingress EXP value to the internal DSCP map. |
| **show mls qos mpls** | Displays an interface summary for MPLS QoS classes in the policy maps. |

# mls qos map ip-prec-dscp

To define an ingress-IP precedence-to-differentiated-services-code-point (DSCP) map for trusted interfaces, use the **mlsqosmapip-prec-dscp**command in global configuration mode. To remove a prior entry, use the **no** form of this command.

**mls qos map ip-prec-dscp** *dscp-values*

**no mls qos map ip-prec-dscp**

## Syntax Description

| | |
|---|---|
| *dscp-values* | DSCP values corresponding to IP precedence value s 0 to 7; valid values are from 0 to 63. |

## Command Default

The default IP precedence-to-DSCP configuration is listed in the table below.

***Table 25: IP Precedence-to-DSCP Default Map***

| IP-Precedence | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| **DSCP** | 0 | 8 | 16 | 24 | 32 | 40 | 48 | 56 |

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

Use the **mlsqosmapip-prec-dscp** command to map the IP precedence of IP packets arriving on trusted interfaces (or flows) to a DSCP when the trust type is trust-ipprec.

You can enter up to eight DSCP values separated by a space.

This map is a table of eight precedence values (0 through 7) and their corresponding DSCP values. The Catalyst 6500 series switch and the Cisco 7600 series router have one map. The IP precedence values are as follows:

- network 7
- internet 6
- critical 5
- flash-override 4
- flash 3
- immediate 2
- priority 1
- routine 0

## Examples

This example shows how to configure the ingress-IP precedence-to-DSCP mapping for trusted interfaces:

```
Router(config)# mls qos map ip-prec-dscp 20 30 1 43 63 12 13 8
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos map cos-dscp** | Defines the ingress CoS-to-DSCP map for trusted interfaces. |
| **mls qos map dscp-cos** | Defines an egress DSCP-to-CoS map. |
| **mls qos map policed-dscp** | Sets the mapping of policed DSCP values to marked-down DSCP values. |
| **show mls qos maps** | Displays information about the QoS-map configuration and runtime-version. |

# mls qos map policed-dscp

To set the mapping of policed differentiated services code point (DSCP) values to marked-down DSCP values, use the **mlsqosmappoliced-dscp**command in global configuration mode. To remove a prior entry, use the **no** form of this command.

**mls qos map policed-dscp** *dscp-list* **to** *policed-dscp*

**no mls qos map policed-dscp**

### Catalyst 6500 Series Switches and Cisco 7600 Series Routers

**mls qos map policed-dscp** {**normal-burst**| **max-burst**} *dscp1* [*dscp2* [*dscp3* [*dscp4* [*dscp5* [*dscp6* [*dscp7* [ *dscp8* ]]]]]]] **to** *policed-dscp*

**no mls qos map policed-dscp**

## Syntax Description

| | |
|---|---|
| normal-burst | Configures the markdown map used by the **exceed-actionpoliced-dscp-transmit** keywords. |
| max-burst | Configures the markdown map used by the **violate-actionpoliced-dscp-transmit** keywords. |
| *dscp1* | DSCP value. Range: 0 to 63. |
| *dscp2* through *dscp8* | (Optional) DSCP values. Range: 0 to 63. |
| **to** | Defines mapping. |
| *policed-dscp* | Policed-to-DSCP values; valid values are from 0 to 63. |

## Command Default

No marked-down values are configured.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |

| Release | Modification |
|---|---|
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

The DSCP-to-policed-DSCP map determines the marked-down DSCP value that is applied to out-of-profile flows. The Catalyst 6500 series switch and the Cisco 7600 series router have one map.

You can enter up to eight DSCP values separated by a space.

You can enter up to eight policed DSCP values separated by a space.

**Note** To avoid out-of-sequence packets, configure the DSCP-to-policed-DSCP map so that marked-down packets remain in the same queue as the in-profile traffic.

## Examples

This example shows how to map multiple DSCPs to a single policed-DSCP value:

```
Router(config)# mls qos map policed-dscp 20 25 43 to 4
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos map cos-dscp** | Defines the ingress CoS-to-DSCP map for trusted interfaces. |
| **mls qos map dscp-cos** | Defines an egress DSCP-to-CoS map. |
| **mls qos map in-prec-dscp** | Defines an ingress-IP precedence-to-DSCP map for trusted interfaces. |
| **show mls qos** | Displays MLS QoS information. |

# mls qos marking ignore port-trust

To mark packets even if the interface is trusted, use the **mlsqosmarkingignoreport-trust**command in global configuration mode. To return to the default settings, use the **no** form of this command.

**mls qos marking ignore port-trust**

**no mls qos marking ignore port-trust**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Port trust is enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXF5 | This command was introduced. |

## Usage Guidelines

Use the **mlsqosmarkingignoreport-trust**command to mark packets even if the interface is trusted.

## Examples

This example shows how to mark packets even if the interface is trusted:

```
mls qos marking ignore port-trust
```

This example shows how to re-enable port trust:

```
no mls qos marking ignore port-trust
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos trust** | Sets the trusted state of an interface. |

# mls qos marking statistics

To disable allocation of the policer-traffic class identification with set actions, use the **mlsqosmarkingstatistics** command in global configuration mode. To return to the default settings, use the **no** form of this command.

**mls qos marking statistics**

**no mls qos marking statistics**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Enabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(17a)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(18)SXE | This command was changed to add the collection of statistics for a policy that sets a trust state. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Use the **showpolicy-mapinterface** command to display policy-map statistics.

## Examples

This example shows how to disable allocation of the policer-traffic class identification with set actions:

```
Router(config)# mls qos marking statistics
```

This example shows how to allow allocation of the policer-traffic class identification with set actions:

```
Router(config)# no mls qos marking statistics
```

## Related Commands

| Command | Description |
|---|---|
| **show policy-map interface** | Displays the statistics and the configurations of the input and output policies that are attached to an interface. |

# mls qos mpls trust experimental

To set the trusted state of Multiprotocol Label Switching (MPLS) packets only, use the **mlsqosmplstrustexperimental** command in interface configuration mode. To set the trusted state of MPLS packets to untrusted, use the **no** form of this command.

**mls qos mpls trust experimental**

**no mls qos mpls trust experimental**

## Syntax Description

This command has no arguments or keywords.

## Command Default

With the trusted state enabled, the defaults are as follows:

- Untrusted--The packets are marked to 0 or by policy.
- trust-cos.

With the trusted state disabled, the defaults are as follows:

- trust-exp--The port or policy trust state is ignored.
- The packets are marked by policy.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXF2 | This command was introduced on the Supervisor Engine 720. |

## Usage Guidelines

You can enter the **mlsqosmplstrustexperimental**command to treat MPLS packets as other Layer 2 packets for class of service (CoS) and egress queueing purposes (for example, to apply port or policy trust). All trusted cases (trust CoS/IP/Differentiated Services Code Point (DSCP)) are treated as trust-cos.

Class of Service (CoS) refers to three bits in either an ISL header or an 802.1Q header that are used to indicate the priority of the Ethernet frame as it passes through a switched network. The CoS bits in the 802.1Q header are commonly referred to as the 802.1p bits. To maintain QoS when a packet traverses both Layer 2 and Layer 3 domain, the ToS and CoS values can be mapped to each other.

## Examples

This example shows how to set the trusted state of MPLS packets to trust-cos:

```
Router(config-if)# mls qos mpls trust experimental
```

This example shows how to set the trusted state of MPLS packets to untrusted:

```
Router(config-if)# no mls qos mpls trust experimental
```

## Related Commands

| Command | Description |
|---|---|
| **show mls qos mpls** | Displays an interface summary for MPLS QoS classes in the policy maps. |

# mls qos police redirected

To turn on access control list (ACL)-redirected packet policing, use the **mlsqospoliceredirected**command in global configuration mode. To turn off ACL-redirected packet policing, use the **no** form of this command.

**mls qos police redirected**

**no mls qos police redirected**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Enabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(17b)SXA | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is supported on PFC3BXL or PFC3B mode only. With Release 12.2(17b)SXA, enter the **showplatformearl-mode** command to display the PFC3 mode.

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Use the **nomlsqospoliceredirected** command whenever you require NetFlow Data Export (NDE) accuracy (if you do not require QoS-redirected packets).

## Examples

This example shows how to turn on the ACL-redirected packet policing:

```
Router(config)# mls qos police redirected
```

This example shows how to turn off the ACL-redirected packet policing:

```
Router(config)# no mls qos police redirected
```

## Related Commands

| Command | Description |
|---|---|
| **show platform earl-mode** | Displays platform information. |

# mls qos police serial

To enable serial mode for ingress and egress policers on the PFC3C or PFC3CXL, use the **mlsqospoliceserial** command in global configuration mode. To reset the policing mode to parallel, use the **no** form of the command.

**mls qos police serial**

**no mls qos police serial**

## Syntax Description

This command has no arguments or keywords.

## Command Default

This command is disabled by default.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRB | This command was introduced. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

You can use the **mlsqospoliceserial** command to configure the PFC3C or PFC3CXL ingress and egress policers to operate independently of each other (in *serial mode* ). Normally, ingress and egress policers operate in parallel mode, where action by one policer causes a corresponding action in the other. For example, if the egress policer drops a packet, the ingress policer does not count the packet either. In serial mode, however, action by one policer does not cause a corresponding action in the other.

**Note** This command does not affect marking using policers.

## Examples

The following command example shows how to enable serial policing mode on the PFC3C or PFC3CXL:

```
Router(config)# mls qos police serial
```

# mls qos protocol

To define routing-protocol packet policing, use the mls qos protocol command in global configuration mode. To return to the default settings, use the **no** form of this command.

**mls qos protocol** *protocol-name* {**pass-through**| **police** *rate* [ *burst* ]| **precedence** *value* [**police** *rate* [ *burst* ]]}

**no mls qos protocol** *protocol-name*

## Syntax Description

| | |
|---|---|
| *protocol-name* | Protocol name. Valid values include the following:<br>• **arp**<br>• **bfd-ctrl**<br>• **bfd-echo**<br>• **bgp**<br>• **eigrp**<br>• **glbp**<br>• **igrp**<br>• **isis**<br>• **ldp**<br>• **nd**<br>• **ospf**<br>• **rip**<br>• **vrrp** |
| **pass-through** | Specifies pass-through mode. |
| **police** *rate* | Specifies the maximum bits per second (bps) to be policed. Valid values are from 32000 to 4000000000 . |
| *burst* | (Optional) Normal burst bytes. Valid values are from 1000 to 31250000. |
| **precedence** *value* | Specifies the IP-precedence value of the protocol packets to rewrite. Valid values are fro m 0 to 7. |

## Command Default

The defaults are as follows:

- *burst* is 1000 bits per second.

- If quality of service (QoS) is enabled, the differentiated services code point (DSCP) value is rewritten to zero.
- If QoS is disabled, the port is in a pass-through mode (no marking or policing is applied).

**Command Modes**

Global configuration (config)

**Command History**

| Release | Modification |
|---|---|
| 12.2(17a)SX | This command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was modified to support the ISIS protocol. |
| 12.2(18)SXE | This command was modified as follows on the Supervisor Engine 720 only:<br>• Support for the marking of global **mlsqosprotocol** QoS policies was added.<br>• Support for this command was introduced on the Supervisor Engine 2 but does not support Address Resolution Protocol (ARP), Integrated Intermediate System-to-Intermediate System (ISIS), or Enhanced Interior Gateway Routing Protocol (EIGRP).<br>• The **nd** keyword was added to support neighbor discovery protocol packets.<br>• The **igrp** keyword was removed. |
| 12.2(18)SXF | The **no** form of this command was modified to remove the arguments and keywords. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SRE1 | This command was modified. The **bfd-ctrl**, **bfd-echo**, **glbp**, and **vrrp** keywords were added. |

**Usage Guidelines**

This command does not support ARP, ISIS, or EIGRP on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

If you enter the **precedence***value*keyword and arguments without entering the **police***rateburst*keyword and arguments, only the packets from an untrusted port are marked.

You can make the protocol packets avoid the per-interface policy maps by entering the **police***rate*, **pass-through**, or **precedence***value* keywords and arguments.

The **mlsqosprotocol** command allows you to define the routing-protocol packet policing as follows:

- When you specify the **pass-through** mode, the DSCP value does not change and is not policed.
- When you set the **police***rate*, the DSCP value does not change and is policed.

- When you specify the **precedence***value*, the DSCP value changes for the packets that come from an untrusted port, the class of service (CoS) value that is based on DSCP-to-CoS map changes, and the traffic is not policed.
- When you specify the **precedence***value*and the **police***rate*, the DSCP value changes, the CoS value that is based on DSCP-to-CoS map changes, and the DSCP value is policed. In this case, the DSCP value changes are based on the trust state of the port; the DSCP value is changed only for the packets that come from an untrusted port.
- If you do not enter a **precedence***value*, the DSCP value is based on whether or not you have enabled multilayer switching (MLS) QoS as follows:
  - If you enabled MLS QoS and the port is untrusted, the internal DSCP value is overwritten to zero.
  - If you enabled MLS QoS and the port is trusted, then the incoming DSCP value is maintained.

You can make the protocol packets avoid policing completely if you choose the pass-through mode. If the police mode is chosen, the committed information rate (CIR) specified is the rate that is used to police all the specified protocol's packets, both entering or leaving the Cisco 7600 series router.

To protect the system by ARP broadcast, you can enter the **mlsqosprotocolarppolice***bps* command.

## Examples

This example shows how to define the routing-protocol packet policing:

```
Router(config)# mls qos protocol arp police 43000
```

This example shows how to avoid policing completely:

```
Router(config)# mls qos protocol arp pass-through
```

This example shows how to define the IP-precedence value of the protocol packets to rewrite:

```
Router(config)# mls qos protocol bgp precedence 4
```

This example shows how to define the IP-precedence value of the protocol packets to rewrite and police the DSCP value:

```
Router(config)# mls qos protocol bgp precedence 4 police 32000 1200
```

## Related Commands

| Command | Description |
|---|---|
| **show mls qos protocol** | Displays protocol pass-through information. |

# mls qos queueing-only

To enable port-queueing mode, use the **mlsqosqueueing-only** command in global configuration mode. To disable the port-queueing mode, use the **no** form of this command.

**mls qos queueing-only**

**no mls qos queueing-only**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Quality of service (QoS) is globally disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

In port-queueing mode, Policy Feature Card (PFC) QoS (marking and policing) is disabled, and packet type of service (ToS) and class of service (CoS) are not changed by the PFC. All queueing on rcv and xmt is based on a QoS tag in the incoming packet, which is based on the incoming CoS.

For 802.1Q or Inter-Link Switch (ISL)-encapsulated port links, queueing is based on the packet 802.1Q or ISL CoS.

For router main interfaces or access ports, queueing is based on the configured per-port CoS (the default CoS is 0).

## Examples

This example shows how to enable the port-queueing mode globally:

```
Router(config)# mls qos queueing-only
```

This example shows how to disable the port-queueing mode globally:

```
Router(config)# no mls qos queueing-only
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos (global configuration mode)** | Enables the QoS functionality globally. |
| **show mls qos** | Displays MLS QoS information. |

# mls qos queue-mode mode-dscp

To set the queuing mode to Differentiated Services Code Point (DSCP) on an interface, use the **mlsqosqueue-modemode-dscp** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

**mls qos queue-mode mode-dscp**

**no mls qos queue-mode mode-dscp**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The queuing mode of an interfaces is class of service (CoS) mode.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXF5 | This command was introduced. |

## Usage Guidelines

This command is supported on 10-Gigabit Ethernet ports only.

You should configure ports to trust DSCP only if they receive traffic that carries valid Layer 3 DSCP.

In Release 12.2(18)SXF5 and later releases, you can enable DSCP-based ingress queues and thresholds on WS-X6708-10GE ports to provide congestion avoidance.

In releases earlier than Release 12.2(18)SXF5, the ingress port queues and thresholds use only Layer 2 Class of Service (CoS), and Policy Feature Card (PFC) QoS does not implement ingress port congestion avoidance on ports configured to trust DSCP.

For traffic from trust DSCP ports, Policy Feature Card (PFC) QoS uses the received DSCP value as the initial internal DSCP value. PFC QoS does not mark any traffic on ingress ports configured to trust received DSCP.

## Examples

This example shows how to set the queuing mode to DSCP on an interface:

```
mls qos queue-mode mode-dscp
```

## Related Commands

| Command | Description |
|---|---|
| **priority-queue queue-limit** | Allocates the available buffer space to a queue. |
| **show mls qos** | Displays MLS QoS information. |

# mls qos rewrite ip dscp

To enable type of service (ToS)-to-differentiated services code point (DSCP) rewrite, use the **mlsqosrewriteipdscp** command in global configuration mode. To disable ToS-to-DSCP rewrite, use the **no** form of this command.

**mls qos rewrite ip dscp** [**slot** *slot1 slot2 slot3...*]

**no mls qos rewrite ip dscp** [**slot** *slot1 slot2 slot3...*]

## Syntax Description

| | |
|---|---|
| **slot** *slot* | (Optional) Specifies the slot number. Use the mls qos rewrite ip dscp slot ? command to determine the valid slots for your chassis. |

## Command Default

ToS-to-DSCP rewrite is enabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(17a)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SRD3 | This command was modified. The **slot***slot* keyword/argument pair was added. |

## Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

If you disable ToS-to-DSCP rewrite, and QoS is enabled globally, the following occurs:

- Final ToS-to-DSCP rewrite is disabled, and the DSCP packet is preserved.
- Policing and marking function according to the QoS configuration.
- Marked and marked-down class of service (CoS) is used for queueing.
- In QoS disabled mode, both ToS and CoS are preserved.

The **nomlsqosrewriteipdscp** command is incompatible with Multiprotocol Label Switching (MPLS). The default **mlsqosrewriteipdscp** command must remain enabled in order for the PFC3BXL or PFC3B to assign the correct MPLS Experimental (EXP) value for the labels that it imposes. This restriction does not apply to PFC3C or PFC3CXL forward.

The **mlsqosrewriteipdscpslot** command can be used for disabling ToS-to-DSCP rewrite on supervisors or DFC linecards. Although the command will be accepted for non-DFC linecard slots, it does not come into effect unless a DFC linecard is inserted into that slot.

To disable rewrite on packets that are coming in on non-DFC linecards, disable the rewrite on the supervisor slots. Note that this disables the rewrite on packets that are coming in on all non-DFC linecards on the system.

## Examples

The following example shows how to enable ToS-to-DSCP rewrite in slot 4:

```
Router(config)# mls qos rewrite ip dscp slot 4
```

The following example shows how to disable port-queueing mode globally:

```
Router(config)# no mls qos rewrite ip dscp
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos (global configuration mode)** | Enables the QoS functionality globally. |
| **show mls qos** | Displays MLS QoS information. |

# mls qos statistics-export (global configuration)

To enable quality of service (QoS)-statistics data export globally, use the **mlsqosstatistics-export**command in global configuration mode. To disable QoS-statistics data export globally, use the **no** form of this command.

**mls qos statistics-export**

**no mls qos statistics-export**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

You must enable data export globally to set up data export on your Cisco 7600 series routers.

QoS-statistics data export is not supported on OSM interfaces.

For QoS-statistics data export to perform correctly, you should set the export-destination hostname or IP address and the User Datagram Port (UDP) number.

## Examples

This example shows how to enable data export globally:

```
Router(config)# mls qos statistics-export
```

This example shows how to disable data export globally:

```
Router(config)# no mls qos statistics-export
```

## Related Commands

| Command | Description |
|---|---|
| **show mls qos statistics-export info** | Displays information about the MLS-statistics data-export status and configuration. |

# mls qos statistics-export (interface configuration)

To enable per-port quality of service (QoS)-statistics data export, use the **mlsqosstatistics-export**command in interface configuration mode. To disable per-port QoS-statistics data export, use the **no** form of this command.

**mls qos statistics-export**

**no mls qos statistics-export**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

QoS-statistics data export is not supported on OSM interfaces.

You must enable data export on the port and globally to set up data export on your Cisco 7600 series routers.

For QoS-statistics data export to perform correctly, you should set the export-destination hostname or IP address and the User Datagram Port (UDP) number.

QoS-statistics data is exported using delimiter-separated fields. You can set the delimiter by entering the **mlsqosstatistics-exportdelimiter**command.

Port statistics are exported; port QoS statistics are not exported. For each data export-enabled port, the following information is exported:

- Type (1 denotes the type of port)
- Module/port
- In packets (cumulated hardware-counter values)
- In bytes (cumulated hardware-counter values)
- Out packets (cumulated hardware-counter values)
- Out bytes (cumulated hardware-counter values)

- Time stamp (time in seconds since January 1, 1970 UTC relative)

For example, if you have QoS-statistics data export that is enabled on FastEthernet4/5, the exported records could be (in this example, the delimiter is a | [pipe]) as follows:

```
|1|4/5|123|80|12500|6800|982361894|
```

## Examples

This example shows how to enable QoS-statistics data export:

```
Router(config-if)# mls qos statistics-export
```

This example shows how to disable QoS-statistics data export:

```
Router(config-if)# no mls qos statistics-export
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos statistics-export delimiter** | Sets the QoS-statistics data-export field delimiter. |
| **show mls qos statistics-export info** | Displays information about the MLS-statistics data-export status and configuration. |

# mls qos statistics-export aggregate-policer

To enable quality of service (QoS)-statistics data export on the named aggregate policer, use the **mlsqosstatistics-exportaggregate-policer** command in global configuration mode. To disable QoS-statistics data export on the named aggregate policer, use the **no** form of this command.

**mls qos statistics-export aggregate-policer** *policer-name*

**no mls qos statistics-export aggregate-policer** *policer-name*

## Syntax Description

| | |
|---|---|
| *policer-name* | Name of the policer. |

## Command Default

Disabled for all shared aggregate policers.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

QoS-statistics data export is not supported on Optical Services Modules (OSM) interfaces.

You must enable data export on the shared aggregate policer and globally to set up data export on your Cisco 7600 series routers.

QoS-statistics data is exported using delimiter-separated fields. You can set the delimiter by entering the **mlsqosstatistics-exportdelimiter** command.

For each data export-enabled shared aggregate or named policer, statistics data per policer per EARL is exported. For each data export-enabled shared aggregate or named policer, the following information is exported:

- Type (3 denotes aggregate policer export type)
- Aggregate name
- Direction (in or out)
- Encoded Address Recognition Logic (EARL) identification
- Accepted packets (accumulated hardware-counter values)

- Exceeded normal-rate packets (accumulated hardware-counter values)
- Exceeded excess-rate packets (accumulated hardware-counter values)
- Time stamp (time in seconds since January 1, 1970 UTC relative)

If a shared aggregate policer is attached to policies in both directions, two records are exported (one in each direction). Each record will contain the same counter values for accepted packets, exceeded normal packet rates, and exceeded excess packet rates.

For example, if you have the following configuration:

- QoS-statistics data export that is enabled on the shared aggregate policer named “aggr_1”
- An EARL in the supervisor engine that is installed in slot 1
- An EARL on the Distributed Forwarding Card (DFC) that is installed in slot 3

the exported records could be (note that in this example, the delimiter is a | [pipe]) as follows:

```
|3|agg_1|in|1|45543|2345|982361894|
|3|agg_1|in|3|45543|2345|982361894|
```

## Examples

This example shows how to enable per-shared aggregate or named-policer data export:

```
Router(config)# mls qos statistics-export aggregate-policer aggr1M
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos statistics-export delimiter** | Sets the QoS-statistics data-export field delimiter. |
| **show mls qos statistics-export info** | Displays information about the MLS-statistics data-export status and configuration. |

# mls qos statistics-export class-map

To enable quality of service (QoS)-statistics data export for a class map, use the **mlsqosstatistics-exportclass-map** command in global configuration mode. To disable QoS-statistics data export for a class map, use the **no** form of this command.

**mls qos statistics-export class-map** *classmap-name*

**no mls qos statistics-export class-map** *classmap-nam e*

## Syntax Description

| | |
|---|---|
| *classmap-name* | Name of the class map. |

## Command Default

Disabled

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

QoS-statistics data export is not supported on OSM interfaces.

You must enable data export on the class map and globally to set up data export on your Cisco 7600 series routers.

QoS-statistics data is exported using delimiter-separated fields. You can set the delimiter by entering the **mlsqosstatistics-exportdelimiter**command.

For each data export-enabled class map, statistics data per policer per interface is exported. If the interface is a physical interface, the following information is exported:

- Type (4 denotes class map physical export)
- Class-map name
- Direction (in or out)
- Module/port
- Accepted packets (accumulated hardware-counter values)

- Exceeded normal-rate packets (accumulated hardware-counter values)
- Exceeded excess-rate packets (accumulated hardware-counter values)
- Time stamp (time in seconds since January 1, 1970 UTC relative)

If the interface is a Cisco 7600 series router VLAN, the following information is exported:

- Type (5 denotes class-map VLAN export)
- Class-map name
- Direction (in or out)
- Encoded Address Recognition Logic (EARL) identification (slot number in which the EARL is installed)
- VLAN number
- Accepted packets (cumulated hardware-counter values)
- Exceeded normal-rate packets (cumulated hardware-counter values)
- Exceeded excess-rate packets (cumulated hardware-counter values)
- Time stamp (time in seconds since January 1, 1970 UTC relative)

If the interface is a Cisco 7600 series router port channel, the following information is exported:

- Type (6 denotes class-map port-channel export)
- Class-map name
- Direction (in or out)
- EARL identification (slot number in which the EARL is installed)
- Port-channel number
- Accepted packets (cumulated hardware-counter values)
- Exceeded normal-rate packets (cumulated hardware-counter values)
- Exceeded excess-rate packets (cumulated hardware-counter values)
- Time stamp (time in seconds since January 1, 1970 UTC relative)

For example, if you have the following configuration:

- QoS-statistics data export enabled on the class map named “class_1”
- An EARL in the supervisor engine that is installed in slot 1
- An EARL on the Distributed Forwarding Card (DFC) that is installed in slot 3
- The Cisco 7600 series router is in the policy map named “policy_1”
- policy_1 is attached to the following interfaces in the ingress direction:
    - FastEthernet4/5
    - VLAN 100
    - Port-channel 24

The exported records could be (in this example, the delimiter is a | [pipe]) as follows:

|4|class_1|in|4/5|45543|2345|2345|982361894|

|5|class_1|in|1|100|44000|3554|36678|982361894|

|5|class_1|in|3|100|30234|1575|1575|982361894|

## Examples

This example shows how to enable QoS-statistics data export for a class map:

```
Router(config)# mls qos statistics-export class-map class3
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos statistics-export delimiter** | Sets the QoS-statistics data-export field delimiter. |
| **show mls qos statistics-export info** | Displays information about the MLS-statistics data-export status and configuration. |

# mls qos statistics-export delimiter

To set the quality of service (QoS)-statistics data-export field delimiter, use the **mlsqosstatistics-exportdelimiter** command in global configuration mode. To return to the default settings, use the **no** form of this command.

**mls qos statistics-export delimiter**

**no mls qos statistics-export delimiter**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The default delimiter is the pipe character (|).

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

QoS-statistics data export is not supported on Optical Service Module (OSM) interfaces.

You must enable data export globally to set up data export on your Cisco 7600 series routers.

## Examples

This example shows how to set the QoS-statistics data-export field delimiter (a comma) and verify the configuration:

```
Router(config)# mls qos statistics-export delimiter ,
```

## Related Commands

| Command | Description |
|---|---|
| **show mls qos statistics-export info** | Displays information about the MLS-statistics data-export status and configuration. |

# mls qos statistics-export destination

To configure the quality of service (QoS)-statistics data-export destination host and User Datagram Protocol (UDP) port number, use the **mlsqosstatistics-exportdestination** command in global configuration mode. To return to the default settings, use the **no** form of this command.

**mls qos statistics-export destination** {*host-name*| *host-ip-address*} {**port** *port-number*| **syslog**} [**facility** *facility-name*] [**severity** *severity-value*]

## Syntax Description

| | |
|---|---|
| *host-name* | Hostname. |
| *host-ip-address* | Host IP address. |
| **port** *port-number* | Specifies the UDP port number. |
| **syslog** | Specifies the syslog port. |
| **facility** *facility-name* | (Optional) Specifies the type of facility to export; see the “Usage Guidelines” section for a list of valid values. |
| **severity** *severity-value* | (Optional) Specifies the severity level to export; see the “Usage Guidelines” section for a list of valid values. |

## Command Default

The default is none unless **syslog** is specified. If **syslog** is specified, the defaults are as follows:

- *port* is 514 .
- *facility* is local6 .
- *severity* is debug .

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

**Usage Guidelines**

QoS-statistics data export is not supported on Optical Service Module (OSM) interfaces.

Valid *facility*values are as follows:

- **authorization** --Security/authorization messages
- **cron** --Clock daemon
- **daemon** --System daemon
- **kernel** --Kernel messages
- **local0** --Local use 0
- **local1** --Local use 1
- **local2** --Local use 2
- **local3** --Local use 3
- **local4** --Local use 4
- **local5** --Local use 5
- **local6** --Local use 6
- **local7** --Local use 7
- **lpr** --Line printer subsystem
- **mail** --Mail system
- **news** --Network news subsystem
- **syslog** --Messages that are generated internally by syslogd
- **user** --User-level messages
- **uucp** --UNIX-to-UNIX Copy Program (UUCP) subsystem

Valid *severity* levels are as follows:

- **alert** --Action must be taken immediately
- **critical** --Critical conditions
- **debug** --Debug-level messages
- **emergency** --System is unusable
- **error** --Error conditions
- **informational** --Informational
- **notice** --Normal but significant conditions
- **warning** --Warning conditions

## Examples

This example shows how to specify the destination host address and syslog as the UDP port number:

```
Router(config)# mls qos statistics-export destination 172.20.52.3 syslog
```

## Related Commands

| Command | Description |
|---|---|
| **show mls qos statistics-export info** | Displays information about the MLS-statistics data-export status and configuration. |

# mls qos statistics-export interval

To specify how often a port and/or aggregate-policer quality of service (QoS)-statistics data is read and exported, use the **mlsqosstatistics-exportinterval** command in global configuration mode. To return to the default settings, use the **no** form of this command.

**mls qos statistics-export interval** *interval*

**no mls qos statistics-export interval**

## Syntax Description

| | |
|---|---|
| *interval* | Export time; valid values are from 30 to 65535 se conds. |

## Command Default

**300** seconds

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

QoS-statistics data export is not supported on Optical Services Module (OSM) interfaces.

The *interval* needs to be short enough to avoid counter wraparound with the activity in your configuration.

**Caution** Be careful when decreasing the interval because exporting QoS statistics imposes a noticeable load on the Cisco 7600 series routers.

## Examples

This example shows how to set the QoS-statistics data-export interval:

```
Router(config)# mls qos statistics-export interval 250
```

## Related Commands

| Command | Description |
|---|---|
| **show mls qos statistics-export info** | Displays information about the MLS-statistics data-export status and configuration. |

# mls qos supervisor 10g-only

To configure the Cisco 7600 RSP720-10GE to run QoS only on the 10GE uplink ports, use the **mlsqossupervisor10g-only** command in global configuration mode. Use the no form of the command to reconfigure the RSP to run QoS on all the uplink ports (10GE and 1GE).

**mls qos supervisor 10g-only**

**no mls qos supervisor 10g-only**

## Syntax Description

This command has no arguments or keywords.

## Command Default

This command is disabled by default.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRC | This command was introduced on the Cisco 7600 series routers. |

## Usage Guidelines

The RSP720-10GE has both 10GE and 1GE uplink ports. You can configure the RSP720-10GE to run QoS features on all uplink ports (mixed mode) or on 10GE ports only. The number of queues available for QoS depends on which mode is used:

- In mixed mode (10GE and 1GE ports), the default, only four queues are available for QoS.

The QoS port architecture for fixed mode for 1GE ports is (Rx/Tx): **2q8t/1p3q8t**.

- In 10GE only mode, eight queues are available for QoS.

The QoS port architecture for 10GE only mode is as follows (Rx/Tx):

- 
  - **8q8t/1p7q8t** (CoS)
  - **16q8t/1p15q8t** (DSCP)
  - **16q1t/1p15q1t** (VLAN)

When you switch between mixed-mode QoS and 10GE only mode, service is temporarily lost on the RSP720-10GE uplinks. In addition, when you switch between modes, any existing QoS configuration on the uplinks is lost. You must reconfigure QoS.

When you switch from 10GE only to mixed-mode QoS, you must issue the **noshutdown** command on each of the three 1GE ports to resume QoS service on those ports.

In 10GE only mode, the 1GE ports are visible but they remain in an administratively down state.

**Note** To obtain more information on queues, use the **showqueueinginterface** command.

## Examples

The following example shows how to configure the RSP720-10GE to run QoS on 10GE ports only:

```
Router(config)# mls qos supervisor 10g-only
The following ports will be shut to enable 10g-only mode:
Gix/1 Gix/2 Gix/3
```

The following example shows how in a redundant setup (High Availability), the 1GE uplink ports on both supervisors are shut down even though the redundant links are not used:

```
Router(config)# mls qos supervisor 10g-only
The following ports will be shut to enable 10g-only mode:
Gi6/1 Gi6/2 Gi6/3 Gi5/1 Gi5/2 Gi5/3
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos (interface configuration)** | Displays information about the traffic on an interface. |

# mls qos trust

To configure the quality of service (QoS) port trust state and to classify traffic by examining the class of service (CoS) or differentiated services code point (DSCP) value, use the **mlsqostrust** command in interface configuration mode. To return a port to its untrusted state, use the **no** form of this command.

**mls qos trust** [**cos**| **device cisco-phone**| **dscp**| **ip-precedence**]

**no mls qos trust**

## Syntax Description

| | |
|---|---|
| **cos** | (Optional) Classifies incoming packets that have packet CoS values. The CoS bits in incoming frames are trusted. The internal DSCP value is derived from the CoS bits. The port default CoS value should be used for untagged packets. |
| **device cisco-phone** | (Optional) Configures Cisco Discovery Protocol (CDP) to detect whether or not a Cisco IP phone is attached to the port.<br>• If CDP detects a Cisco IP phone, QoS applies a configured **mlsqostrustdscp**, **mlsqostrustip-precedence**, or **mlsqostrustcos** interface command.<br>• If CDP does not detect a Cisco IP phone, QoS ignores any configured nondefault trust state. |
| **dscp** | (Optional) Classifies incoming packets that have packet DSCP values (the most significant 6 bits of the 8-bit service-type field). The ToS bits in the incoming packets contain the DSCP value. For non-IP packets, the packet CoS value is 0. If you do not enter a keyword, **mlsqostrustdscp** is assumed. |
| **ip-precedence** | (Optional) Specifies that the ToS bits in the incoming packets contain an IP precedence value. The internal DSCP value is derived from the IP-precedence bits. |

## Command Default

The defaults are as follows:

- If you enable global QoS, the port is not trusted.
- If no keyword is specified or the global QoS is disabled, the default is **dscp**.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.1(6)EA2 | This command was introduced. |
| 12.2(14)SX | This command was modified. Support for this command was introduced on the Catalyst 6500 series switches and the Cisco 7600 series routers. |
| 12.2(15)ZJ | This command was implemented on the following platforms: Cisco 2600 series routers, Cisco 3600 series routers, and Cisco 3700 series routers. |
| 12.2(17d)SXB | This command was implemented on the Cisco 7600 series routers and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.2(33)SXI | This command was modified. The **devicecisco-phone** keywords were added. |

## Usage Guidelines

Packets that enter a QoS domain are classified at its edge. Because the packets are classified at the edge, the switch port within the QoS domain can be configured to a trusted state. It is not necessary to classify the packets at every switch within the domain. Use the **mlsqostrust** command to set the trusted state of an interface and to indicate which fields of the packet are used to classify traffic.

When a port is configured with trust DSCP or trust IP precedence and the incoming packet is a non-IP packet, the CoS-to-DSCP map is used to derive the corresponding DSCP value from the CoS value. The CoS can be the packet CoS for trunk ports or the port default CoS for nontrunk ports.

If the DSCP is trusted, the DSCP field of the IP packet is not modified. However, it is still possible that the CoS value of the packet is modified (according to DSCP-to-CoS map).

If the CoS is trusted, the CoS field of the packet is not modified, but the DSCP can be modified (according to CoS-to-DSCP map) if the packet is an IP packet.

The trusted boundary with Cisco device verification feature, implemented with the **devicecisco-phone** keywords, prevents security problems if users connect a non-phone device to a switch port that is configured to support a Cisco IP phone. You must globally enable CDP on the switch and on the port connected to the IP phone. If a Cisco IP phone is not detected, QoS does not apply any configured nondefault trust setting, which prevents misuse of a high-priority queue.

If you configure the trust setting for DSCP or IP precedence, the DSCP or IP precedence values in the incoming packets are trusted. If you configure the **mlsqoscosoverride** interface configuration command on the switch port connected to the IP phone, the switch overrides the CoS of the incoming voice and data packets and assigns the default CoS value to them.

For an inter-QoS domain boundary, you can configure the port to the DSCP-trusted state and apply the DSCP-to-DSCP-mutation map if the DSCP values are different between the QoS domains.

Classification using a port trust state (for example, mls qos trust [**cos** | **dscp** | **ip-precedence**] and a policy map (for example, **service-policyinput***policy-map-name*) are mutually exclusive. The last one configured overwrites the previous configuration.

The following conditions apply to the **mlsqostrust** command running on the Catalyst 6500 series switches or the Cisco 7600 series routers:

- **The cos** keyword is not supported for **pos** or **atm** interface types.
- The trust state does not apply to FlexWAN modules.
- The trust state does not apply to 1q4t LAN ports except for Gigabit Ethernet ports.
- Incoming queue drop thresholds are not implemented when you enter the **mlsqostrustcos** command on 4-port Gigabit Ethernet WAN modules.

**Note** Use the **setqos-group** command to set the trust state on Catalyst 6500 series switch and Cisco 7600 series router Layer 2 WAN interfaces.

## Examples

The following example shows how to set the trusted state of an interface to IP precedence:

```
Router(config-if)# mls qos trust ip-precedence
```

The following example shows how to configure CDP to detect a Cisco IP phone connected to the port:

```
Router(config-if)# mls qos trust device cisco-phone
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos cos** | Defines the default CoS value of a port or assigns the default CoS to all incoming packets on the port. |
| **mls qos map** | Defines the CoS-to-DSCP map or the DSCP-to-CoS map. |
| **show mls qos interface** | Displays QoS information. |

# mls qos trust extend

To configure the trust mode of the phone, use the **mlsqostrustextend** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

**mls qos trust extend** [**cos** *value*]

**no mls qos trust extend**

## Syntax Description

| | |
|---|---|
| **cos** *value* | (Optional) Specifies the class of service (CoS) value that is used to remark the packets from the PC; valid values are from 0 to 7. |

## Command Default

The default settings are as follows:

- Mode is untrusted.
- **cos** *value* is 0.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is not supported on WAN modules.

If you set the phone to trusted mode, all the packets from the PC are sent untouched directly through the phone to the Cisco 7600 series router. If you set the phone to untrusted mode, all the traffic coming from the PC are remarked with the configured CoS value before being sent to the Cisco 7600 series router.

Each time that you enter the **mlsqostrustextend** command, the mode is changed. For example, if the mode was previously set to trusted, if you enter the command, the mode changes to untrusted. Enter the **showqueueinginterface** command to display the current trust mode.

## Examples

This example shows how to set the phone that is attached to the switch port in trust mode:

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# mls qos trust extend
```

This example shows how to change the mode to untrusted and set the remark CoS value to 3:

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# mls qos trust extend cos 3
```

This example shows how to set the configuration to the default mode:

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# no mls qos trust extend
```

## Related Commands

| Command | Description |
|---|---|
| **show queueing interface** | Displays queueing information. |

# mls qos tunnel gre input uniform-mode

To enable the original quality of service (QoS) marking of ingress packets to be copied into the differentiated services code point (DSCP) field of the ingress packet and the Generic Routing Encapsulation (GRE) header, use the **mlsqostunnelgreinputuniform-mode** command in interface configuration mode. To disable the copying operation, use the **no** form of this command.

**mls qos tunnel gre input uniform-mode**

**no mls qos tunnel gre input uniform-mode**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No marking operation is performed on the incoming packets or the GRE headers.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |

## Usage Guidelines

This command is supported only in PFC3C mode or PFC3CXL mode.

Enter the **showmlsqos** command to verify the configuration.

## Examples

The following example shows how to enable the original QoS marking of ingress packets to be copied into the DSCP field and copied in the GRE header:

```
Router(config-if)# mls qos tunnel gre input uniform-mode
```

## Related Commands

| Command | Description |
|---|---|
| **show mls qos** | Displays MLS QoS information. |

# mls qos vlan-based

To enable per-VLAN quality of service (QoS) for a Layer 2 interface, use the **mlsqosvlan-based**command in interface configuration mode. To disable per-VLAN QoS for a Layer 2 interface, use the **no** form of this command.

**mls qos vlan-based**

**no mls qos vlan-based**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is supported on switch-port and port-channel interfaces only.

In VLAN-based mode, the policy map that is attached to the Layer 2 interface is ignored, and QoS is driven by the policy map that is attached to the corresponding VLAN interface.

You can configure per-VLAN QoS only on Layer 2 interfaces.

**Note** Layer 3 interfaces are always in interface-based mode. Layer 3 VLAN interfaces are always in VLAN-based mode.

## Examples

This example shows how to enable per-VLAN QoS for a Layer 2 interface:

```
Router(config-if)# mls qos vlan-based
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos bridged** | Enables the microflow policing for bridged traffic on Layer 3 LAN interfaces. |
| **mls qos cos** | Defines the default CoS value for an interface. |
| **show queueing interface** | Displays queueing information. |

# monitor pids

To configure the program identifiers (PIDs) to be monitored in the Media Delivery Index (MDI) flow, use the **monitorpids** command in the monitor metric mdi mode. To auto-learn the PIDs, use the **no** form of this command.

**monitor pids** *pid1* [ *pid2* ] [ *pid3* ] [ *pid4* ] [ *pid5* ]

**no monitor pids**

## Syntax Description

| | |
|---|---|
| *pid1* [*pid2*] [*pid3*] [*pid4*] [*pid5* | *PIDs you monitor in the MDI flows. The PID value range is 2 to 8190. (Corresponding hexadecimal format range for PIDs: 0x2 to 0x1FFE)* |

## Command Default

No PIDs are configured.

## Command Modes

(config-pmap-c-metric) #

## Command History

| Release | Modification |
|---|---|
| 15.1(1)S | This command was introduced. |

## Usage Guidelines

Use the**monitorpids**command to configure the PIDs to monitor in a MDI flow. By default, the first five PIDs in a new MDI flow stream are logged for monitoring. These PIDs can be video, audio or caption PIDs. However, monitoring PIDs for audio or caption data is not a priority for a customer implementing inline video monitoring, and is optional.

## Examples

This example shows how to configure the PIDs:

```
router(config-pmap-c-metric)# monitor pids 4050 4678 8902
```

## Related Commands

| Command | Description |
|---|---|
| **show policy-map type performance-traffic** | Displays policy-map information along with the monitored PIDs, if configured. |

# mpls experimental

To configure Multiprotocol Label Switching (MPLS) experimental (EXP) levels for a virtual circuit (VC) class that can be assigned to a VC bundle and thus applied to all VC members of that bundle, use the **mplsexperimental**command in VC-class configuration mode. To remove the MPLS EXP levels from the VC class, use the **no** form of this command.

To configure the MPLS EXP levels for a VC member of a bundle, use the **mplsexperimental**command in bundle-vc configuration mode. To remove the MPLS EXP levels from the VC, use the **no** form of this command.

**mpls experimental** [**other**| *range*]

**no mpls experimental**

## Syntax Description

| | |
|---|---|
| **other** | (Optional) Specifies any MPLS EXP levels in the range from 0 to 7 that are not explicitly configured. This is the default. |
| *range* | (Optional) A single MPLS EXP level specified as a number from 0 to 7, or a range of levels, specified as a hyphenated range. |

## Command Default

Defaults to **other**, that is, any MPLS EXP levels in the range from 0 to 7 that are not explicitly configured.

## Command Modes

VC-class configuration for a VC class (config-vc-class) Bundle-vc configuration for ATM VC bundle members (config-if-atm-member)

## Command History

| Release | Modification |
|---|---|
| 12.2(8)T | This command was introduced. |
| 12.0(26)S | This command was implemented on the Cisco 10000 series router. |
| 12.0(29)S | This command was integrated into Cisco IOS Release 12.0(29)S. |
| 12.2(16)BC | This command was implemented on the ESR-PRE2. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB. |

## Usage Guidelines

Assignment of MPLS EXP levels to VC bundle members allows you to create differentiated service because you can distribute the MPLS EXP levels over the different VC bundle members. You can map a single level

or a range of levels to each discrete VC in the bundle, thereby enabling VCs in the bundle to carry packets marked with different levels. Alternatively, you can configure a VC with the **mplsexperimentalother** command to indicate that it can carry traffic marked with levels not specifically configured for it. Only one VC in the bundle can be configured with the **mplsexperimentalother** command to carry all levels not specified. This VC is considered the default one.

To use this command in VC-class configuration mode, enter the **vc-classatm** global configuration command before you enter this command. This command has no effect if the VC class that contains the command is attached to a standalone VC, that is, if the VC is not a bundle member.

To use this command to configure an individual bundle member in bundle-VC configuration mode, first enter the **bundle** command to enact bundle configuration mode for the bundle to which you want to add or modify the VC member to be configured. Then use the **pvc-bundle** command to specify the VC to be created or modified and enter bundle-VC configuration mode.

VCs in a VC bundle are subject to the following configuration inheritance guidelines (listed in order of next highest MPLS EXP level):

- VC configuration in bundle-VC mode
- Bundle configuration in bundle mode (with the effect of assigned VC class configuration)
- Subinterface configuration in subinterface mode

**Note** If you are using an ATM interface, you must configure all MPLS EXP levels (ranging from 0 to 7) for the bundle. For this configuration, Cisco recommends configuring one member of the bundle with the **mplsexperimentalother** command. The **other** keyword defaults to any MPLS EXP level in a range from 0 to 7 that is not explicitly configured.

## Examples

The following example configures a class named control-class that includes an **mplsexperimental**command that, when applied to a bundle, configures all VC members of that bundle to carry MPLS EXP level 7 traffic. Note that VC members of that bundle can be individually configured with the **mplsexperimental**command at the bundle-vc level, which would supervene.

```
vc-class atm control-class
 mpls experimental 7
```

The following example configures a permanent virtual circuit (PVC) 401, named control-class, to carry traffic with MPLS EXP levels in the range of 4 to 2, overriding the level mapping set for the VC through VC-class configuration:

```
pvc-bundle control-class 401
 mpls experimental 4-2
```

## Related Commands

| Command | Description |
|---|---|
| **bump** | Configures the bumping rules for a VC class that can be assigned to a VC bundle. |
| **bundle** | Creates a bundle or modifies an existing bundle, and enters bundle configuration mode. |

| Command | Description |
|---|---|
| **class-vc** | Assigns a VC class to an ATM PVC, SVC, or VC bundle member. |
| **protect** | Configures a VC class with protected group or protected VC status for application to a VC bundle member. |
| **pvc-bundle** | Adds a VC to a bundle as a member and enters bundle-VC configuration mode to configure that VC bundle member. |
| **ubr** | Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member. |
| **vbr-nrt** | Configures the VBR-nrt QoS and specifies the output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member. |
| **vc-class atm** | Creates a VC class for an ATM PVC, SVC, or ATM interface, and enters VC-class configuration mode. |

# N through P


- non-tcp, page 785
- non-tcp contexts, page 786
- oam-bundle, page 788
- platform ip features sequential, page 791
- platform ipsec fips-mode, page 794
- platform ipsec llq, page 795
- platform punt-police queue, page 796
- platform qos marker-statistics, page 799
- platform qos match-statistics per-ace, page 801
- platform qos match-statistics per-filter, page 803
- platform vfi dot1q-transparency, page 805
- plim qos input, page 807
- plim qos input map, page 810
- plim qos input map cos (classify CoS values for VLAN), page 815
- police, page 819
- police (EtherSwitch), page 829
- police (percent), page 831
- police (policy map), page 840
- police (two rates), page 848
- police rate (control-plane), page 855
- police rate pdp, page 861
- policy-map, page 865
- policy-map copp-peruser, page 872
- precedence, page 873

- precedence (WRED group), page 876
- preempt-priority, page 879
- priority, page 881
- priority (10000 series), page 885
- priority (SIP400), page 888
- priority-group, page 891
- priority level, page 894
- priority-list default, page 896
- priority-list interface, page 898
- priority-list protocol, page 900
- priority-list queue-limit, page 905
- priority-queue cos-map, page 907
- priority-queue queue-limit, page 909
- pvc-bundle, page 911

# non-tcp

To enable non-Transmission-Control-Protocol (non-TCP) header compression within an IP Header Compression (IPHC) profile, use the **non-tcp**command in IPHC-profile configuration mode. To disable non-TCP header compression within an IPHC profile, use the **no** form of this command.

**non-tcp**

**no non-tcp**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Non-TCP header compression is enabled.

## Command Modes

IPHC-profile configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

### Intended for Use with IPHC Profiles

The **non-tcp**command is intended for use as part of an IPHC profile. An IPHC profile is used to enable and configure header compression on a network. For more information about using IPHC profiles to configure header compression, see the "Header Compression" module and the "Configuring Header Compression Using IPHC Profiles" module of the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4T.

## Examples

The following example shows how to configure an IPHC profile called profile2. In this example, non-TCP header compression is configured.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp
Router(config-iphcp)# end
```

## Related Commands

| Command | Description |
|---|---|
| **iphc-profile** | Creates an IPHC profile. |

# non-tcp contexts

To set the number of contexts available for non-Transmission-Control-Protocol (TCP) header compression, use the **non-tcpcontexts** command in IPHC-profile configuration mode. To remove the number of previously configured contexts, use the **no** form of this command.

**non-tcp contexts** {**absolute** *number-of-connections*| **kbps-per-context** *kbps*}

**no non-tcp contexts**

## Syntax Description

| | |
|---|---|
| **absolute** | Indicates that the maximum number of compressed non-TCP contexts will be based on a fixed (absolute) number. |
| *number-of-connections* | Number of non-TCP connections. Range is from 1 to 1000. |
| **kbps-per-context** | Indicates that the maximum number of compressed non-TCP contexts will be based on available bandwidth. |
| *kbps* | Number of kbps to allow for each context. Range is from 1 to 100. |

## Command Default

The **non-tcpcontexts** command calculates the number of contexts on the basis of bandwidth and allocates 4 kbps per context.

## Command Modes

IPHC-profile configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

Use the **non-tcpcontexts** command to set the number of contexts available for non-TCP header compression. A context is the state that the compressor uses to compress a header and that the decompressor uses to decompress a header. The context is the uncompressed version of the last header sent and includes information used to compress and decompress the packet.

### Intended for Use with IPHC Profiles

The **non-tcpcontexts**command is intended for use as part of an IPHC profile. An IPHC profile is used to enable and configure header compression on your network. For more information about using IPHC profiles to configure header compression, see the “Header Compression” module and the “Configuring Header

Compression Using IPHC Profiles" module of the *Cisco IOS Quality of Service Solutions Configuration Guide* , Release 12.4T.

**Setting the Number of Contexts as an Absolute Number**

The **non-tcpcontexts**command allows you to set the number of contexts as an absolute number. To set the number of contexts as an absolute number, enter a number between 1 and 1000.

**Calculating the Number of Contexts on the Basis of Bandwidth**

The **non-tcpcontexts**command can calculate the number of contexts on the basis of the bandwidth available on the network link to which the IPHC profile is applied.

To have the number of contexts calculated on the basis of the available bandwidth, enter the **kbps-per-context**keyword followed by a value for the *kbps* argument. The command divides the available bandwidth by the kbps specified. For example, if the bandwidth of the network link is 3000 kbps, and you enter 5 for the *kbps* argument, the command calculates 600 contexts.

## Examples

The following is an example of an IPHC profile called profile2. In this example, the number of non-TCP contexts has been set to 75.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp contexts absolute 75
Router(config-iphcp)# end
```

## Related Commands

| Command | Description |
|---|---|
| **iphc-profile** | Creates an IPHC profile. |

# oam-bundle

To enable end-to-end F5 Operation, Administration, and Maintenance (OAM) loopback cell generation and OAM management for all virtual circuit (VC) members of a bundle or a VC class that can be applied to a VC bundle, use the **oam-bundle** command in SVC-bundle configuration mode or VC-class configuration mode. To remove OAM management from the bundle or class configuration, use the **no** form of this command.

To enable end-to-end F5 OAM loopback cell generation and OAM management for all VC members of a bundle, use the **oam-bundle** command in bundle configuration mode. To remove OAM management from the bundle, use the **no** form of this command.

**oam-bundle [manage]** [ *frequency* ]

**no oam-bundle [manage]** [ *frequency* ]

## Syntax Description

| | |
|---|---|
| **manage** | (Optional) Enables OAM management. If this keyword is omitted, loopback cells are sent, but the bundle is not managed. |
| *frequency* | (Optional) Number of seconds between transmitted OAM loopback cells. Values range from 0 to 600 seconds. The default value for the *frequency* argument is 10 seconds. |

## Command Default

End-to-end F5 OAM loopback cell generation and OAM management are disabled, but if OAM cells are received, they are looped back.

## Command Modes

SVC-bundle configuration (for an SVC bundle) VC-class configuration (for a VC class) Bundle configuration (for an ATM VC bundle)

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.0(26)S | This command was introduced on the Cisco 10000 series router. |
| 12.2(16)BX | This command was implemented on the ESR-PRE2. |
| 12.2(4)T | This command was made available in SVC-bundle configuration mode. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB. |

| Release | Modification |
|---|---|
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command defines whether a VC bundle is OAM managed. If this command is configured for a bundle, every VC member of the bundle is OAM managed. If OAM management is enabled, further control of OAM management is configured using the **oamretry**command.

This command has no effect if the VC class that contains the command is attached to a standalone VC; that is, if the VC is not a bundle member. In this case, the attributes are ignored by the VC.

To use this command in VC-class configuration mode, first enter the **vc-classatm** global configuration command.

To use this command in bundle configuration mode, first enter the **bundle** subinterface configuration command to create the bundle or to specify an existing bundle.

VCs in a VC bundle are subject to the following configuration inheritance rules (listed in order of next-highest precedence):

- VC configuration in bundle-VC mode
- Bundle configuration in bundle mode (with the effect of assigned VC-class configuration)

## Examples

The following example enables OAM management for a bundle called “bundle 1”:

```
bundle bundle1
 oam-bundle manage
```

## Related Commands

| Command | Description |
|---|---|
| **broadcast** | Configures broadcast packet duplication and transmission for an ATM VC class, PVC, SVC, or VC bundle. |
| **bundle** | Enters bundle configuration mode to create a bundle or modify an existing bundle. |
| **class-bundle** | Configures a VC bundle with the bundle-level commands contained in the specified VC class. |
| **encapsulation** | Sets the encapsulation method used by the interface. |
| **inarp** | Configures the Inverse ARP time period for an ATM PVC, VC class, or VC bundle. |
| **oam retry** | Configures parameters related to OAM management for an ATM PVC, SVC, VC class, or VC bundle. |

| Command | Description |
|---|---|
| **protocol (ATM)** | Configures a static map for an ATM PVC, SVC, VC class, or VC bundle, and enables Inverse ARP or Inverse ARP broadcasts on an ATM PVC by configuring Inverse ARP either directly on the PVC, on the VC bundle, or in a VC class (applies to IP and IPX protocols only). |
| **vc-class atm** | Creates a virtual circuit (VC) class for an ATM permanent virtual circuit (PVC), switched virtual circuit (SVC), or ATM interface. |

# platform ip features sequential

To enable Internet Protocol (IP) precedence-based or differentiated services code point (DSCP)-based egress quality of service (QoS) filtering to use any IP precedence or DSCP policing or marking changes made by ingress policy feature card (PFC) QoS, use the **platformipfeaturessequential** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

**platform ip features sequential** [**access-group** {*ip-acl-name*| *ip-acl-number*}]

**no platform ip features sequential** [**access-group** {*ip-acl-name*| *ip-acl-number*}]

## Syntax Description

| | |
|---|---|
| **access-group** *ip-acl-name* | (Optional) Specifies the name of the ACL that is used to specify the match criteria for the recirculation packets. |
| **access-group** *ip-acl-number* | (Optional) Specifies the number of the ACL that is used to specify the match criteria for the recirculation packets; valid values are from 1 to 199 and from 1300 to 2699. |

## Command Default

IP precedence-based or DSCP-based egress QoS filtering uses received IP precedence or DSCP values and does not use any IP precedence or DSCP changes made by ingress QoS as the result of policing or marking.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.2(50)SY | This command was introduced. |
| 12.2(18)SXE | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelin

**Caution** If the switch is operating in PFC3A mode with egress ACL support for remarked DSCP configured, when the PFC3 processes traffic to apply ingress PFC QoS, it applies ingress PFC QoS filtering and ingress PFC QoS, and incorrectly applies any egress QoS filtering and egress PFC QoS configured on the ingress interface, which results in unexpected behavior if QoS filtering is configured on an interface where egress ACL support for remarked DSCP is enabled. This problem does not occur in other PFC3 modes.

The enhanced egress-QoS filtering enables the IP precedence-based or DSCP-based egress-QoS filtering to use any IP precedence or DSCP policing or marking changes made by ingress QoS.

The nonenhanced egress-QoS filtering behavior is the normal Cisco 7600 series router or the Catalyst 6500 series switch behavior when QoS is applied in the hardware.

The PFC3 provides egress PFC QoS only for Layer 3-switched and routed traffic on egress Layer 3 interfaces (either LAN ports configured as Layer 3 interfaces or VLAN interfaces).

You configure enhanced egress QoS filtering on ingress Layer 3 interfaces (either LAN ports configured as Layer 3 interfaces or VLAN interfaces).

To enable enhanced egress QoS filtering only for the traffic filtered by a specific standard, extended named, or extended numbered IP ACL, enter the IP ACL name or number.

If you do not enter an IP ACL name or number, enhanced egress QoS filtering is enabled for all IP ingress IP traffic on the interface.

**Note** When you configure enhanced egress-QoS filtering, the PFC3A processes traffic to apply ingress PFC QoS. The PFC3A applies ingress-QoS filtering and Cisco 7600 series router or the Catalyst 6500 series switch hardware ingress QoS. The PFC3A incorrectly applies any egress-QoS filtering and Cisco 7600 series router or the Catalyst 6500 series switch hardware egress QoS that is configured on the ingress interface.

**Note** If you configure enhanced egress-QoS filtering on an interface that uses Layer 2 features to match the IP precedence or DSCP as modified by ingress-QoS marking, the packets are redirected or dropped and prevented from being processed by egress QoS.

**Note** If you enable enhanced egress-QoS filtering, the hardware acceleration of NetFlow-based features such as reflexive ACL, NAT, and TCP intercept are disabled.

To verify configuration, use the **showrunning-configinterface** command.

## Examples

The following example shows how to enable enhanced egress-QoS filtering:

```
Router(config-if)# platform ip features sequential

Router(config-if)#
```

The following example shows how to disable enhanced egress-QoS filtering:

```
Router(config-if)# no platform ip features sequential

Router(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **show running-config interface** | Displays the contents of the currently running configuration file. |

# platform ipsec fips-mode

To enable the Federal Information Processing Standard (FIPS) and hardware entropy, use the **platform ipsec fips-mode** command in the global configuration mode. To disable the FIPS and hardware entropy, use the **no** form of this command.

**platform ipsec fips-mode**

**no platform ipsec fips-mode**

## Syntax Description

This command has no arguments or keywords.

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.7.3S | This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. |

## Examples

The following example shows how to enable the FIPS mode and hardware entropy on a Cisco ASR 1000 Series Aggregation Services Router using the **platform ipsec fips-mode** command:

```
Router(config)# platform ipsec fips-mode

 enable FIPS mode will take effect after reboot!
```

## Related Commands

| Command | Description |
|---|---|
| show crypto entropy status | |

# platform ipsec llq

To enable low latency queuing (LLQ) for quality of service (QoS) groups, use the **platform ipsec llq** command in global configuration mode. To disable LLQ use the **no** version of this command.

**platform ipsec llq qos-group** *group-number*

**no platform ipsec llq qos-group** *group-number*

## Syntax Description

| | |
|---|---|
| **qos-group** | Specifies the QoS group to enable LLQ |
| *group-number* | The number that identifies the group. Valid values are from 1 to 99. |

## Command Default

LLQ is not enabled.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 2.4 | This command was introduced. |

## Usage Guidelines

This command allows users to configure specified QoS groups as high priority for IPsec on tunnel interfaces where Tunnel Protection is used. This prevents high priority packets from being queued to the default queue, thus reducing latency and traffic loss during oversubscription.

## Examples

The following example shows how to configure low latency queuing on QoS group 1:

```
ASR1006-1(config)# platform ipsec llq qos-group 1
```

## Related Commands

| Command | Description |
|---|---|
| **set qos-group** | Sets a QoS group ID that can be used later to classify packets. |

# platform punt-police queue

To enable punt policing on a queue, and to specify the maximum punt rate and burst rate on a per-queue basis, use the **platform punt-police queue** command in global configuration mode. To return to the default settings, use the **no** form of this command.

**platform punt-police queue** *queue-id max-punt-rate max-burst-rate*

**no platform punt-police queue** *queue-id*

## Syntax Description

| | |
|---|---|
| *queue-id* | Unique number that identifies the queue. Valid range is a number from 0 to 28. |
| *max-punt-rate* | Maximum punt-rate for the queue, in packets per second (pps). Valid range is a number from 10 to 10000. |
| *max-burst-rate* | Maximum burst-rate for the queue, in packets per second (pps). Valid range is a number from 1000 to 10000. |

## Command Default

Punt policing is enabled on the queues. See the table in the "Usage Guidelines" section for a list of the defaults for each queue.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.5S | This command was introduced on the Cisco ASR 903 router. |

## Usage Guidelines

Punt policing protects a Route Processor (RP) from having to process noncritical traffic. Traffic is placed on different CPU queues based on various criteria. You can then configure the maximum punt rate on a per-queue basis. By default, no explicit policing is done on a queue.

**Note** Traffic on a certain CPU queue could be dropped, irrespective of the configured punt rate, based on the queue priority, queue size, or traffic punt rate.

To verify the configuration, use the **show platform software infrastructure punt statistics** command.

Punt policing is enabled by default. The following table shows the default punt policing settings for each queue:

*Table 26: Default Punt Policing Settings*

| Ring /Queue | Queue Name | Punt Rate (pps) | Burst Rate (pps) |
|---|---|---|---|
| 0 | SW FORWARDING Q | 500 | 1000 |
| 1 | ROUTING PROTOCOL Q | 500 | 1000 |
| 2 | ICMP Q | 500 | 1000 |
| 3 | HOST Q | 1000 | 2000 |
| 4 | ACL LOGGIN Q | 500 | 1000 |
| 5 | STP Q | 3000 | 6000 |
| 6 | L2 PROTOCOL Q | 1000 | 2000 |
| 7 | MCAST CONTROL Q | 1000 | 2000 |
| 8 | BROADCAST Q | 500 | 1000 |
| 9 | REP Q | 3000 | 6000 |
| 10 | CFM Q | 3000 | 6000 |
| 11 | CONTROL Q | 1000 | 2000 |
| 12 | IP MPLS TTL Q | 1000 | 2000 |
| 13 | DEFAULT MCAST Q | 500 | 1000 |
| 14 | MCAST ROUTE DATA Q | 500 | 1000 |
| 15 | MCAST MISMATCH Q | 500 | 1000 |
| 16 | RPF FAIL Q | 500 | 1000 |
| 17 | ROUTING THROTTLE Q | 500 | 1000 |
| 18 | MCAST Q | 500 | 1000 |
| 19 | MPLS OAM | 1000 | 2000 |
| 20 | IP MPLS MTU | 500 | 1000 |
| 21 | PTP Q | 3000 | 6000 |

| Ring /Queue | Queue Name | Punt Rate (pps) | Burst Rate (pps) |
|---|---|---|---|
| 22 | LINUX ND Q | 500 | 1000 |
| 23 | KEEPALIVE Q | 1000 | 2000 |
| 24 | ESMC Q | 3000 | 6000 |
| 25 | FPGA BFD Q | 3000 | 6000 |
| 26 | FPGA CCM Q | 3000 | 6000 |
| 27 | FPGA CFE Q | 3000 | 6000 |
| 28 | L2PT DUP Q | 4000 | 8000 |

## Examples

The following example shows how to enable punt policing on queue 20, set the maximum punt rate to 9000 pps, and set the maximum burst rate to 10000 pps:

```
Router(config)# platform punt-police queue 20 9000 10000
```

## Related Commands

| Command | Description |
|---|---|
| **show platform hardware pp active infrastructure pi npd rx policer** | Displays punt policing statistics for all queues. |
| **show platform software infrastructure punt statistics** | Displays whether queue-based punt policing is enabled. |

# platform qos marker-statistics

To display the number of packets that have modified headers and have been classified into a category for local router processing at a system-wide (platform) level, use the **platformqosmarker-statistics** command in global configuration mode. To disable displaying the QoS: Packet Marking Statistics feature, use the **no** form of this command.

**platform qos marker-statistics**

**no platform qos marker-statistics**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled (no packet marking statistics are displayed).

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.3S | This command was introduced. |

## Usage Guidelines

Ensure no policy maps are associated with interfaces on the system. If there are, the system returns the following message:

```
Either a) A system RELOAD or
       b) Remove all service-policies, re-apply the change
            to the statistics, re-apply all service-policies
   is required before this command will be activated.
```

Enabling the Qos: Packet Marking Statistics feature may increase CPU utilization on a scaled configuration. Before enabling the Qos: Packet Marking Statistics feature, weigh the benefits of the statistics information against the increased CPU utilization for your system.

## Examples

The following example shows how to do the following:

- Enable the QoS: Packet Marking Statistics feature
- Configure an input service policy on an ingress interface
- Classify traffic to a configured class
- Configure marking in the class to set the IP precedence to 1
- Display the **showpolicy-mapinterface** command output

```
Router#
platform qos marker-statistics
```

```
class-map test_class
    match access-group 101
  policy-map test_policy
    class test_class
       set ip precedence 1
Interface POS2/0/1
  service-policy input test_policy
Router#
show policy-map interface
POS2/0/1
  Service-policy input: test_policy
    Class-map: test_class (match-all)
      6644560 packets, 757479840 bytes
      5 minute offered rate 8720000 bps, drop rate 0000 bps
      Match:  precedence 5
      QoS Set
        precedence 1
          Packets marked 6644560
    Class-map: class-default (match-any)
      18 packets, 1612 bytes
      5 minute offered rate 0000 bps, drop rate 0000 bps
      Match: any
```

## Related Commands

| Command | Description |
|---|---|
| **show platform hardware qfp active feature qos config global** | Displays whether the QoS: Packet Marking Statistics feature is enabled. |
| **show policy-map interface** | Displays packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |
| **show policy-map session** | Displays the QoS policy map in effect for a PPPoE session. |

# platform qos match-statistics per-ace

To enable the quality of service (QoS) packet-matching statistics to count the number of packets and bytes matching individual access control elements (ACEs) used in QoS policies, use the **platform qos match-statistics per-ace** command in global configuration mode. To disable the QoS packet-matching statistics per ACE, use the **no** form of this command.

**platform qos match-statistics per-ace**

**no platform qos match-statistics per-ace**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled (ACE statistics for QoS are not incremented).

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.10S | This command was introduced. |

## Usage Guidelines

You must configure the **platform qos match-statistics per-filter** command to enable QoS per-filter packet-matching statistics before you configure the **platform qos match-statistics per-ace** command to enable QoS per-ACE packet-matching statistics.

Ensure that policy maps are not associated with the interfaces on the system. If they are, the system returns the following message:

```
Either a) A system RELOAD or
       b) Remove all service-policies, re-apply the change
          to the statistics, re-apply all service-policies
   is required before this command will be activated.
```

Enabling the Per ACE QoS Statistics feature may increase CPU utilization on a scaled configuration. Before you enable it you should weigh the benefits of the statistics information against the increased CPU utilization on the system.

## Examples

The following example shows how to configure a per-ACE filter for a QoS policy map:

```
Device(config)# platform qos match-statistics per-filter
Device(config)# platform qos match-statistics per-ace
```

## Related Commands

| Command | Description |
|---|---|
| **class-map match-any** | Creates a class map to be used for matching packets to a specified class. |
| **platform qos match-statistics per-filter** | Enables QoS per-filter packet matching statistics at the system-wide (platform) level. |
| **show access lists** | Displays ACE statistics for all configured ACLs including those used in QoS service policies. |
| **show platform hardware qfp active feature qos config global** | Displays whether the QoS Packet Matching Statistics feature is enabled. |
| **show policy-map interface** | Displays packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# platform qos match-statistics per-filter

To define a QoS packet filter at the system-wide (platform) level, then display the number of packets and bytes matching that filter, use the **platformqosmatch-statisticsper-filter** command in global configuration mode. To stop filtering, use the **no** form of this command.

**platform qos match-statistics per-filter**

**no platform qos match-statistics per-filter**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled (no packet matching statistics are displayed).

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.3S | This command was introduced. |

## Usage Guidelines

Ensure no policy maps are associated with interfaces on the system. If there are, the system returns the following message:

```
Either a) A system RELOAD or
       b) Remove all service-policies, re-apply the change
            to the statistics, re-apply all service-policies
   is required before this command will be activated.
```

Enabling the QoS: Packet Matching Statistics feature may increase CPU utilization on a scaled configuration. Before enabling QoS: Packet Matching Statistics, weigh the benefits of the statistics information against the increased CPU utilization for your system.

```
Ensure you have defined a filter using the class-map
 command with the match-any
 keyword.
```

## Examples

The following example shows you how to use the this command:

```
Router>
enable
Router#
configure terminal
Router(config)#
platform qos match-statistics per-filter
Router# end
```

## Related Commands

| Command | Description |
|---|---|
| **class-map match-any** | Creates a class map to be used for matching packets to a specified class. |
| **show platform hardware qfp active feature qos config global** | Displays whether or not the QoS: Packet Matching Statistics feature is currently enabled. |
| **show policy-map interface** | Displays packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# platform vfi dot1q-transparency

To enable 802.1Q transparency mode, use the**platformvfidot1q-transparency** command in global configuration mode. To disable 802.1Q transparency, use the **no** form of this command.

**platform vfi dot1q-transparency**

**no platform vfi dot1q-transparency**

## Syntax Description

This command has no arguments or keywords.

## Command Default

802.1Q transparency mode is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXF2 | This command was introduced on the Supervisor Engine 720. |

## Usage Guidelines

This command is supported on Optical Services Modules (OSMs) only.

802.1Q transparency allows a service provider to modify the Multiprotcol Label Switching Experimental bits (MPLS EXP) bits for core-based QoS policies while leaving any Virtual Private LAN Service (VPLS) customer 802.1p bits unchanged.

With releases before Cisco IOS Release 12.2(18)SXF1, application of a service policy to a VLAN interface that matches all and sets the MPLS EXP bits had an effect on both the Interior Gateway Protocol (IGP) label and the VC label. Because the 802.1p bits were rewritten on the egress Provider Edge (PE) based on the received Virtual Circuit (VC) MPLS EXP bits, the VPLS customer's 802.1p bits were changed.

The Dot1q Transparency for EoMPLS feature causes the VLAN-applied policy to affect only the IGP label (for core QoS) and leaves the VC label EXP bits equal to the 802.1p bits. On the egress PE, the 802.1p bits are still rewritten based on the received VC EXP bits; however, because the EXP bits now match the ingress 802.1p bits, a VPLS customer's 802.1p bits do not change.

Global configuration applies to all virtual forwarding instance (VFI) and switched virtual interface (SVI) EoMPLS VCs configured on the Cisco 7600 series routers.

To ensure interoperability, apply the Dot1q Transparency for EoMPLS feature to all participating PE routers.

## Examples

This example shows how to enable 802.1Q transparency:

```
platform vfi dot1q-transparency
```

This example shows how to disable 802.1Q transparency:

```
no platform vfi dot1q-transparency
```

## Related Commands

| Command | Description |
|---|---|
| **show cwan vfi dot1q-transparency** | Displays 802.1Q transparency mode. |

# plim qos input

To attach an ingress classification template to an interface of Packet over SONET (POS), channelized, and clear-channel SPAs, use the **plim qos input class-map** *class-map index*commandin interface configuration mode. To assign excess weight value to the low-priority packets on an interface for a clear-channel SPA, use the **plim qos input** *weight weight-value* command. To remove the ingress classification template assignment for a specified index, use the **no**form of the **plim qos input class-map**command. To remove excess scheduling of low-priority packets from an interface, use the **no** form of **plim qos input weight** command.

**plim qos input** {**class-map** *class-map index*| **weight** *weight-value*}

**no plim qos input** {**class-map** *class-map index*| **weight**}

## Syntax Description

| | |
|---|---|
| **class-map** | Maps the ingress classification template class map to the interface. |
| *class-map index* | The index classification template number for which the classification criteria is applied to the interface. |
| weight | Schedules the weight assigned to an interface to share excess bandwidth among low priority packets. |
| *weight-value* | The weight value assigned to an interface to share excess bandwidth among low priority packets. The excess bandwidth assigned to the interface is relative and dependent on free bandwith assigned to other interfaces and the free bandwidth available. The valid range is 40 to 10000. |

## Command Default

SIP0 uses templates 1 to 62, SIP1 uses templates 63 to 124, and so on.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 3.1.0S | This command was introduced to attach the classification template to an interface, and to assign weight to the interface to enable excess bandwidth distribution. |

## Usage Guidelines

The classification template-specific details are defined in the template, and the template is attached to an interface using the **plim qos input class-map***class-map index*command. The classification template can be

deleted using the **no** form of the command. The **plim qos input class-map***class-mapi ndex* command is applicable to POS SPA, channelized SPA, and clear-channel SPA.

The **plim qos input weight***weight-value* command is used to assign sharing of excess bandwidth for low priority packets. The **plim qos input weight***weight-value*command is used to assign weight to an interface, and depending on the relative weight assigned to other interfaces, bandwidth is shared among the interfaces. The excess bandwidth is allocated after the high priority packets are processed.

**Note** The **plim qos input weight***weight-value*command is applicable to only clear-channel SPAs.

**Note** The option to configure minimum bandwidth for 'strict-priority' queue at port-level (interface-level) is deprecated as it is not applicable to the current mode of operation. Existing configuration will be rejected with an error.

**Note** The **plim qos input** command is not supported from the CEM interface on the Circuit Emulation over Packet (CEoP) OC-3 SPA on Cisco ASR 1000 Series Routers.

**Note** This **plim qos input** is not supported from the CEM interface on the Channelized T1/E1 (CTE1) CEoP SPA on Cisco ASR 1000 Series Routers.

The following commands are present in command-line interface but do not have any effect on the CEoP OC3 SPA and CTE1 CEoP SPA on Cisco ASR 1000 Series Routers. If you configure one of these commands, a message stating that the command is not supported on the CEoP OC3 SPA is displayed. When either these commands are configured, a message stating the same is displayed on the Cisco ASR 1000 Series Router:

**hw-module subslot** {*slot*/*subslot*} **qos input** {{**policer bandwidth** *bandwidth* **strict-policy**} | **weight** *weight*}}

## Examples

The following example shows how to attach a classification template to an interface using the **plim qos input class-map***class-map index* command:

```
Router# config
Router(config)# interface POS 0/2/0
Router(config-if)# plim qos input class-map
2
```

The following example shows how to assign a weight of 50 to an interface to enable sharing of excess bandwidth among low priority packets using the **plim qos input weight***50*command:

```
Router# config
Router(config)# interface POS 0/2/0
Router(config-if)# plim qos input weight
50
```

## Related Commands

| Command | Description |
|---|---|
| **plim qos class-map** | Attaches the classification template to an interface. |

# plim qos input map

To configure a priority queue on Gigabit Ethernet Shared Port Adaptors (SPAs), use the **plim qos input map** command in the interface configuration mode or the subinterface configuration mode. To remove a priority queue, use the **no** form of this command.

**plim qos input map** { **cos** {**enable** | *cos-value* **queue low-latency**} | **ip** {**precedence-based** | **precedence** *precedence-value* **queue low-latency**} | **ipv6 tc** *tc-value* **queue low-latency** | **mpls exp** *exp-value* **queue low-latency**

**no plim qos input map** { **cos** {**enable** | *cos-value* **queue low-latency**} | **ip** {**precedence-based** | **precedence** *precedence-value* **queue low-latency**} | **ipv6 tc** *tc-value* **queue low-latency** | **mpls exp** *exp-value* **queue low-latency**

## Syntax Description

| | |
|---|---|
| **cos enable** | Enables classification of ingress VLAN traffic according to the IEEE 802.1Q networking standard TCI priority bits.<br>**Note** This command can only be applied to VLAN interfaces. |
| **cos** *cos-value* **queue low-latency** | Classifies incoming VLAN traffic on a subinterface according to the 802.1Q priority bits and places the traffic into the appropriate queue. By default, traffic with 802.1Q priority bits set to 6 or 7 are placed in the high-priority queue and all other traffic is placed in the low-priority queue.<br>*cos-value* specifies the IEEE 802.1Q or ISL class of service(CoS) value from 0 to 7.<br>**Note** When you configure a CoS value on a QinQ subinterface, the CoS value applies to all the QinQ subinterfaces having the same outer VLAN ID.<br>**low-latency** specifies the high-priority queue. |
| **ip dscp-based** | Enables the classification of incoming IP traffic according to the value of the DSCP bits.<br>**Note** This command is applicable only to physical interfaces. |

| | |
|---|---|
| **ip dscp** *dscp-value* **queue low-latency** | Classifies incoming IP traffic according to the value of the Differentiated Services Code Point (DSCP) bits and places the traffic into the appropriate queue. By default, IP traffic with DSCP bits equal to Expedited Forwarding (EF) will use the low-latency queue, and traffic with any other DSCP value will use the low-priority queue.<br>**dscp-value** is the value of the DSCP bits. You can specify a range of values separated by a dash or a list of values. For a list of valid values, see the Usage Guidelines section.<br>*low-latency* specifies the high-priority queue. |
| **ip precedence-based** | Enables the classification of incoming IP traffic according to the IP precedence value.<br>**Note** This command is applicable only to physical interfaces. |
| **ip precedence** *precedence-value* **queue low-latency** | Classifies incoming IP traffic according to the value of the IP precedence bits and places the traffic into the appropriate queue. IP traffic with IP precedence bits set to 6 or 7 uses the low-latency queue; all other traffic uses the low-priority queue.<br>*precedence-value* is the value of the IP precedence bits (0 to 7). You can specify a range of values separated by a dash or a list of values, see the Usage Guidelines section.<br>**low-latency** specifies the high-priority queue. |
| **ipv6 tc** *tc-value* **queue low-latency** | Classifies ingress IPv6 traffic based on the value of the traffic class bits and places the traffic into the appropriate queue. By default, IPv6 traffic with a traffic-class value equal to **ef** uses the high-priority queue; all other traffic uses the low-priority queue. Only the most significant six bits of the traffic-class octet is used for the classification.<br>**Note** This command is applicable to physical interfaces.<br>*tc-value* is the value of the traffic class bits. You can specify a range of values separated by a dash or a list of values. For a list of valid values, see the Usage Guidelines section.<br>**low-latency** specifies the high-priority queue. |

| | |
|---|---|
| **mpls exp** *exp-value* **queue low-latency** | Classifies incoming MPLS traffic according to the value of the EXP bits and places the traffic into the appropriate queue. By default, traffic with the EXP bits set to 6 or 7 uses the high-priority queue; all other traffic uses the low-priority queue.<br>**Note** This command see is applicable to physical interfaces.<br>*exp-value* is the value of the EXP bits (0 to 7). You can specify a range of values separated by a dash or a list of values.<br>**low-latency** specifies the high-priority queue. |

**Command Default**

Disabled

**Command Modes**

Interface configuration (config-if) Subinterface configuration (config-subif)

**Command History**

| Release | Modification |
|---|---|
| 12.2(33)SB | This command was introduced on the Cisco 10000 Series Routers for PRE3 and PRE4. |
| 12.2(33)SCB | This command was integrated into Cisco IOS Release 12.2(33)SCB. |
| 3.1.0S | This command was supported to the ATM interfaces on the Cisco ASR 1000 Series Routers. |

**Usage Guidelines**

The **plim qos input map** command separates high-priority traffic from low-priority traffic and places the traffic in the appropriate interface queue. The command separates priority and non-priority traffic at the SPA interface processor (SIP) to prevent the dropping of high-priority traffic in an oversubscription scenario. Each SPA supports one priority queue.

The router supports the following classification types for the prioritization of ingress traffic on the Gigabit Ethernet SPAs:

- VLAN 802.1Q priority bits
- IP DSCP bits
- IP precedence bits
- IPv6 traffic class bits

In the **plim qos input map ip dscp** *dscp-value* **queue low-latency** command, valid values for *dscp-value* can be one of the following:

- 0 to 63—Differentiated services codepoint value

- af11—001010
- af12—001100
- af13—001110
- af21—010010
- af22—010100
- af23—010110
- af31—011010
- af32—011100
- af33—011110
- af41—100010
- af42—100100
- af43—100110
- cs1—Precedence 1 (001000)
- cs2—Precedence 2 (010000)
- cs3—Precedence 3 (011000)
- cs4—Precedence 4 (100000)
- cs5—Precedence 5 (101000)
- cs6—Precedence 6 (110000)
- cs7—Precedence 7 (111000)
- default—000000
- ef—101110

In the **plim qos input map ipv6 tc** *tc-value* **queue low-latency** command, valid values for *tc-value* can be one of the following:

- 0 to 63—Differentiated services codepoint value
- af11—001010
- af12—001100
- af13—001110
- af21—010010
- af22—010100
- af23—010110
- af31—011010
- af32—011100
- af33—011110

- af41—100010
- af42—100100
- af43—100110
- cs1—Precedence 1 (001000)
- cs2—Precedence 2 (010000)
- cs3—Precedence 3 (011000)
- cs4—Precedence 4 (100000)
- cs5—Precedence 5 (101000)
- cs6—Precedence 6 (110000)
- cs7—Precedence 7 (111000)
- default—000000
- ef—101110

## Examples

The following example shows how to use the **plim qos input map ip dscp-based** command to enable DSCP-based classification on the SPA that is located in subslot 0 of the SIP in slot 1 of a Cisco 10000 Series Router:

```
Router(config)# interface gigabitethernet 3/0/1
Router(config-if)# plim qos input map ip dscp-based
```

The following example shows how to use the **plim qos input map** command to classify incoming IP traffic according to the value of the DSCP bits, and place the traffic into the appropriate queue on an ATM interface on a Cisco ASR 1000 Series Router:

```
Router# configure terminal
Router(config)# interface ATM0/1/0
Router(config-if)# plim qos input map ip dscp af11 - af12 queue strict-priority
Router(config-if)# plim qos input map ipv6 tc af11 - af12 queue strict-priority
Router(config-if)# plim qos input map mpls exp 7 queue 0
```

## Related Commands

| Command | Description |
|---|---|
| **card** | Preprovisions the SIP-600 and SPAs. |
| **mtu** | Configures the maximum packet size for an interface. The default is 1500 bytes. The maximum configurable MTU is 9129 bytes. |
| **negotiation auto** | Enables auto negotiation on a Gigabit Ethernet SPA interface on the Cisco 10000 SIP-600. |

# plim qos input map cos (classify CoS values for VLAN)

To classify ingress traffic on Ethernet shared port adapters (SPAs) based on the Class of Service (CoS) value or CoS range of either the inner or the outer VLAN tag of a QinQ subinterface as either high priority (low latency) or low priority (queue 0), use the **plim qos input map cos** command in subinterface configuration mode. To disable the CoS-based classification, use the **no** form of this command.

### Syntax for Classifying the CoS Values for an Inner VLAN as High Priority or Low Priority

**plim qos input map cos** {**enable**| **inner-based**| **inner** {*cos-value*| *cos-range*} **queue** {**strict-priority**| **0**}}

**no plim qos input map cos enable**

### Syntax for Classifying the CoS Values for an Outer VLAN as High Priority or Low Priority

**plim qos input map cos** {**enable**| **outer-based**| **outer** {*cos-value*| *cos-range*} **queue** {**strict-priority**| **0**}}

**no plim qos input map cos enable**

## Syntax Description

| | |
|---|---|
| **enable** | Enables IEEE 802.1Q CoS-based classification. |
| **inner-based** | Enables an inner VLAN-based classification. Before you can configure the CoS values for an inner VLAN, you must first enable the inner VLAN-based classification. |
| **outer-based** | Enables an outer VLAN-based classification. Before you can configure the CoS values for an outer VLAN, you must first enable the outer VLAN-based classification. |
| **inner** | Allows you to configure the CoS value or range that requires strict priority for inner VLANs. |
| **outer** | Allows you to configure the CoS value or range that requires strict priority for outer VLANs. |
| *cos-value* | The inner or outer VLAN CoS value for which you want to classify the packets mapping the CoS value as high priority or low priority. |
| *cos-range* | The inner or outer VLAN CoS range for which you want to classify the packets mapping the CoS range as high priority or low priority. |
| **queue** | Enables the classification of inner or outer VLAN CoS values or CoS range as high priority or low priority. |

| | |
|---|---|
| **strict-priority** | Classifies the specified CoS value or range as high priority (low latency). |
| **0** | Classifies the specified CoS value or range as low priority (queue 0). |

**Command Default**

A CoS value of 6 or 7 of an outer VLAN is classified as high priority.

**Command Modes**

Subinterface configuration mode (config-subif)

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.1S | This command was introduced for Ethernet SPAs and was supported on the ATM interfaces on the Cisco ASR 1000 Series Routers. |

**Usage Guidelines**

### Configuring CoS-based Classification for an Inner VLAN

Before you can classify ingress traffic based on inner VLAN CoS values, you must first enable the inner VLAN CoS-based classification using the **plim qos input map cos inner-based** command.

### Configuring CoS-based Classification for an Outer VLAN

Before you can classify ingress traffic based on outer VLAN CoS values, you must first enable the outer VLAN CoS-based classification using the **plim qos input map cos outer-based** command.

To disable the CoS-based classification at the subinterface level and enable the Layer 3 information-based classification at the main interface level, use the **no plim qos input map cos enable** command in subinterface configuration mode. Once the **no plim qos input map cos enable** command is configured, a message indicating that the main interface-level classification configuration will be applicable is displayed.

**Note** With CSCtd91658, if you try to configure CoS-based classification for an inner VLAN on a subinterface that already has classification based on an outer VLAN (or vice versa), or if you try to remove a non-existent CoS-based classification, a warning message is displayed.

**Note** The **plim qos input map cos** command is supported only on Ethernet SPAs. The **plim qos input map cos** command is executed from VLAN subinterface configuration mode under a QinQ subinterface.

## Examples

The following example shows how to classify a CoS value of 3 of an inner VLAN as high priority:

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0.1
Router(config-subif)# plim qos input map cos inner-based
Router(config-subif)# plim qos input map cos inner 3 queue strict-priority
```

The following example shows how to classify a CoS value of 3 of an outer VLAN as high priority:

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0.1
Router(config-subif)# plim qos input map cos outer-based
Router(config-subif)# plim qos input map cos outer 3 queue strict-priority
```

The following example shows how to enable the IEEE 802.1Q CoS-based classification in QinQ subinterface configuration mode:

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0.2
Router(config-subif)# encapsulation dot1q 2 second-dot1q 100
Router(config-subif)# plim qos input map cos enable
```

The following example shows how to disable IEEE 802.1Q CoS-based classification in QinQ subinterface configuration mode. A message is displayed indicating that the main interface-level classification configuration will be applicable.

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0.2
Router(config-subif)# encapsulation dot1q 2 second-dot1q 100
Router(config-subif)# no plim qos input map cos enable
%Classification will now be based on Main interface configuration.
```

The following example shows how to enable IEEE 802.1Q CoS-based classification in Dot1Q subinterface configuration mode:

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0.1
Router(config-subif)# encapsulation dot1Q 1 native
Router(config-subif)# plim qos input map cos enable
```

The following example shows how to disable IEEE 802.1Q CoS-based classification in Dot1Q subinterface configuration mode. A message is displayed indicating that the main interface-level classification configuration will be applicable.

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0.1
Router(config-subif)# encapsulation dot1Q 1 native
Router(config-subif)# no plim qos input map cos enable
%Classification will now be based on Main interface configuration.
```

The following example shows how to use the **plim qos input map** command to classify incoming IP traffic according to the value of the DSCP bits, and place the traffic into the appropriate queue on an ATM interface on a Cisco ASR 1000 Series Router.

```
Router# configure terminal
Router(config)# interface ATM0/1/0
Router(config-if)# plim qos input map ip dscp af11 - af12 queue strict-priority
Router(config-if)# plim qos input map ipv6 tc af11 - af12 queue strict-priority
Router(config-if)# plim qos input map mpls exp 7 queue 0
```

## Related Commands

| Command | Description |
|---|---|
| **encapsulation** | Sets the encapsulation method used by the interface. |

# police

To configure traffic policing, use the **police** command in policy-map class configuration mode or policy-map class police configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

**police** *bps* [ *burst-normal* ] [ *burst-max* ] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

**no police** *bps* [ *burst-normal* ] [ *burst-max* ] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

## Syntax Description

| | |
|---|---|
| *bps* | Average rate, in bits per second. Valid values are 8000 to 128000000000 (128 Gb/s). |
| *burst-normal* | (Optional) Normal burst size in bytes. Valid values are 1000 to 2000000000 (2 Gb). Default normal burst size is 1500. |
| *burst-max* | (Optional) Maximum burst size, in bytes. Valid values are 1000 to 2000000000 (2 Gb). Default varies by platform. |
| **conform-action** | Specifies the action to take on packets that conform to the rate limit. |
| **exceed-action** | Specifies the action to take on packets that exceed the rate limit. |
| **violate-action** | (Optional) Specifies the action to take on packets that violate the normal and maximum burst sizes. |

| | |
|---|---|
| *action* | |

Action to take on packets. Specify one of the following keywords:

- **drop —**Drops the packet.
- **set-clp-transmit** *value***—**Sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and transmits the packet with the ATM CLP bit set to 1.
- **set-cos-inner-transmit** *value***—**Sets the inner class of service field as a policing action for a bridged frame on the Enhanced FlexWAN module when using bridging features on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router.
- **set-cos-transmit** *value***—**Sets the class of service (CoS) packet value and sends it.
- **set-discard-class-transmit —**Sets the discard class attribute of a packet and transmits the packet with the new discard class setting.
- **set-dscp-transmit** *value***—**Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value.
- **set-dscp-tunnel-transmit** *value***—**Sets the DSCP value (0 to 63) in the tunnel header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) or Generic Routing Encapsulation (GRE) tunneled packet for tunnel marking and transmits the packet with the new value.
- **set-frde-transmit** *value***—**Sets the Frame Relay Discard Eligibility (DE) bit from 0 to 1 on the Frame Relay frame and transmits the packet with the DE bit set to 1.
- **set-mpls-experimental-imposition-transmit** *value* **—**Sets the Multiprotocol Label Switching (MPLS) experimental (EXP) bits (0 to 7) in the imposed label headers and transmits the packet with the new MPLS EXP bit value.
- **set-mpls-experimental-topmost** *value***—**Rewrites the experimental value.
- **set-mpls-experimental-topmost-transmit** *value***—**Sets the MPLS EXP field value in the topmost MPLS label header at the input and/or output interfaces.
- **set-prec-transmit** *value***—**Sets the IP

| | |
|---|---|
| | precedence and transmits the packet with the new IP precedence value.<br>• **set-prec-tunnel-transmit** *value*—Sets the precedence value (0 to 7) in the tunnel header of an L2TPv3 or GRE tunneled packet for tunnel marking and transmits the packet with the new value.<br>• **set-qos-transmit** *value*—Sets the QoS group value and transmits the packet with the new QoS group value.<br>• **transmit** —Transmits the packet. The packet is not altered. |

**Command Default**

Traffic policing is not configured.

**Command Modes**

Policy-map class configuration (config-pmap-c) when specifying a single action to be applied to a marked packet

Policy-map class police configuration (config-pmap-c-police) when specifying multiple actions to be applied to a marked packet

**Command History**

| Release | Modification |
|---|---|
| 12.0(5)XE | This command was introduced. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. The **violate-action** keyword was added. |
| 12.2(2)T | This command was modified.<br>• The **set-clp-transmit** keyword for the *action* argument was added.<br>• The **set-frde-transmit** keyword for the *action* argument was added.<br>**Note** However, the **set-frde-transmit** keyword is not supported for AToM traffic in this release. Also, the **set-frde-transmit** keyword is supported only when Frame Relay is implemented on a physical interface without encapsulation.<br>• The **set-mpls-experimental-transmit** keyword for the action argument was added. |

| Release | Modification |
|---|---|
| 12.2(8)T | This command was modified for the Policer Enhancement—Multiple Actions feature. This command can now accommodate multiple actions for packets marked as conforming to, exceeding, or violating a specific rate. |
| 12.2(13)T | This command was modified. In the *action* argument, the **set-mpls-experimental-transmit** keyword was renamed to **set-mpls-experimental-imposition-transmit**. |
| 12.2(28)SB | This command was modified. The **set-dscp-tunnel-transmit** and **set-prec-tunnel-transmit** keywords for the *action* argument were added. These keywords are intended for marking Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunneled packets. |
| 12.2(33)SRA | This command was modified. The **set-cos-inner-transmit** keyword for the action argument was added when using multipoint bridging (MPB) features on the Enhanced FlexWAN module and when using MPB on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router. |
| 12.2(31)SB2 | This command was modified. Support for the **set-frde-transmit** *action* argument was added on the Cisco 10000 series router. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SRC | This command was modified. Support for the Cisco 7600 series router was added. |
| 12.4(15)T2 | This command was modified to include support for marking Generic Routing Encapsulation (GRE) tunneled packets.<br>**Note** For this release, marking GRE-tunneled packets is supported only on platforms equipped with a Cisco MGX Route Processor Module (RPM-XF). |
| 12.2(33)SB | This command was modified to include support for marking GRE-tunneled packets, and support for the Cisco 7300 series router was added. |
| 15.1(1)T | This command was modified to include support for policing on SVI interfaces for Cisco ISR 1800, 2800, and 3800 series routers. |
| 12.2(50)SY | This command was modified. Support for the **set-mpls-experimental-topmost** *value* argument was added. |
| 15.0(1)SY | This command was modified. The maximum value for the *bps*, *burst-normal*, and *burst-max* arguments was increased. |
| Cisco IOS XE Release 3.5S | This command was modified. Support was added for the Cisco ASR 903 Router. |

## Usage Guidelines

Use the **police** command to mark a packet with different quality of service (QoS) values based on conformance to the service-level agreement.

In Cisco IOS release 12.2(50)SY, when you apply the **set-mpls-experimental-topmost** *value* in the egress direction the **set-mpls-experimental-imposition** *value* is blocked.

**Note** In Cisco IOS Release 15.0(1)SY and above, if you configure a policy map without specifying the burst size, then the default burst size can reach 2 Gb/s.

If you configure a high rate or high burst size and then change to a Cisco IOS software release that does not support your settings, the configuration is rejected on boot up and the **police** command is removed from the policy map.

### Specifying Multiple Actions

The **police** command allows you to specify multiple policing actions. When specifying multiple policing actions when configuring the **police** command, note the following points:

- You can specify a maximum of four actions at one time.
- You cannot specify contradictory actions such as **conform-action transmit** and **conform-action drop**.

### Using the police Command with the Traffic Policing Feature

The **police** command can be used with the Traffic Policing feature. The Traffic Policing feature works with a token bucket algorithm. Two types of token bucket algorithms are in Cisco IOS Release 12.1(5)T: a single-token bucket algorithm and a two-token bucket algorithm. A single-token bucket system is used when the **violate-action** option is not specified, and a two-token bucket system is used when the **violate-action** option is specified.

The token bucket algorithm for the **police** command that was introduced in Cisco IOS Release 12.0(5)XE is different from the token bucket algorithm for the **police** command that was introduced in Cisco IOS Release 12.1(5)T. For information on the token bucket algorithm introduced in Release 12.0(5)XE, see the *Traffic Policing* document for Release 12.0(5)XE. This document is available on the New Features for 12.0(5)XE documentation index (under Modular QoS CLI-related feature modules) at www.cisco.com.

The following are explanations of how the token bucket algorithms introduced in Cisco IOS Release 12.1(5)T work.

### Token Bucket Algorithm with Single-Token Bucket

The single-token bucket algorithm is used when the **violate-action** option is not specified in the **police** command CLI.

The conform bucket is initially set to the full size (the full size is the number of bytes specified as the normal burst size).

When a packet of a given size (for example, "B" bytes) arrives at specific time (time "T"), the following actions occur:

- Tokens are updated in the conform bucket. If the previous arrival of the packet was at T1 and the current time is T, the bucket is updated with (T - T1) worth of bits based on the token arrival rate. The token arrival rate is calculated as follows:

(time between packets (which is equal to T - T1) * policer rate)/8 bytes

- If the number of bytes in conform bucket B is greater than or equal to the packet size, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is completed for the packet.
- If the number of bytes in conform bucket B (minus the packet size to be limited) is fewer than 0, the exceed action is taken.

**Token Bucket Algorithm with a Two-Token Bucket**

The two-token bucket algorithm is used when the **violate-action** option is specified in the **police** command.

The conform bucket is initially full (the full size is the number of bytes specified as the normal burst size).

The exceed bucket is initially full (the full exceed bucket size is the number of bytes specified in the maximum burst size).

The tokens for both the conform and exceed token buckets are updated based on the token arrival rate, or committed information rate (CIR).

When a packet of given size (for example, “B” bytes) arrives at specific time (time “T”) the following actions occur:

- Tokens are updated in the conform bucket. If the previous arrival of the packet was at T1 and the current arrival of the packet is at T, the bucket is updated with T -T1 worth of bits based on the token arrival rate. The refill tokens are placed in the conform bucket. If the tokens overflow the conform bucket, the overflow tokens are placed in the exceed bucket.

The token arrival rate is calculated as follows:

(time between packets (which is equal to T-T1) * policer rate)/8 bytes

- If the number of bytes in conform bucket B is greater than or equal to the packet size, the packet conforms and the conform action is taken on the packet. If the packet conforms, B bytes are removed from the conform bucket and the conform action is taken. The exceed bucket is unaffected in this scenario.
- If the number of bytes in conform bucket B is less than the packet size, the excess token bucket is checked for bytes by the packet. If the number of bytes in exceed bucket B is greater than or equal to 0, the exceed action is taken and B bytes are removed from the exceed token bucket. No bytes are removed from the conform bucket.
- If the number of bytes in exceed bucket B is less than the packet size, the packet violates the rate and the violate action is taken. The action is complete for the packet.

**Using the set-cos-inner-transmit Action for SIPs and SPAs on the Cisco 7600 Series Router**

The **set-cos-inner-transmit** keyword action was introduced in Cisco IOS Release 12.2(33)SRA to support marking of the inner CoS value as a policing action when using MPB features on the Enhanced FlexWAN module and when using MPB features on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router.

This command is not supported on the Cisco 7600 SIP-600.

For more information about QoS and the forms of **police** commands supported by the SIPs on the Cisco 7600 series router, see the *Cisco 7600 Series SIP, SSC, and SPA Software Configuration Guide*.

**Using the police command on the Cisco ASR 903 Router**

The following restrictions apply when using the **police** command on the Cisco ASR 903 router:

- Class-based policing on subinterfaces is not supported.

- Policing is supported for ingress policy maps only.
- Hierarchical policing (policing at both parent level and child level) is not supported.
- The Cisco ASR 903 router supports the following action keywords only:
  - **drop**
  - **set-cos-transmit**
  - **set-discard-class-transmit**
  - **set-dscp-transmit**
  - **set-mpls-exp-imposition-transmit**
  - **set-mpls-exp-topmost-transmit**
  - **set-precp-transmit**
  - **set-qos-transmit**
  - **transmit**

## Examples

## Examples

The following example shows how to define a traffic class (using the **class-map** command) and associate the match criteria from the traffic class with the traffic policing configuration, which is configured in the service policy (using the **policy-map** command). The **service-policy** command is then used to attach this service policy to the interface.

In this particular example, traffic policing is configured with the average rate at 8000 bits per second and the normal burst size at 1000 bytes for all packets leaving Fast Ethernet interface 0/0:

```
Router(config)# class-map access-match
Router(config-cmap)# match access-group 1
Router(config-cmap)# exit
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# police 8000 1000 conform-action transmit exceed-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 0/0
Router(config-if)# service-policy output police-setting
```

In this example, the initial token buckets starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the token bucket ((0.25 * 8000)/8), leaving 800 bytes in the token bucket. If the next packet is 900 bytes, the packet exceeds and the exceed action (drop) is taken. No bytes are taken from the token bucket.

## Examples

In this example, traffic policing is configured with the average rate at 8000 bits per second, the normal burst size at 1000 bytes, and the excess burst size at 1000 bytes for all packets leaving Fast Ethernet interface 0/0.

```
Router(config)# class-map access-match
Router(config-cmap)# match access-group 1
Router(config-cmap)# exit
```

```
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action
set-qos-transmit 1 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet 0/0
Router(config-if)# service-policy output police-setting
```

In this example, the initial token buckets starts full at 1000 bytes. If a 450-byte packet arrives, the packet conforms because enough bytes are available in the conform token bucket. The conform action (send) is taken by the packet, and 450 bytes are removed from the conform token bucket (leaving 550 bytes).

If the next packet arrives 0.25 seconds later, 250 bytes are added to the conform token bucket ((0.25 * 8000)/8), leaving 800 bytes in the conform token bucket. If the next packet is 900 bytes, the packet does not conform because only 800 bytes are available in the conform token bucket.

The exceed token bucket, which starts full at 1000 bytes (as specified by the excess burst size), is then checked for available bytes. Because enough bytes are available in the exceed token bucket, the exceed action (set the QoS transmit value of 1) is taken and 900 bytes are taken from the exceed bucket (leaving 100 bytes in the exceed token bucket).

If the next packet arrives 0.40 seconds later, 400 bytes are added to the token buckets ((.40 * 8000)/8). Therefore, the conform token bucket now has 1000 bytes (the maximum number of tokens available in the conform bucket) and 200 bytes overflow the conform token bucket (because only 200 bytes were needed to fill the conform token bucket to capacity). These overflow bytes are placed in the exceed token bucket, giving the exceed token bucket 300 bytes.

If the arriving packet is 1000 bytes, the packet conforms because enough bytes are available in the conform token bucket. The conform action (transmit) is taken by the packet, and 1000 bytes are removed from the conform token bucket (leaving 0 bytes).

If the next packet arrives 0.20 seconds later, 200 bytes are added to the token bucket ((.20 * 8000)/8). Therefore, the conform bucket now has 200 bytes. If the arriving packet is 400 bytes, the packet does not conform because only 200 bytes are available in the conform bucket. Similarly, the packet does not exceed because only 300 bytes are available in the exceed bucket. Therefore, the packet violates and the violate action (drop) is taken.

## Examples

The following example shows that if packets conform to the rate limit, the MPLS EXP field is set to 5. If packets exceed the rate limit, the MPLS EXP field is set to 3.

```
Router(config)# policy-map input-IP-dscp
Router(config-pmap)# class dscp24
Router(config-pmap-c)# police 8000 1500 1000 conform-action
set-mpls-experimental-imposition-transmit 5 exceed-action
set-mpls-experimental-imposition-transmit 3
Router(config-pmap-c)# violate-action drop
```

## Examples

The following example shows configuration of a QoS class that filters all traffic for virtual LAN (VLAN) 100 into a class named “vlan-inner-100” and establishes a traffic shaping policy for the vlan-inner-100 class. The service policy limits traffic to an average rate of 500 kb/s, with a normal burst of 1000 bytes and a maximum burst of 1500 bytes, and sets the inner CoS value to 3. Since setting of the inner CoS value is supported only with bridging features, the configuration also shows the service policy being applied as an output policy for an ATM SPA interface permanent virtual circuit (PVC) that bridges traffic into VLAN 100 using the **bridge-domain** command.

```
Router(config)# class-map match-all vlan-inner-100
Router(config-cmap)# match vlan inner 100
Router(config-cmap)# exit
```

```
Router(config)# policy-map vlan-inner-100
Router(config-pmap)# class vlan-inner-100
Router(config-pmap-c)# police 500000 1000 1500 conform-action set-cos-inner-transmit 3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm3/0/0
Router(config-if)# pvc 100/100
Router(config-if-atm-vc)# bridge-domain 100 dot1q
Router(config-if-atm-vc)# service-policy output vlan-inner-100
Router(config-if-atm-vc)# end
```

## Related Commands

| Command | Description |
|---|---|
| **bridge-domain** | Enables RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged VLAN to an ATM PVC or Frame Relay data-link connection identifier (DLCI). |
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **service-policy** | Specifies the name of the service policy to be attached to the interface. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

# police (EtherSwitch)

To define a policer for classified traffic, use the **police** command in policy-map class configuration mode. To remove an existing policer, use the **no** form of this command.

**police** {*bps*| **cir** *bps*} [*burst-byte*| **bc** *burst-byte*] **conform-action transmit** [**exceed-action** {**drop**| **dscp** *dscp-value*}]

**no police** {*bps*| **cir** *bps*} [*burst-byte*| **bc** *burst-byte*] **conform-action transmit** [**exceed-action** {**drop**| **dscp** *dscp-value*}]

## Syntax Description

| | |
|---|---|
| *bps* \| **cir** *bps* | Average traffic rate or committed information rate (CIR) in bits per second (bps).<br>For 10/100 ports, the range is 1000000 to 100000000, and the granularity is 1 Mbps.<br>For Gigabit-capable Ethernet ports, the range is 8000000 to 128000000000 (or 128 Gbps). Policer granularity above 16 Mbps is .1% of the rate, policer granularity below 16 Mbps is 8 Mbps. |
| *burst-byte* \| **bc** *burst-byte* | (Optional) Normal burst size or burst count in bytes. Valid values are 1000 to 2000000000 (2 Gb). |
| **conform-action transmit** | Sends packets that conform to the rate limit. |
| **exceed-action drop** | (Optional) When the specified rate is exceeded, specifies that the switch drops the packet. |
| **exceed-action dscp** *dscp-value* | (Optional) When the specified rate is exceeded, specifies that the switch changes the differentiated services code point (DSCP) of the packet to the specified *dscp-value* and then sends the packet. |

## Command Default

No policers are defined.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(6)EA2 | This command was introduced. |
| 12.2(15)ZJ | This command was modified. This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |

| Release | Modification |
|---|---|
| 12.3(4)T | This command was modified. This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.0(1)SY | This command was modified. The maximum value for the *burst-byte* argument was increased. |

## Usage Guidelines

You can configure up to six policers on ingress Fast Ethernet ports.

You can configure up to 60 policers on ingress Gigabit-capable Ethernet ports.

Policers cannot be configured on egress Fast Ethernet and Gigabit-capable Ethernet ports.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

Use the **show policy-map** privileged EXEC command to verify your settings.

## Examples

The following example shows how to configure a policer that sets the DSCP value to 46 if traffic does not exceed a 1-Mbps average rate with a burst size of 65536 bytes and drops packets if traffic exceeds these conditions:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set ip dscp 46
Router(config-pmap-c)# police 1000000 65536 conform-action transmit exceed-action drop
Router(config-pmap-c)# end
```

## Related Commands

| Command | Description |
|---|---|
| **policy-map** | Creates or modifies a policy map that can be attached to multiple interfaces and enters policy-map configuration mode. |
| **show policy-map** | Displays QoS policy maps. |

# police (percent)

To configure traffic policing on the basis of a percentage of bandwidth available on an interface, use the **police** command in policy-map class configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

**police cir percent** *percentage* [ *burst-in-msec* ] [**bc** *conform-burst-in-msec* **ms**] [**be** *peak-burst-in-msec* **ms**] [**pir percent** *percentage*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

**no police cir percent** *percentage* [ *burst-in-msec* ] [**bc** *conform-burst-in-msec* **ms**] [**be** *peak-burst-in-msec* **ms**] [**pir percent** *percentage*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

**police cir percent** *percent* [ *burst-in-msec* ] [**bc** *conform-burst-in-msec* **ms**] [**pir** *percent*] [**be** *peak-burst-in-msec* **ms**] [**conform-action action**] [**exceed-action action**] [**violate-action action**]

**no police cir percent** *percent* [ *burst-in-msec* ] [**bc** *conform-burst-in-msec* **ms**] [**pir** *percent*] [**be** *peak-burst-in-msec* **ms**] [**conform-action action**] [**exceed-action action**] [**violate-action action**]

## Syntax Description

| | |
|---|---|
| **cir** | Specifies the information rate. Indicates that the CIR will be used for policing traffic. |
| **percent** | Specifies that a percentage of bandwidth will be used for calculating the CIR. |
| *percentage* | The bandwidth percentage. Valid range is a number from 1 to 100. |
| *burst-in-msec* | (Optional) Burst in milliseconds. Valid range is a number from 1 to 2000. |
| **bc** | (Optional) Specifies the conform burst (bc) size used by the first token bucket for policing traffic. |
| *conform-burst-in-msec* | (Optional) The bc value in milliseconds. Valid range is a number from 1 to 2000. |
| **ms** | (Optional) Indicates that the burst value is specified in milliseconds. |
| **be** | (Optional) Specifies the peak burst (be) size used by the second token bucket for policing traffic. |
| *peak-burst-in-msec* | (Optional) The be size in milliseconds. Valid range is a number from 1 to 2000. |
| **pir** | (Optional) Indicates that the Peak Information Rate (PIR) will be used for policing traffic. |

| | |
|---|---|
| *percent* | (Optional) The percentage of bandwidth tht will be used for calculating the PIR. |
| **conform-action** | (Optional) Action to take on packets whose rate is less than the conform burst. You must specify a value for peak-burst-in-msec before you specify the **conform-action**. |
| **exceed-action** | (Optional) Specifies the action to take on packets whose rate is within the conform and conform plus exceed burst. |
| **violate-action** | (Optional) Specifies the action to take on packets whose rate exceeds the conform plus exceed burst. You must specify the exceed-action before you specify the violate-action. |

| | |
|---|---|
| *action* | (Optional) The action to take on packets. Specify one of the following keywords:<br>**All Supported Platforms**<br>• **drop** --Drops the packet.<br>• **set-clp-transmit** --Sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and sends the packet with the ATM CLP bit set to 1.<br>• **set-dscp-transmit** *new-dscp* -- Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value setting.<br>• **set-frde-transmit** --Sets the Frame Relay discard eligible (DE) bit from 0 to 1 on the Frame Relay frame and sends the packet with the DE bit set to 1.<br>• **set-prec-transmit** *new-prec* --Sets the IP precedence and sends the packet with the new IP precedence value setting.<br>• **transmit** --Sends the packet with no alteration.<br>**Supported Platforms Except the Cisco 10000 Series Router**<br>• **policed-dscp-transmit** --(Exceed and violate action only). Changes the DSCP value per the policed DSCP map and sends the packet.<br>• **set-cos-inner-transmit** *value* --Sets the inner class of service field as a policing action for a bridged frame on the Enhanced FlexWAN module, and when using bridging features on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router.<br>• **set-cos-transmit** *value*--Sets the packet cost of service (CoS) value and sends the packet.<br>• **set-mpls-exposition-transmit** --Sets the Multiprotocol Label Switching (MPLS) experimental bits from 0 to 7 and sends the packet with the new MPLS experimental bit value setting.<br>• **set-mpls-topmost-transmit** --Sets the MPLS experimental bits on the topmost label and sends the packet. |

| | |
|---|---|
| *action (continued)* | **Cisco 10000 Series Routers**<br>• **drop** --Drops the packet.<br>• **set-clp-transmit** *value* --Sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and transmits the packet with the ATM CLP bit set to 1.<br>• **set-cos-inner-transmit** *value* --Sets the inner class of service field as a policing action for a bridged frame on the Enhanced FlexWAN module, and when using bridging features on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router.<br>• **set-cos-transmit** *value* --Sets the packet COS value and sends it.<br>• **set-discard-class-transmit** --Sets the discard class attribute of a packet and transmits the packet with the new discard class setting.<br>• **set-dscp-transmit** *value* --Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value setting.<br>• **set-frde-transmit** *value* --Sets the Frame Relay Discard Eligibility (DE) bit from 0 to 1 on the Frame Relay frame and transmits the packet with the DE bit set to 1.<br>• **set-mpls-experimental-imposition-transmit** *value* --Sets the Multiprotocol Label Switching (MPLS) experimental (EXP) bits (0 to 7) in the imposed label headers and transmits the packet with the new MPLS EXP bit value setting.<br>• **set-mpls-experimental-topmost-transmit** *value* --Sets the MPLS EXP field value in the topmost MPLS label header at the input and/or output interfaces.<br>• **set-prec-transmit** *value* --Sets the IP precedence and transmits the packet with the new IP precedence value setting.<br>• **set-qos-transmit** *value* --Sets the quality of service (QoS) group value and transmits the packet with the new QoS group value setting. Valid values are from 0 to 99.<br>• **transmit** --Transmits the packet. The packet is not altered. |

**Command Default** The default **bc** and **be** values are 4 ms.

**Command Default** The default action for **conform-action** is transmit.

The default action for **exceed-action** and **violate-action** is drop.

**Command Modes** Policy-map class configuration (config-pmap-c)

**Command History**

| Release | Modification |
|---|---|
| 12.0(5)XE | This command was introduced. |
| 12.0(25)SX | This command was modified. The Percent-based Policing feature was introduced on the Cisco 10000 series router. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.2(1)E. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.2(13)T | This command was modified for the Percentage-Based Policing and Shaping feature. |
| 12.0(28)S | The command was integrated into Cisco IOS Release 12.0(28)S. |
| 12.2(18)SXE | The command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 12.2(28)SB | The command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was modified. The **set-cos-inner-transmit** keyword for the action argument was added when using multipoint bridging (MPB) features on the Enhanced FlexWAN module, and when using MPB on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router. |
| 12.2(31)SB2 | This command was modified. Support was added on the PRE3 for the **set-frde-transmit** action argument for the Cisco 10000 series router. |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers. |
| 15.0(1)SY | This command was modified. The maximum value for the CIR and PIR was increased. |

This command calculates the cir and pir on the basis of a percentage of the maximum amount of bandwidth available on the interface. When a policy map is attached to the interface, the equivalent cir and pir values in

bits per second (bps) are calculated on the basis of the interface bandwidth and the percent value entered with this command. The **show policy-map interface** command can then be used to verify the bps rate calculated.

The calculated cir and pir bps rates must be in the range of 8000 and 128000000000 bps (or 128 Gbps). If the rates are outside this range, the associated policy map cannot be attached to the interface. If the interface bandwidth changes (for example, more is added), the bps values of the cir and the pir are recalculated on the basis of the revised amount of bandwidth. If the cir and pir percentages are changed after the policy map is attached to the interface, the bps values of the cir and pir are recalculated.

This command also allows you to specify the values for the conform burst size and the peak burst size in milliseconds. If you want bandwidth to be calculated as a percentage, the conform burst size and the peak burst size must be specified in milliseconds (ms).

Policy maps can be configured in two-level (nested) hierarchies; a top (or "parent") level and a secondary (or "child") level. The **police** (percent) command can be configured for use in either a parent or child policy map.

The **police** (percent) command uses the maximum rate of bandwidth available as the reference point for calculating the bandwidth percentage. When the **police** (percent) command is configured in a child policy map, the **police** (percent) command uses the bandwidth amount specified in the next higher-level policy (in this case, the parent policy map). If the parent policy map does not specify the maximum bandwidth rate available, the **police** (percent) command uses the maximum bandwidth rate available on the next higher level (in this case, the physical interface, the highest point in the hierarchy) as the reference point. The **police** (percent) command always looks to the next higher level for the bandwidth reference point. The following sample configuration illustrates this point:

```
Policymap parent_policy
 class parent
  shape average 512000
  service-policy child_policy
Policymap child_policy
 class normal_type
  police cir percent 30
```

In this sample configuration, there are two hierarchical policies: one called parent_policy and one called child_policy. In the policy map called child_policy, the police command has been configured in the class called normal_type. In this class, the percentage specified by for the **police** (percent) command is 30 percent. The command will use 512 kbps, the peak rate, as the bandwidth reference point for class parent in the parent_policy. The **police** (percent) command will use 512 kbps as the basis for calculating the cir rate (512 kbps * 30 percent).

```
interface serial 4/0
 service-policy output parent_policy
Policymap parent_policy
 class parent
  bandwidth 512
  service-policy child_policy
```

In the above example, there is one policy map called parent_policy. In this policy map, a peak rate has not been specified. The **bandwidth** command has been used, but this command does not represent the maximum rate of bandwidth available. Therefore, the **police** (percent) command will look to the next higher level (in this case serial interface 4/0) to get the bandwidth reference point. Assuming the bandwidth of serial interface

4/0 is 1.5 Mbps, the **police** (percent) command will use 1.5 Mbps as the basis for calculating the cir rate (1500000 * 30 percent).

The **police** (percent) command is often used in conjunction with the **bandwidth** and **priority** commands. The **bandwidth** and **priority** commands can be used to calculate the total amount of bandwidth available on an entity (for example, a physical interface). When the **bandwidth** and **priority** commands calculate the total amount of bandwidth available on an entity, the following guidelines are invoked:

- If the entity is a physical interface, the total bandwidth is the bandwidth on the physical interface.
- If the entity is a shaped ATM permanent virtual circuit (PVC), the total bandwidth is calculated as follows:
  - For a variable bit rate (VBR) virtual circuit (VC), the sustained cell rate (SCR) is used in the calculation.
  - For an available bit rate (ABR) VC, the minimum cell rate (MCR) is used in the calculation.

For more information on bandwidth allocation, see the "Congestion Management Overview" chapter in the *Cisoc IOS Quality of Service Solutions Configuration Guide*.

Using the set-cos-inner-transmit Action for SIPs and SPAs on the Cisco 7600 Series Router

The **set-cos-inner-transmit** keyword action was introduced in Cisco IOS Release 12.2(33)SRA to support marking of the inner CoS value as a policing action when using MPB features on the Enhanced FlexWAN module, and when using MPB features on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router.

This command is not supported on the Cisco 7600 SIP-600.

For more information about QoS and the forms of **police** commands supported by the SIPs on the Cisco 7600 series router, see the *Cisco 7600 Series SIP, SSC, and SPA Software Configuration Guide* .

## Examples

The following example shows how to configure traffic policing using a CIR and a PIR on the basis of a percentage of bandwidth. In this example, a CIR of 20 percent and a PIR of 40 percent have been specified. Additionally, an optional bc value and be value (300 ms and 400 ms, respectively) have been specified.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# police cir percent 20 bc 300 ms be 400 ms pir percent 40

Router(config-pmap-c-police)# exit
```

After the policy map and class maps are configured, the policy map is attached to an interface as shown in the following example:

```
Router> enable
Router# configure terminal
Router(config)# interface serial4/0
Router(config-if)# service-policy input policy1
Router(config-if)# exit
```

Setting the Inner CoS Value as an Action for SIPs and SPAs on the Cisco 7600 Series Router

The following example shows configuration of a QoS class that filters all traffic for virtual LAN (VLAN) 100 into a class named vlan-inner-100 and establishes a traffic shaping policy for the vlan-inner-100 class. The service policy limits traffic to a CIR of 20 percent and a PIR of 40 percent, with a conform burst (bc) of 300 ms, and peak burst (be) of 400 ms, and sets the inner CoS value to 3. Because setting of the inner CoS value is only supported with bridging features, the configuration also shows the service policy being applied as an output policy for an ATM shared port adapter (SPA) interface permanent virtual circuit (PVC) that bridges traffic into VLAN 100 using the **bridge-domain** command.

```
Router(config)# class-map match-all vlan-inner-100
Router(config-cmap)# match vlan inner 100
Router(config-cmap)# exit
Router(config)# policy-map vlan-inner-100
Router(config-pmap-c)# police cir percent 20 bc 300 ms be 400 ms pir percent 40 conform-action
 set-cos-inner-transmit 3
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm3/0/0
Router(config-if)# pvc 100/100
Router(config-if-atm-vc)# bridge-domain 100 dot1q
Router(config-if-atm-vc)# service-policy output vlan-inner-100
Router(config-if)# end
```

The following example shows how to configure the police (percent) command for a priority service. In the example, the priority class named Voice is configured in the policy map named New-Traffic. The router allocates 25 percent of the committed rate to Voice traffic and allows committed bursts of 4 ms and excess bursts of 1 ms. The router transmits Voice traffic that conforms to the committed rate, sets the QoS transmit value to 4 for Voice traffic that exceeds the burst sizes, and drops Voice traffic that violates the committed rate.

```
Router(config)# policy-map New-Traffic
Router(config-pmap)# class Voice
Router(config-pmap-c)# priority
Router(config-pmap-c)# queue-limit 32
Router(config-pmap-c)# police percent 25 4 ms 1 ms conform-action transmit exceed-action
set-qos-transmit 4 violate-action drop
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth (policy-map class)** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map. |
| **bridge-domain** | Enables RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged VLAN to an ATM PVC or Frame Relay DLCI. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **priority** | Gives priority to a traffic class in a policy map. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |

| Command | Description |
|---|---|
| **shape (percent)** | Specifies average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# police (policy map)

To create a per-interface policer and configure the policy-map class to use it, use the **police** command in policy-map class configuration mode. To delete the per-interface policer from the policy-map class, use the **no** form of this command.

**police** *bps* [**[bc]** *normal-burst-bytes* [*maximum-burst-bytes*| **[be]** [ *burst-bytes* ]]] [**pir** *bps* [**be** *burst-bytes*]] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

**no police** *bps*

**police aggregate** *name*

**no police aggregate** *name*

**police cir** *bps* [[ *bc* ] *normal-burst-bytes* [*maximum-burst-bytes*| **[be]** [ *burst-bytes* ]]] [**pir** *bps* [**be** *burst-bytes*]] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

**no police cir** *bps*

**police cir percent** *percent* [*burst* **ms [be]** [*burst* **ms**]] [**pir percent** *percent* [**be** *burst* **ms**]] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

**no police cir** *percent*

**police flow** *bps* [ *normal-burst-bytes* ] [**conform-action** *action* [**exceed-action** *action*]]

**police flow mask** {**dest-only**| **full-flow**| **src-only**} *bps* [ *normal-burst-bytes* ] [**conform-action** *action* [**exceed-action** *action*]]

**no police flow**

## Syntax Description

| | |
|---|---|
| *bps* | The target bit rate in bits per second (bps). The postfix values **k**, **m**, and **g** are allowed, as is a decimal point. Valid range is from 8000 (or 8k) to 128000000000 (or 128 Gbps). |
| *normal-burst-bytes* | (Optional) The CIR token-bucket size in bytes for handling a burst. Valid values are 1000 to 2000000000 (2 Gb). |
| *maximum-burst-bytes* | (Optional) The PIR token-bucket size in bytes for handling a burst. Valid values are 1000 to 2000000000 (2 Gb). |
| *burst-bytes* | (Optional) The token-bucket size in bytes for handling a burst. Valid values are 1000 to 2000000000 (2 Gb). |
| **bc** | (Optional) Specifies in bytes the allowed (conforming) burst size. |
| **be** | (Optional) Specifies in bytes the allowed excess burst size. |

| | |
|---|---|
| **pir** | (Optional) Specifies the peak information rate (PIR). |
| **cir** | Specifies the committed information rate (CIR). |
| **conform-action** *action* | (Optional) Specifies the action to take on packets that conform to the rate limit. See the "Usage Guidelines" section for valid values for the *action* argument. |
| **exceed-action** *action* | (Optional) Specifies the action to be taken on packets when the packet rate is greater than the rate specified in the *maximum-burst-bytes* argument. See the "Usage Guidelines" section for valid values for the *action* argument. |
| **violate-action** *action* | (Optional) Specifies the action to be taken when the packet rate is greater than the rate specified in the *maximum-burst-bytes* argument. See the "Usage Guidelines" section for valid values for the *action* argument. |
| **aggregate** *name* | Specifies a previously defined aggregate policer name and configures the policy-map class to use the specified aggregate policer. |
| **percent** *percent* | Specifies the percentage of the interface bandwidth to be allowed. Valid range is from 1 to 100. |
| *burst* | (Optional) The token-bucket size in milliseconds (ms) for handling a burst. Valid range is from 1 to 2000. |
| **ms** | Indicates milliseconds. When bandwidth is specified as a percentage, this keyword must follow the *burst* argument. |
| **flow** | Specifies a microflow policer that will police each flow. |
| **mask** | Specifies the flow mask to be used for policing. |
| **dest-only** | Specifies the destination-only flow mask. |
| **full-flow** | Specifies the full-flow mask. |
| **src-only** | Specifies the source-only flow mask. |

**Command Default** No policing is performed.

**Command Modes** Policy-map class configuration (config-pmap-c)

**Command History**

| Release | Modification |
|---|---|
| 12.2(14)SX | This command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was integrated into Cisco IOS Release 12.2(17d)SXB and implemented on the Supervisor Engine 2. |
| 12.2(17d)SXB3 | This command was modified. The **police** *bps* minimum rate was lowered from 32,000 to 8,000 on FlexWAN interfaces only. |
| 12.2(18)SXD | This command was modified as follows:<br>• Added **set-mpls-exp-topmost-transmit** to the valid values for the **conform-action** keyword.<br>• Changed the **set-mpls-exp-transmit** keyword to **set-mpls-exp-imposition-transmit**. |
| 12.2(18)SXE | This command was modified. The bps maximum rate was increased from 4,000,000,000 to 10,000,000,000 bps to support 10-Gigabit Ethernet. |
| 12.2(18)SXF | This command was modified. The CIR maximum rate was increased to 10,000,000,000 bps. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was modified. The command behavior was changed so that if you modify only the police rate parameters and not the police actions, the police actions default to the default actions: conform-action transmit, exceed-action drop, and violate-action drop. This was implemented on the Cisco 10000 series router for the PRE3. |
| 12.2(33)SB | This command was modified. The command behavior was changed so that if you modify only the police rate parameters and not the police actions, the police actions are preserved. This was implemented on the Cisco 10000 series router for the PRE3 and PRE4. For more information, see the “Usage Guidelines” section. |
| 12.2(33)SXH2 | This command was modified. The CIR maximum rate was increased to 64,000,000,000 bps. |
| 12.2(33)SXI | This command was modified. The minimum CIR token bucket size was reduced to 1 byte. |
| 15.0(1)SY | This command was modified. The maximum value for the *normal-burst-bytes*, *maximum-burst-bytes*, and *burst-bytes* arguments was increased to 2 Gb. The maximum value for the bps argument was increased to 128 Gb. |

## Usage Guidelines

In Cisco IOS Release 12.2(17d)SXB3, valid values for the *bps* argument for the FlexWAN interfaces only are from 8,000 to 4,000,000,000 bps.

Use the **mls qos aggregate-policer** *name* command to create a named aggregate policer.

You can create two types of aggregate policers: named and per-interface. Both types can be attached to more than one port as follows:

- You create named aggregate policers using the **mls qos aggregate-policer** command. If you attach a named aggregate policer to multiple ingress ports, it polices the matched traffic from all the ingress ports to which it is attached.
- You define per-interface aggregate policers in a policy-map class using the **police** command. If you attach a per-interface aggregate policer to multiple ingress ports, it polices the matched traffic on each ingress port separately.

Use the **no police aggregate** *name* command to clear the use of the named aggregate policer.

Enter the **police flow** command to define a microflow policer (you cannot apply microflow policing to ARP traffic).

Enter the **police** command to define per-interface (not named) aggregate policers.

If the traffic is both aggregate and microflow policed, the aggregate and the microflow policers must both be in the same policy-map class and each must use the same **conform-action** and **exceed-action** keywords.

**Values for the action Argument**

The valid values for the *action* argument are as follows:

- **drop** --Drops packets that do not exceed the rate set for the *bps* argument.
- **set-clp-transmit** --Sets and sends the ATM cell loss priority (CLP).
- **set-cos-inner-transmit {** *new- cos*}--Marks the matched traffic with a new inner class of service (CoS) value of the *new-cos* argument. Valid values of the *new-cos* argument are from 0 to 7.
- **set-cos-transmit {** *new- cos*}--Marks the matched traffic with a new CoS value of the *new-cos* argument. Valid values of the *new-cos* argument are from 0 to 7.
- **set-cos-transmit** --Sets and sends the ATM cell loss priority (CLP).
- **set-dscp-transmit {** *dscp-bit-pattern* **|** *dscp-value* **| default | ef}** -- Marks the matched traffic with a new DSCP value:
  - *dscp-bit-pattern*--Specifies a DSCP bit pattern. Valid values are listed in Table 1 .
  - *dscp-value*--Specifies a DSCP value. Valid values are from 0 to 63.
  - **default**--Matches packets with the default DSCP value (000000).
  - **ef**--Matches packets with the Expedited Forwarding (EF) per-hop behavior (PHB) DSCP value (101110).

*Table 27: Valid DSCP Bit Pattern Values*

| Keyword | Definition |
|---|---|
| **af11** | Matches packets with AF11 DSCP (001010). |
| **af12** | Matches packets with AF12 DSCP (001100). |
| **af13** | Matches packets with AF13 DSCP (001110). |
| **af21** | Matches packets with AF21 DSCP (010010). |
| **af22** | Matches packets with AF22 DSCP (010100). |
| **af23** | Matches packets with AF23 DSCP (010110). |
| **af31** | Matches packets with AF31 DSCP (011010). |
| **af32** | Matches packets with AF32 DSCP (011100). |
| **af33** | Matches packets with AF33 DSCP (011110). |
| **af41** | Matches packets with AF41 DSCP (100010). |
| **af42** | Matches packets with AF42 DSCP (100100). |
| **af43** | Matches packets with AF43 DSCP (100110). |
| **cs1** | Matches packets with CS1 (precedence 1) DSCP (001000). |
| **cs2** | Matches packets with CS2 (precedence 2) DSCP (010000). |
| **cs3** | Matches packets with CS3 (precedence 3) DSCP (011000). |
| **cs4** | Matches packets with CS4 (precedence 4) DSCP (100000). |
| **cs5** | Matches packets with CS5 (precedence 5) DSCP (101000). |
| **cs6** | Matches packets with CS6 (precedence 6) DSCP (110000). |
| **cs7** | Matches packets with CS7 (precedence 7) DSCP (111000). |

- **set-frde-transmit** --Sets and sends the Frame Relay discard eligible (FR DE) bit. This is valid for the **exceed-action** *action* keyword and argument combination.
- **set-mpls-exp-imposition-transmit** *new-mpls-exp* --Rewrites the Multiprotocol Label Switching (MPLS) experimental (exp) bits on imposed label entries and transmits the bits. The *new-mpls-exp* argument specifies the value used to set the MPLS EXP bits that are defined by the policy map. Valid values for the *new-mpls-exp* argument are from 0 to 7.
- **set-mpls-exp-topmost-transmit** --Sets experimental bits on the topmost label and sends the packet.

**Note** The **set-mpls-exp-topmost-transmit** keyword is not supported in some releases of the Catalyst 6500 series switch or the Cisco 7600 series router.

- **set-prec-transmit** *new-precedence* [ **exceed-action** ] --Marks the matched traffic with a new IP-precedence value and transmits it. Valid values for the *new-precedence* argument are from 0 to 7. You can also follow this action with the **exceed-action** keyword.
- **set-qos-transmit** -- Rewrites qos-group and sends the packet.
- **transmit** --Transmits the packets that do not exceed the rate set for the *bps* argument. The optional keyword and argument combination for the **transmit** keyword is **exceed-action** *action*.

If the following keywords are not specified, the default actions are as follows:

- **conform-action** is **transmit**
- **exceed-action** is **drop**
- **violate-action** is **drop**

**Cisco 10000 Series Router**

In releases earlier than Cisco IOS Release 12.2(31)SB, if you modify the police rate parameters, but not the action parameters, the action parameters revert to the default actions.

For example, the following sample configuration shows the **police** command configured in the policy map named test. The police actions are set to set-clp-transmit for conforming, exceeding, and violating traffic. The police rate parameters are then changed to 500000, 250, and 200, respectively, but no actions are modified. When you display the test policy map again, you can see that the police actions default to transmit, drop, and drop, respectively.

```
Router# show policy-map test
Policy Map test
Class prec1
police 248000 100 10 conform-action set-clp-transmit exceed-action set-clp-transmit
violate-action set-clp-transmit
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map test
Router(config-pmap)# class prec1
Router(config-pmap-c)# police 500000 250 200
Router(config-pmap-c)# end
Router# show policy-map test
Policy Map test
Class prec1
police 500000 250 200 conform-action transmit exceed-action drop violate-action drop
```

Cisco IOS Release 12.2(33)SB and later releases support dual police actions and a police submode; therefore, if you use the **police** command to modify only the rate parameters, the police actions do not default to the default actions and the previous actions are preserved.

For example, the following sample configuration shows the **police** command configured under the traffic class named prec1 in the policy map named test. The police rate is specified and the police actions are then specified in police submodes. After you change only the police rate parameters, the police actions do not default, but rather they retain their original settings.

```
Router# show policy-map test
Policy Map test
Class prec1
police 248000 1000 100
conform-action set-clp-transmit
exceed-action set-clp-transmit
violate-action set-clp-transmit
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map test
Router(config-pmap)# class prec1
Router(config-pmap-c)# police 500000 100 200
Router(config-pmap-c)# end
Router# show policy-map test
Policy Map test
Class prec1
police 500000 100 200
conform-action set-clp-transmit
exceed-action set-clp-transmit
violate-action set-clp-transmit
```

## Examples

This example shows how to specify a previously defined aggregate-policer name and configure the policy-map class to use the specified aggregate policer:

```
Router(config-pmap-c)# police aggregate agg1
```

This example shows how to create a policy map named police-setting that uses the class map access-match, which is configured to trust received IP-precedence values and is configured with a maximum-capacity aggregate policer and a microflow policer:

```
Router# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map police-setting
Router(config-pmap)# class access-match
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 1000000000 200000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# police flow 10000000 10000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Accesses QoS class-map configuration mode to configure QoS class maps. |
| **mls qos aggregate-policer** | Defines a named aggregate policer for use in policy maps. |

| Command | Description |
|---|---|
| **police** | Configures traffic policing in QoS policy-map class configuration mode or QoS policy-map class police configuration mode. |
| **service-policy** | Attaches a policy map to an interface. |
| **show class-map** | Displays class-map information. |
| **show policy-map** | Displays information about the policy map. |
| **show policy-map interface** | Displays the statistics and the configurations of the input and output policies that are attached to an interface. |

# police (two rates)

To configure traffic policing using two rates, the committed information rate (CIR) and the peak information rate (PIR), use the **police** command in policy-map class configuration mode. To remove two-rate traffic policing from the configuration, use the **no** form of this command.

**police cir** *cir* [**bc** *conform-burst*] [**pir** *pir*] [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

**no police cir**

## Syntax Description

| | |
|---|---|
| **cir** | Specifies the ommitted information rate (CIR) at which the first token bucket is updated. |
| *cir* | The CIR value in bits per second. The value is a number from 8000 to 128000000000 (128 Gbps). |
| **bc** | (Optional) Specifies the conform burst (bc) size used by the first token bucket for policing. |
| *conform-burst* | (Optional) The bc value in bytes. The value is a number from 1000 to 2000000000 (2 Gb). |
| **pir** | (Optional) Specifies the peak information rate (PIR) at which the second token bucket is updated. |
| *pir* | (Optional) The PIR value in bits per second. The value is a number from 8000 to 128000000000 (128 Gbps). |
| **be** | (Optional) Specifies the peak burst (be) size used by the second token bucket for policing. |
| *peak-burst* | (Optional) The peak burst (be) size in bytes. The size varies according to the interface and platform in use. |
| **conform-action** | (Optional) Specifies the action to take on packets that conform to the CIR and PIR. |
| **exceed-action** | (Optional) Specifies the action to take on packets that conform to the PIR but not the CIR. |
| **violate-action** | (Optional) Specifies the action to take on packets exceed the PIR. |

| | |
|---|---|
| *action* | (Optional) Specifies the action to take on packets. Specify one of the following keywords:<br>• **drop** --Drops the packet.<br>• **set-clp-transmit** --Sets the ATM Cell Loss Priority (CLP) bit from 0 to 1 on the ATM cell and sends the packet with the ATM CLP bit set to 1.<br>• **set-cos-inner-transmit** *value* --Sets the inner class of service field as a policing action for a bridged frame on the Enhanced FlexWAN module, and when using bridging features on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router.<br>• **set-dscp-transmit** *new-dscp* -- Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value setting.<br>• **set-dscp-tunnel-transmit** *value* --Sets the DSCP value (0 to 63) in the tunnel header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) or Generic Routing Encapsulation (GRE) tunneled packet for tunnel marking and transmits the packet with the new value.<br>• **set-frde-transmit** --Sets the Frame Relay discard eligible (DE) bit from 0 to 1 on the Frame Relay frame and sends the packet with the DE bit set to 1.<br>• **set-mpls-exp-transmit** --Sets the Multiprotocol Label Switching (MPLS) experimental bits from 0 to 7 and sends the packet with the new MPLS experimental bit value setting.<br>• **set-prec-transmit** *new-prec* --Sets the IP precedence and sends the packet with the new IP precedence value setting.<br>• **set-prec-tunnel-transmit** *value* --Sets the precedence value (0 to 7) in the tunnel header of an L2TPv3 or GRE tunneled packet for tunnel marking and transmits the packet with the new value.<br>• **set-qos-transmit** *new-qos* --Sets the quality of service (QoS) group value and sends the packet with the new QoS group value setting.<br>• **transmit** --Sends the packet with no alteration. |

**Command Default** Traffic policing using two rates is disabled.

**Command Modes** Policy-map class configuration (config-pmap-c)

**Command History**

| Release | Modification |
|---|---|
| 12.0(5)XE | This command was introduced. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(5)T | This command was modified. The **violate-action** keyword was added. |
| 12.2(2)T | This command was modified. The following keywords for the *action* argument were added:<br>• **set-clp-transmit**<br>• **set-frde-transmi** t<br>• **set-mpls-exp-transmit** |
| 12.2(4)T | This command was modified. The **cir** and **pir** keywordswere added to accommodate two-rate traffic policing. |
| 12.2(28)SB | This command was modified. The **set-dscp-tunnel-transmit** and **set-prec-tunnel-transmit** keywords for the *action* argument were added. These keywords are intended for marking Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunneled packets. |
| 12.2(33)SRA | This command was modified. The **set-cos-inner-transmit** keyword for the action argument was added when using multipoint bridging (MPB) features on the Enhanced FlexWAN module, and when using MPB on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SRC | This command was modified to support the Cisco 7600 series router equipped with a Cisco Multilayer Switch Feature Card 3 (MSFC3). |
| 12.4(15)T2 | This command was modified to include support for marking Generic Routing Encapsulation (GRE) tunneled packets.<br>**Note** For this release, marking GRE-tunneled packets is supported only on platforms equipped with a Cisco MGX Route Processor Module (RPM-XF). |
| 12.2(33)SB | This command was modified to include support for marking GRE-tunneled packets, and support for the Cisco 7300 series router was added. |

| Release | Modification |
|---|---|
| 12.4(20)T | This command was modified. Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC). |
| 15.0(1)SY | This command was modified. The maximum value for the *cir*, *conform-burst*, and *pir* arguments was increased. |

## Usage Guidelines

### Configuring Priority with an Explicit Policing Rate

When you configure a priority class with an explicit policing rate, traffic is limited to the policer rate regardless of congestion conditions. In other words, even if bandwith is available, the priority traffic cannot exceed the rate specified with the explicit policer.

### Token Buckets

Two-rate traffic policing uses two token buckets--Tc and Tp--for policing traffic at two independent rates. Note the following points about the two token buckets:

- The Tc token bucket is updated at the CIR value each time a packet arrives at the two-rate policer. The Tc token bucket can contain up to the confirm burst (Bc) value.
- The Tp token bucket is updated at the PIR value each time a packet arrives at the two-rate policer. The Tp token bucket can contain up to the peak burst (Be) value.

### Updating Token Buckets

The following scenario illustrates how the token buckets are updated:

A packet of B bytes arrives at time t. The last packet arrived at time t1. The CIR and the PIR token buckets at time t are represented by Tc(t) and Tp(t), respectively. Using these values and in this scenario, the token buckets are updated as follows:

Tc(t) = min(CIR * (t-t1) + Tc(t1), Bc)

Tp(t) = min(PIR * (t-t1) + Tp(t1), Be)

### Marking Traffic

The two-rate policer marks packets as either conforming, exceeding, or violating a specified rate. The following points (using a packet of B bytes) illustrate how a packet is marked:

- If B > Tp(t), the packet is marked as violating the specified rate.
- If B > Tc(t), the packet is marked as exceeding the specified rate, and the Tp(t) token bucket is updated as Tp(t) = Tp(t) - B.

Otherwise, the packet is marked as conforming to the specified rate, and both token buckets--Tc(t) and Tp(t)--are updated as follows:

Tp(t) = Tp(t) - B

Tc(t) = Tc(t) - B

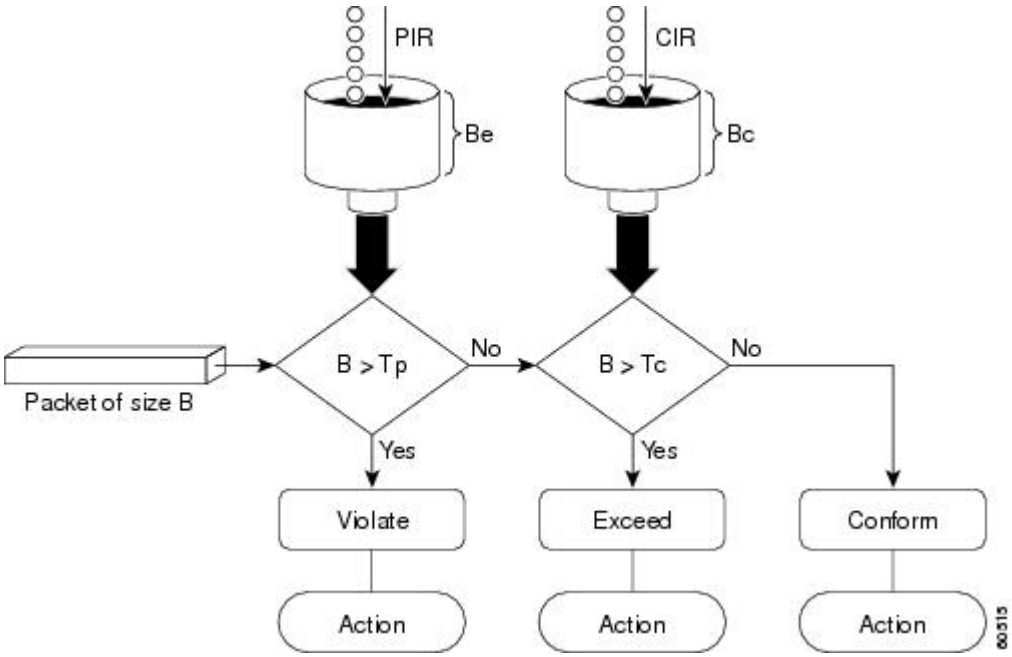
For example, if the CIR is 100 kbps, the PIR is 200 kbps, and a data stream with a rate of 250 kbps arrives at the two-rate policer, the packet would be marked as follows:

- 100 kbps would be marked as conforming to the rate.
- 100 kbps would be marked as exceeding the rate.
- 50 kbps would be marked as violating the rate.

### Marking Packets and Assigning Actions Flowchart

The flowchart in the figure illustrates how the two-rate policer marks packets and assigns a corresponding action (that is, violate, exceed, or conform) to the packet.

***Figure 31: Marking Packets and Assigning Actions with the Two-Rate Policer***




### Using the set-cos-inner-transmit Action for SIPs and SPAs on the Cisco 7600 Series Router

The **set-cos-inner-transmit** keyword action was introduced in Cisco IOS Release 12.2(33)SRA to support marking of the inner CoS value as a policing action when using MPB features on the Enhanced FlexWAN module, and when using MPB features on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router.

This command is not supported on the Cisco 7600 SIP-600.

For more information about QoS and the forms of **police** commands supported by the SIPs on the Cisco 7600 series router, see the *Cisco 7600 Series SIP, SSC, and SPA Software Configuration Guide*.

## Examples

## Examples

In the following example, priority traffic is limited to a committed rate of 1000 kbps regardless of congestion conditions in the network:

```
Router(config)# policy-map p1
Router(config-pmap)# class c1
Router(config-pmap-c)# police cir 1000000 conform-action transmit exceed-action drop
```

## Examples

In the following example, two-rate traffic policing is configured on a class to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps:

```
Router(config)# class-map police
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class police
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
 transmit exceed-action set-prec-transmit 2 violate-action drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial3/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
Router# show policy-map policy1
 Policy Map policy1
  Class police
   police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action transmit
 exceed-action set-prec-transmit 2 violate-action drop
```

Traffic marked as conforming to the average committed rate (500 kbps) will be sent as is. Traffic marked as exceeding 500 kbps, but not exceeding 1 Mbps, will be marked with IP Precedence 2 and then sent. All traffic marked as exceeding 1 Mbps will be dropped. The burst parameters are set to 10000 bytes.

In the following example, 1.25 Mbps of traffic is sent ("offered") to a policer class:

```
Router# show policy-map interface serial3/0
 Serial3/0
  Service-policy output: policy1
   Class-map: police (match all)
    148803 packets, 36605538 bytes
    30 second offered rate 1249000 bps, drop rate 249000 bps
    Match: access-group 101
    police:
     cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
     conformed 59538 packets, 14646348 bytes; action: transmit
     exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
     violated 29731 packets, 7313826 bytes; action: drop
     conformed 499000 bps, exceed 500000 bps violate 249000 bps
   Class-map: class-default (match-any)
    19 packets, 1990 bytes
    30 seconds offered rate 0 bps, drop rate 0 bps
    Match: any
```

The two-rate policer marks 500 kbps of traffic as conforming, 500 kbps of traffic as exceeding, and 250 kbps of traffic as violating the specified rate. Packets marked as conforming to the rate will be sent as is, and packets marked as exceeding the rate will be marked with IP Precedence 2 and then sent. Packets marked as violating the rate are dropped.

## Examples

The following example shows configuration of a QoS class that filters all traffic for virtual LAN (VLAN) 100 into a class named "vlan-inner-100," and establishes a traffic shaping policy for the vlan-inner-100 class. The service policy limits traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps and sets the inner CoS value to 3. Since setting of the inner CoS value is only supported with bridging features, the configuration also shows the service policy being applied as an output policy for an ATM SPA interface permanent virtual circuit (PVC) that bridges traffic into VLAN 100 using the **bridge-domain** command.

```
Router(config)# class-map match-all vlan-inner-100
Router(config-cmap)# match vlan inner 100
Router(config-cmap)# exit
Router(config)# policy-map vlan-inner-100
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
set-cos-inner-transmit 3
```

```
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm3/0/0
Router(config-if)# pvc 100/100
Router(config-if-atm-vc)# bridge-domain 100 dot1q
Router(config-if-atm-vc)# service-policy output vlan-inner-100
Router(config-if-atm-vc)# end
```

## Related Commands

| Command | Description |
|---|---|
| **bridge-domain** | Enables RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged VLAN to an ATM PVC or Frame Relay DLCI. |
| **police** | Configures traffic policing. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **service-policy** | Attaches a policy map to an input interface or an output interface to be used as the service policy for that interface. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# police rate (control-plane)

To configure traffic policing for traffic that is destined for the control plane, use the **police rate** command in QoS policy-map class configuration mode or control plane configuration mode. To remove traffic policing from the configuration, use the **no** form of this command.

**police rate** *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**] [**peak-burst** *peak-burst-in-packets* **packets**] [**conform-action action**]

**no police rate** *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**] [**peak-burst** *peak-burst-in-packets* **packets**] [**conform-action action**]

### Syntax for Packets per Seconds (pps)

**police rate units pps** [**burst burst-in-packets packets**] [**peak-rate peak-rate-in-pps pps**] [**peak-burst peak-burst-in-packets packets**]

**no police rate units pps** [**burst burst-in-packets packets**] [**peak-rate peak-rate-in-pps pps**] [**peak-burst peak-burst-in-packets packets**]

### Syntax for Bytes per Seconds (bps)

**police rate** *units* **bps** [**burst** *burst-in-bytes* **bytes**] [**peak-rate** *peak-rate-in-bps* **bps**] [**peak-burst** *peak-burst-in-bytes* **bytes**]

**no police rate** *units* **bps** [**burst** *burst-in-bytes* **bytes**] [**peak-rate** *peak-rate-in-bps* **bps**] [**peak-burst** *peak-burst-in-bytes* **bytes**]

### Syntax for Percent

**police rate percent** *percentage* [**burst** *ms* **ms**] [**peak-rate percent** *percentage*] [**peak-burst** *ms* **ms**]

**no police rate percent** *percentage* [**burst** *ms* **ms**] [**peak-rate percent** *percentage*] [**peak-burst** *ms* **ms**]

### Syntax for Cisco 10000 Series Router

**police rate** *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**] [**peak-burst** *peak-burst-in-packets* **packets**] [**conform-action action**] [**exceed-action action**] [**violate-action action**]

**no police rate** *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**] [**peak-burst** *peak-burst-in-packets* **packets**] [**conform-action action**] [**exceed-action action**] [**violate-action action**]

### Syntax for Cisco 7600 Series Router with SIP-400

**police rate** *units* [**pps burst** *burst-in-packets* **packets**| **bps burst burst-in-bytes bytes**]

**no police rate** *units* [**pps burst** *burst-in-packets* **packets**| **bps burst** *burst-in-bytes* **bytes**]

## Syntax Description

| | |
|---|---|
| *units* | The police rate. If the police rate is specified in pps, the valid range of values is:<br>• Cisco 10000 series router--Valid range is 1 to 500000.<br>• Cisco 7600 series router with Cisco SIP-400--Valid range is 1 to 100.<br>• Other platforms--Valid range is 1 to 2000000.<br>If the police rate is specified in bps, the valid range of values is:<br>• Cisco 7600 series router with Cisco SIP-400--Valid range is 80 to 8000.<br>• Other platforms--Valid range is 8000 to 128000000000 (or 128 Gbps). |
| **pps** | Specifies that packets per seconds (pps) will be used to determine the rate at which traffic is policed. |
| **burst** *burst-in-packets* **packets** | (Optional) Specifies the burst rate, in packets, that will be used for policing traffic. Valid range of values are:<br>• Cisco 10000 series router--Valid range is 1 to 25000.<br>• Cisco 7600 series router with Cisco SIP-400--Valid range is 1 to 1000.<br>• Other platforms--Valid range is 1 to 512000. |
| **peak-rate** *peak-rate-in-pps* **pps** | (Optional) Specifies the peak information rate (PIR) that will be used for policing traffic and calculating the PIR. Valid range of values are:<br>• Cisco 10000 series router--Valid range is 1 to 500000.<br>• Other platforms--Valid range is 1 to 512000. |
| **peak-burst** *peak-burst-in-packets* **packets** | (Optional) Specifies the peak burst value, in packets, that will be used for policing traffic. Valid range of values are:<br>• Cisco 10000 series router--Valid range is 1 to 25000.<br>• Other platforms--Valid range is 1 to 512000. |

| | |
|---|---|
| **bps** | (Optional) Specifies that bits per second (bps) that will be used to determine the rate at which traffic is policed. |
| **burst** *burst-in-bytes* **bytes** | (Optional) Specifies the burst rate, in bytes, that will be used for policing traffic. Valid range of values are:<br>• Cisco 7600 series router with Cisco SIP-400--Valid range is 100 to 10000.<br>• Other platforms--Valid range is 1000 to 2000000000 (2 Gb). |
| **peak-rate** *peak-rate-in-bps* **bps** | (Optional) Specifies the peak rate value, in bytes, for the peak rate. Valid range is from 1000 to 512000000 . |
| **peak-burst** *peak-burst-in-bytes* **bytes** | (Optional) Specifies the peak burst value, in bytes, that will be used for policing traffic. Valid range is 1000 to 2000000000 (2 Gb). |
| **percent** | Specifies a percentage of interface bandwidth that will be used to determine the rate at which traffic is policed. |
| *percentage* | The bandwidth percentage. Valid range is from 1 to 100. |
| **burst** *ms* **ms** | (Optional) Specifies the burst rate, in milliseconds, that will be used for policing traffic. Valid range is from 1 to 2000. |
| **peak-rate percent** *percentage* | (Optional) Specifies a percentage of interface bandwidth that will be used to determine the PIR. Valid range is from 1 to 100. |
| **peak-burst** *ms* **ms** | (Optional) Specifies the peak burst rate, in milliseconds, that will be used for policing traffic. Valid range is from 1 to 2000. |
| **conform-action** *action* | (Optional) Specifies the action to take on packets that conform to the police rate limit. See the “Usage Guidelines” section for the actions you can specify. |
| **exceed-action** *action* | (Optional) Specifies the action to take on packets that exceed the rate limit. See the “Usage Guidelines” section for the actions you can specify. |

| | |
|---|---|
| **violate-action** *action* | (Optional) Specifies the action to take on packets that continuously exceed the police rate limit. See the "Usage Guidelines" section for the actions you can specify. |

## Command Default

Disabled

## Command Modes

QoS policy-map class configuration (config-pmap)

Control plane configuration (config-cp)

## Command History

| Release | Modification |
|---|---|
| 12.3(7)T | This command was introduced. |
| 12.2(18)SXD1 | This command was modified. Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(25)S | This command was integrated into Cisco IOS Release 12.2(25)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2 and implemented on the Cisco 10000 series router. |
| 12.2(33)SRC | This command was modified to support CoPP enhancements on the Cisco 7600 SIP-400. |
| 15.0(1)SY | This command was modified. The maximum value for the *burst-in-bytes*, *peak-burst-in-bytes*, and *units* arguments was increased. |

## Usage Guidelines

Use the **police rate** command to limit traffic that is destined for the control plane on the basis of packets per second (pps), bytes per seconds (bps), or a percentage of interface bandwidth.

If the **police rate** command is issued, but the a rate is not specified, traffic that is destined for the control plane will be policed on the basis of bps.

The table below lists the actions you can specify for the *action* argument.

***Table 28: action Argument Values***

| Action | Description |
|---|---|
| **drop** | Drops the packet. This is the default action for traffic that exceeds or violates the committed police rate. |

| Action | Description |
|---|---|
| **set-clp-transmit** *value* | Sets the ATM Cell Loss Priority (CLP) bit on the ATM cell. Valid values are 0 or 1. |
| **set-discard-class-transmit** *value* | Sets the discard class attribute of a packet and transmits the packet with the new discard class setting. Valid values are from 0 to 7. |
| **set-dscp-transmit** *value* | Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value setting. Valid values are from 0 to 63. |
| **set-dscp-tunnel-transmit** *value* | Rewrites the tunnel packet DSCP and transmits the packet with the new tunnel DSCP value. Valid values are from 0 to 63. |
| **set-frde-transmit** *value* | Sets the Frame Relay Discard Eligibility (DE) bit from 0 to 1 on the Frame Relay frame and transmits the packet with the DE bit set to 1. |
| **set-mpls-exp-imposition-transmit** *value* | Sets the Multiprotocol Label Switching (MPLS) experimental (EXP) bits in the imposed label headers and transmits the packet with the new MPLS EXP bit value setting. Valid values are from 0 to 7. |
| **set-mpls-exp-transmit** *value* | Sets the MPLS EXP field value in the MPLS label header at the input interface, output interface, or both. Valid values are from 0 to 7. |
| **set-prec-transmit** *value* | Sets the IP precedence and transmits the packet with the new IP precedence value. Valid values are from 0 to 7. |
| **set-prec-tunnel-transmit** *value* | Sets the tunnel packet IP precedence and transmits the packet with the new IP precedence value. Valid values are from 0 to 7. |
| **set-qos-transmit** *value* | Sets the QoS group and transmits the packet with the new QoS group value. Valid values are from 0 to 63. |
| **transmit** | Transmits the packet. The packet is not altered. |

## Examples

The following example shows how to configure the action to take on packets that conform to the police rate limit:

```
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
Router(config)# access-list 140 permit tcp any any eq telnet
```

```
Router(config)# class-map match-any pps-1
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map copp-pps
Router(config-pmap)# class pps-1
Router(config-pmap)# police rate 10000 pps burst 100 packets peak-rate 10100 pps peak-burst
 150 packets conform-action transmit
Router(config-cmap)# exit
Router(config)# control-plane
Router(config-cp)# service-policy input copp-pps
Router(config-cp)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |

# police rate pdp

To configure Packet Data Protocol (PDP) traffic policing using the police rate, use the **police rate pdp** command in policy-map class configuration mode or policy-map class police configuration mode. To remove PDP traffic policing from the configuration, use the **no** form of this command.

**police rate pdp** [**burst** *bytes*] [**peak-rate pdp** [**peak-burst** *bytes*]] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

**no police rate pdp** [**burst** *bytes*] [**peak-rate pdp** [**peak-burst** *bytes*]] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

## Syntax Description

| | |
|---|---|
| **burst** *bytes* | (Optional) Specifies the committed burst size, in bytes. The size varies according to the interface and platform in use. Valid range is 1000 to 2000000000 (2 Gb). Default is 1500. |
| **peak-rate pdp** | (Optional) Specifies that the peak rate of sessions be considered when PDP traffic is policed. |
| **peak-burst** *bytes* | (Optional) Specifies the peak burst size, in bytes. The size varies according to the interface and platform in use. Valid range is 1000 to 2000000000 (2 Gb). Default is 2500. |
| **conform-action** | Specifies the action to take on packets when the rate is less than the conform burst. |
| **exceed-action** | Specifies the action to take on packets when the rate exceeds the conform burst. |
| **violate-action** | (Optional) Specifies the actionction to take on packets when the rate violates the conform burst. |
| *action* | The action to take on packets. Specify one of the following keywords:<br>• **drop** --Drops the packet.<br>• **set-dscp-transmit** *new-dscp-value* --Sets the IP differentiated services code point (DSCP) value and sends the packet with the new IP DSCP value.<br>• **set-prec-transmit** *new-prec-value* --Sets the IP precedence and sends the packet with the new IP precedence value.<br>• **transmit** --Sends the packet with no alteration. |

**Command Default** PDP traffic policing is disabled.

**Command Modes** Policy-map class configuration (config-pmap-c) Policy-map class police configuration (config-pmap-c-police)

**Command History**

| Release | Modification |
|---|---|
| 12.3(8)XU | This command was introduced. |
| 12.3(11)YJ | This command was integrated into Cisco IOS Release 12.3(11)YJ. |
| 12.3(14)YQ | This command was integrated into Cisco IOS Release 12.3(14)YQ. |
| 12.4(9)T | This command was integrated into Cisco IOS Release 12.4(9)T. |
| 15.0(1)SY | This command was modified. The maximum value for the *bytes* argument was increased. |

**Usage Guidelines** The **police rate pdp** command is included with the Flow-Based QoS for GGSN feature available with Cisco IOS Release 12.4(9)T.

The Flow-Based QoS for GGSN feature is designed specifically for the Gateway General Packet Radio Service (GPRS) Support Node (GGSN).

**Per-PDP Policing**

The Flow-Based QoS for GGSN feature includes per-PDP policing (session-based policing).

Per-PDP policing is a gateway GPRS support node traffic conditioner (3G TS 23.107) function that can be used to limit the maximum rate of traffic received on the Gi interface for a particular PDP context.

The policing function enforces the call admission control (CAC)-negotiated data rates for a PDP context. The GGSN can be configured to either drop nonconforming traffic or mark nonconforming traffic for preferential dropping if congestion should occur.

The policing parameters used depend on the PDP context, such as the following:

- For GTPv1 PDPs with R99 quality of service (QoS) profiles, the maximum bit rate (MBR) and guaranteed bit rate (GBR) parameters from the CAC-negotiated QoS profile are used. For nonreal time traffic, only the MBR parameter is used.
- For GTPv1 PDPs with R98 QoS profiles and GTPv0 PDPs, the peak throughput parameter from the CAC-negotiated QoS policy is used.

Before configuring per-PDP policing, note the following points:

- Universal Mobile Telecommunications System (UMTS) QoS mapping must be enabled on the GGSN.
- Cisco Express Forwarding (CEF) must be enabled on the Gi interface.
- Per-PDP policing is supported for downlink traffic at the Gi interface only.

- The initial packets of a PDP context are not policed.
- Hierarchical policing is not supported.
- If flow-based policing is configured in a policy map that is attached to an Access Point Network (APN), the **show policy-map apn** command displays the total number of packets received before policing and does not display the policing counters.

**Note** To clear policing counters displayed by the **showpolicy-mapapn** command, use the **clear gprs access-point statistics***access-point-index*command.

- A service policy that has been applied to an APN cannot be modified. To modify a service policy, remove the service policy from the APN, modify it, and then reapply the service policy.
- Multiple class maps, each with **match flow pdp** configured and a different differentiated services code point (DSCP) value specified, are supported in a policy map only if the DSCP is trusted (the **gprs umts-qos dscp unmodified** global configuration command has not been configured on the GGSN).

**For More Information**

For more information about the GGSN, along with the instructions for configuring the Flow-Based QoS for GGSN feature, see the "*Cisco GGSN Release 6.0 Configuration Guide*" , Cisco IOS Release 12.4(2)XB.

**Note** To configure the Flow-Based QoS for GGSN feature, follow the instructions in the section called "Configuring Per-PDP Policing ."

For more information about the **show policy-map apn** command, the **gprs umts-qos dscp unmodified** command, the **clear gprs access-point statistics** command, and other GGSN-specific commands, see the "*Cisco GGSN Release 6.0 Command Reference*", Cisco IOS Release 12.4(2)XB.

## Examples

The following is an example of a per-PDP policing policy map applied to an APN:

```
class-map match-all class-pdp
 match flow pdp
!
! Configures a policy map and attaches this class map to it.
policy-map policy-gprs
 class class-pdp
  police rate pdp
    conform-action set-dscp-transmit 15
    exceed-action set-dscp-transmit 15
    violate-action drop
! Attaches the policy map to the APN.

gprs access-point-list gprs
  access-point 1
   access-point-name static
   service-policy input policy-gprs
```

## Related Commands

| Command | Description |
|---|---|
| **clear gprs access-point statistics** | Clears statistics counters for a specific access point or for all access points on the GGSN. |
| **gprs umts-qos dscp unmodified** | Specifies that the subscriber datagram be forwarded through the GTP path without modifying its DSCP. |
| **match flow pdp** | Specifies PDP flows as the match criterion in a class map. |
| **show policy-map apn** | Displays statistical and configuration information for all input and output policies attached to an APN. |

# policy-map

To enter policy-map configuration mode and create or modify a policy map that can be attached to one or more interfaces to specify a service policy, use the **policy-map**command in global configuration mode. To delete a policy map, use the **no** form of this command.

### Supported Platforms Other Than Cisco 10000 and Cisco 7600 Series Routers

**policy-map** [**type** {**stack**| **access-control**| **port-filter**| **queue-threshold**| **logging** *log-policy*}] *policy-map-name*

**no policy-map** [**type** {**stack**| **access-control**| **port-filter**| **queue-threshold**| **logging** *log-policy*}] *policy-map-name*

### Cisco 10000 Series Router

**policy-map** [**type** {**control**| **service**}] *policy-map-name*

**no policy-map** [**type** {**control**| **service**}] *policy-map-name*

### Cisco CMTS and 7600 Series Router

**policy-map** [**type** {**class-routing ipv4 unicast** *unicast-name*| **control** *control-name*| **service** *service-name*}] *policy-map-name*

**no policy-map** [**type** {**class-routing ipv4 unicast** *unicast-name*| **control** *control-name*| **service** *service-name*}] *policy-map-name*

## Syntax Description

| | |
|---|---|
| **type** | (Optional) Specifies the policy-map type. |
| **stack** | (Optional) Determines the exact pattern to look for in the protocol stack of interest. |
| **access-control** | (Optional) Enables the policy map for the flexible packet matching feature. |
| **port-filter** | (Optional) Enables the policy map for the port-filter feature. |
| **queue-threshold** | (Optional) Enables the policy map for the queue-threshold feature. |
| **logging** | (Optional) Enables the policy map for the control-plane packet logging feature. |
| *log-policy* | (Optional) Type of log policy for control-plane logging. |
| *policy-map-name* | Name of the policy map. |
| **control** | (Optional) Creates a control policy map. |

| | |
|---|---|
| *control-name* | Name of the control policy map. |
| **service** | (Optional) Creates a service policy map. |
| *service-name* | Name of the policy-map service. |
| **class-routing** | Configures the class-routing policy map. |
| **ipv4** | Configures the class-routing IPv4 policy map. |
| **unicast** | Configures the class-routing IPv4 unicast policy map. |
| *unicast-name* | Unicast policy-map name. |

**Command Default**

The policy map is not configured.

**Command Modes**

Global configuration (config)

**Command History**

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.4(4)T | This command was modified. The **type** and**access-control**keywords were added to support flexible packet matching. The **port-filter** and **queue-threshold** keywords were added to support control-plane protection. |
| 12.4(6)T | This command was modified. The **logging** keyword was added to support control-plane packet logging. |
| 12.2(31)SB | This command was modified. The **control** and **service**keywords were added to support the Cisco 10000 series router. |
| 12.2(18)ZY | This command was modified.<br>• The **type** and**access-control**keywords were integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series switch that is equipped with the Supervisor 32/programmable intelligent services accelerator (PISA) engine.<br>• The command was modified to enhance the Network-Based Application Recognition (NBAR) functionality on the Catalyst 6500 series switch that is equipped with the Supervisor 32/PISA engine. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

| Release | Modification |
|---|---|
| 12.2(33)SRC | This command was modified. Support for this command was implemented on Cisco 7600 series routers. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 series routers. |
| 12.2(33)SCF | This command was integrated into Cisco IOS Release 12.2(33)SCF. |

## Usage Guidelines

Use the **policy-map** command to specify the name of the policy map to be created, added, or modified before you configure policies for classes whose match criteria are defined in a class map. The **policy-map** command enters policy-map configuration mode, in which you can configure or modify the class policies for a policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. Use the **class-map** and **match** commands to configure match criteria for a class. Because you can configure a maximum of 64 class maps, a policy map cannot contain more than 64 class policies, except as noted for quality of service (QoS) class maps on Cisco 7600 systems.

**Note** For QoS class maps on Cisco 7600 series routers, the limits are 1024 class maps and 256 classes in a policy map.

A policy map containing ATM set cell loss priority (CLP) bit QoS cannot be attached to PPP over X (PPPoX) sessions. The policy map is accepted only if you do not specify the **set atm-clp** command.

A single policy map can be attached to more than one interface concurrently. Except as noted, when you attempt to attach a policy map to an interface, the attempt is denied if the available bandwidth on the interface cannot accommodate the total bandwidth requested by class policies that make up the policy map. In such cases, if the policy map is already attached to other interfaces, the map is removed from those interfaces.

**Note** This limitation does not apply on Cisco 7600 series routers that have session initiation protocol (SIP)-400 access-facing line cards.

Whenever you modify a class policy in an attached policy map, class-based weighted fair queuing (CBWFQ) is notified and the new classes are installed as part of the policy map in the CBWFQ system.

**Note** Policy-map installation via subscriber-profile is not supported. If you configure an unsupported policy map and there are a large number of sessions, an equally large number of messages print on the console. For example, if there are 32,000 sessions, then 32,000 messages print on the console at 9,600 baud.

### Class Queues (Cisco 10000 Series Routers Only)

The Performance Routing Engine (PRE)2 allows you to configure 31 class queues in a policy map.

In a policy map, the PRE3 allows you to configure one priority level 1 queue, one priority level 2 queue, 12 class queues, and one default queue.

### Control Policies (Cisco 10000 Series Routers Only)

Control policies define the actions that your system will take in response to the specified events and conditions.

A control policy is made of one or more control policy rules. A control policy rule is an association of a control class and one or more actions. The control class defines the conditions that must be met before the actions are executed.

There are three steps involved in defining a control policy:

1 Using the **class-map type control** command, create one or more control class maps.

2 Using the **policy-map type control** command, create a control policy map.

A control policy map contains one or more control policy rules. A control policy rule associates a control class map with one or more actions. Actions are numbered and executed sequentially.

1 Using the **service-policy type control** command, apply the control policy map to a context.

### Service Policies (Cisco 10000 Series Routers Only)

Service policy maps and service profiles contain a collection of traffic policies and other functions. Traffic policies determine which function is applied to which session traffic. A service policy map or service profile may also contain a network-forwarding policy, which is a specific type of traffic policy that determines how session data packets will be forwarded to the network.

### Policy Map Restrictions (Catalyst 6500 Series Switches Only)

Cisco IOS Release 12.2(18)ZY includes software intended for use on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine. This release and platform has the following restrictions for using policy maps and **match** commands:

- You cannot modify an existing policy map if the policy map is attached to an interface. To modify the policy map, remove the policy map from the interface by using the **no** form of the **service-policy** command.
- Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) on the basis of a protocol type or application. You can create as many traffic classes as needed. However, the following restrictions apply:
  - A single traffic class can be configured to match a maximum of 8 protocols or applications.
  - Multiple traffic classes can be configured to match a cumulative maximum of 95 protocols or applications.

## Examples

The following example shows how to create a policy map called “policy1” and configure two class policies included in that policy map. The class policy called “class1” specifies a policy for traffic that matches access control list (ACL) 136. The second class is the default class to which packets that do not satisfy the configured match criteria are directed.

```
! The following commands create class-map class1 and define its match criteria:
class-map class1
```

```
 match access-group 136
! The following commands create the policy map, which is defined to contain policy
! specification for class1 and the default class:
policy-map policy1
class class1
 bandwidth 2000
 queue-limit 40
class class-default
 fair-queue 16
 queue-limit 20
```

The following example shows how to create a policy map called “policy9” and configure three class policies to belong to that map. Of these classes, two specify the policy for classes with class maps that specify match criteria based on either a numbered ACL or an interface name, and one specifies a policy for the default class called “class-default” to which packets that do not satisfy the configured match criteria are directed.

```
policy-map policy9

class acl136
 bandwidth 2000
 queue-limit 40

class ethernet101
 bandwidth 3000
 random-detect exponential-weighting-constant 10
class class-default
 fair-queue 10
 queue-limit 20
```

The following is an example of a modular QoS command-line interface (MQC) policy map configured to initiate the QoS service at the start of a session.

```
Router> enable
Router# configure terminal
Router(config)# policy-map type control TEST
Router(config-control-policymap)# class type control always event session-start
Router(config-control-policymap-class-control)# 1
 service-policy type service name QoS_Service
Router(config-control-policymap-class-control)# end
```

## Examples

The following example shows the configuration of a control policy map named “rule4”. Control policy map rule4 contains one policy rule, which is the association of the control class named “class3” with the action to authorize subscribers using the network access server (NAS) port ID. The **service-policy type control** command is used to apply the control policy map globally.

```
class-map type control match-all class3
 match access-type pppoe
 match domain cisco.com
 available nas-port-id
!
policy-map type control rule4
 class type control class3
  authorize nas-port-id
!
service-policy type control rule4
```

The following example shows the configuration of a service policy map named “redirect-profile”:

```
policy-map type service redirect-profile
 class type traffic CLASS-ALL
  redirect to group redirect-sg
```

## Examples

The following example shows how to define a policy map for the 802.1p domain:

```
enable
configure terminal
 policy-map cos7
  class cos7
  set cos 2
  end
```

The following example shows how to define a policy map for the MPLS domain:

```
enable
configure terminal
 policy-map exp7
  class exp7
  set mpls experimental topmost 2
  end
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth (policy-map class)** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map. |
| **class (policy-map)** | Specifies the name of the class whose policy you want to create or change, and its default class before you configure its policy. |
| **class class-default** | Specifies the default class whose bandwidth is to be configured or modified. |
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **fair-queue (class-default)** | Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy. |
| **match access-group** | Configures the match criteria for a class map on the basis of the specified ACL. |
| **queue-limit** | Specifies or modifies the maximum number of packets that the queue can hold for a class policy configured in a policy map. |
| **random-detect (interface)** | Enables WRED or DWRED. |
| **random-detect exponential-weighting-constant** | Configures the WRED and DWRED exponential weight factor for the average queue size calculation. |
| **random-detectservice-policy precedence** | Configures WRED and DWRED parameters for a particular IP precedence. |

| Command | Description |
|---|---|
| **service-policy** | Attaches a policy map to an input interface or VC or an output interface or VC to be used as the service policy for that interface or VC. |
| **set atm-clp precedence** | Sets the ATM CLP bit when a policy map is configured. |

# policy-map copp-peruser

To create a policy map that defines a Control Plane Policing and Protection (CoPP) per-user policy, use the **policy-mapcopp-peruser**command in global configuration mode. To disable, use the **no** form of the command.

**policy-map copp-peruser**

**no policy-map copp-peruser**

## Syntax Description

This command has no keywords or arguments.

## Command Default

No policy map is configured.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRB | This command was introduced. |

## Usage Guidelines

Use this command to create a CoPP per-user policy map when configuring CoPP.

## Examples

The following example creates a CoPP per-user policy map:

```
Router(config)# policy-map copp-peruser
Router(config-pmap)# class arp-peruser
Router(config-pmap-c)# police rate 5 pps burst 50 packets
Router(config-pmap-c)# class dhcp-peruser
Router(config-pmap-c)# police rate 10 pps burst 100 packets
```

## Related Commands

| Command | Description |
|---|---|
| **class-map arp-peruser** | Creates a class map to be used for matching ARP per-user packets. |
| **match subscriber access** | Matches subscriber access traffic to a policy map. |

# precedence

To configure precedence levels for a virtual circuit (VC) class that can be assigned to a VC bundle and thus applied to all VC members of that bundle, use the **precedence** command in vc-class configuration mode. To remove the precedence levels from the VC class, use the **no** form of this command.

To configure the precedence levels for a VC or permanent virtual circuit (PVC) member of a bundle, use the **precedence** command in bundle-vc configuration mode for ATM VC bundle members, or in switched virtual circuit (SVC)-bundle-member configuration mode for an ATM SVC. To remove the precedence levels from the VC or PVC, use the **no** form of this command.

**precedence** [**other**| *range*]

**no precedence**

## Syntax Description

| | |
|---|---|
| **other** | (Optional) Any precedence levels in the range from 0 to 7 that are not explicitly configured. |
| *range* | (Optional) A single precedence level specified either as a number from 0 to 7 or a range of precedence levels, specified as a hyphenated range. |

## Command Default

Defaults to **other**--that is, any precedence levels in the range from 0 to 7 that are not explicitly configured.

## Command Modes

VC-class configuration (for a VC class) Bundle-vc configuration (for ATM VC bundle members) SVC-bundle-member configuration (for an ATM SVC)

## Command History

| Release | Modification |
|---|---|
| 11.1(22)CC | This command was introduced. |
| 12.0(3)T | This command was integrated into Cisco IOS Release 12.0(3)T. This command was extended to configure precedence levels for a VC member of a bundle. |
| 12.2(4)T | This command was made available in SVC-bundle-member configuration mode. |
| 12.0(23)S | This command was made available in vc-class and bundle-vc configuration modes on the 8-port OC-3 STM-1 ATM line card for Cisco 12000 series Internet routers. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Assignment of precedence levels to VC or PVC bundle members allows you to create differentiated service because you can distribute the IP precedence levels over the various VC/PVC bundle members. You can map a single precedence level or a range of levels to each discrete VC/PVC in the bundle, thereby enabling VCs/PVCs in the bundle to carry packets marked with different precedence levels. Alternatively, you can use the **precedenceother** command to indicate that a VC/PVC can carry traffic marked with precedence levels not specifically configured for other VCs/PVCs. Only one VC/PVC in the bundle can be configured using the **precedenceother** command. This VC/PVC is considered the default one.

To use this command in vc-class configuration mode, first enter the **vc-classatm** command in global configuration mode. The **precedence** command has no effect if the VC class that contains the command is attached to a standalone VC; that is, if the VC is not a bundle member.

To use the **precedence** command to configure an individual bundle member in bundle-VC configuration mode, first enter the **bundle** command to enact bundle configuration mode for the bundle to which you want to add or modify the VC member to be configured. Then use the **pvc-bundle** command to specify the VC to be created or modified and enter bundle-VC configuration mode.

VCs in a VC bundle are subject to the following configuration inheritance guidelines (listed in order of next-highest precedence):

- VC configuration in bundle-vc mode
- Bundle configuration in bundle mode (with effect of assigned vc-class configuration)
- Subinterface configuration in subinterface mode

## Examples

The following example configures a class called “control-class” that includes a **precedence** command that, when applied to a bundle, configures all VC members of that bundle to carry IP precedence level 7 traffic. Note, however, that VC members of that bundle can be individually configured with the **precedence** command at the bundle-vc level, which would supervene.

```
vc-class atm control-class
 precedence 7
```

The following example configures PVC 401 (with the name of “control-class”) to carry traffic with IP precedence levels in the range of 4-2, overriding the precedence level mapping set for the VC through vc-class configuration:

```
pvc-bundle control-class 401
 precedence 4-2
```

## Related Commands

| Command | Description |
|---|---|
| **bump** | Configures the bumping rules for a VC class that can be assigned to a VC bundle. |
| **bundle** | Creates a bundle or modifies an existing bundle to enter bundle configuration mode. |
| **class-vc** | Assigns a VC class to an ATM PVC, SVC, or VC bundle member. |

| Command | Description |
|---|---|
| **dscp (frame-relay vc-bundle-member)** | Specifies the DSCP value or values for a specific Frame Relay PVC bundle member. |
| **match precedence** | Identifies IP precedence values as match criteria. |
| **mpls experimental** | Configures the MPLS experimental bit values for a VC class that can be mapped to a VC bundle and thus applied to all VC members of that bundle. |
| **protect** | Configures a VC class with protected group or protected VC status for application to a VC bundle member. |
| **pvc-bundle** | Adds a PVC to a bundle as a member of the bundle and enters bundle-vc configuration mode in order to configure that PVC bundle member. |
| **pvc** | Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters interface-ATM-VC configuration mode. |
| **ubr** | Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member. |
| **ubr+** | Configures UBR QoS and specifies the output peak cell rate and output minimum guaranteed cell rate for an ATM PVC, SVC, VC class, or VC bundle member. |
| **vbr-nrt** | Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member. |
| **vc-class atm** | Configures a VC class for an ATM VC or interface. |

# precedence (WRED group)

To configure a Weighted Random Early Detection (WRED) or VIP-distributed WRED (DWRED) group for a particular IP Precedence, use the **precedence**command in random-detect-group configuration mode. To return the values for each IP Precedence for the group to the default values, use the **no** form of this command.

**precedence** *precedence min-threshold max-threshold mark-probability-denominator*

**no precedence** *precedence min-threshold max-threshold mark-probability-denominator*

## Syntax Description

| | |
|---|---|
| *precedence* | IP Precedence number. Values range from 0 to 7. |
| *min-threshold* | Minimum threshold in number of packets. Value range from 1 to 4096. When the average queue length reaches this number, WRED or DWRED begins to drop packets with the specified IP Precedence. |
| *max-threshold* | Maximum threshold in number of packets. The value range is *min-threshold* to 4096. When the average queue length exceeds this number, WRED or DWRED drops all packets with the specified IP Precedence. |
| *mark-probability-denominator* | Denominator for the fraction of packets dropped when the average queue depth is *max-threshold* . For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the *max-threshold* . The value is 1 to 65536. The default is 10; 1 out of every 10 packets is dropped at the *max-threshold* . |

## Command Default

For all IP Precedences, the *mark-probability-denominator* argument is 10, and the *max-threshold* argument is based on the output buffering capacity and the transmission speed for the interface.

The default *min-threshold* argument depends on the IP Precedence. The *min-threshold* argument for IP Precedence 0 corresponds to half of the *max-threshold*argument. The values for the remaining IP Precedences fall between half the *max-threshold* argument and the *max-threshold* argument at evenly spaced intervals. See the table below in the “Usage Guidelines” section for a list of the default minimum value for each IP Precedence.

## Command Modes

Random-detect-group configuration

## Command History

| Release | Modification |
|---|---|
| 11.1(22)CC | This command was introduced. |

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. DWRED is similar to WRED but uses the Versatile Interface Processor (VIP) instead of the Route Switch Processor (RSP).

If used, this command is issued after the **random-detect-group** command.

When you configure the **random-detectgroup**command on an interface, packets are given preferential treatment based on the IP Precedence of the packet. Use the **precedence** command to adjust the treatment for different IP Precedences.

If you want WRED or DWRED to ignore the IP Precedence when determining which packets to drop, enter this command with the same parameters for each IP Precedence. Remember to use reasonable values for the minimum and maximum thresholds.

**Note** The default WRED or DWRED parameter values are based on the best available data. We recommend that you do not change the parameters from their default values unless you have determined that your applications would benefit from the changed values.

The table below lists the default minimum value for each IP Precedence.

***Table 29: Default WRED Minimum Threshold Values***

| IP Precedence | Minimum Threshold Value (Fraction of Maximum Threshold Value) |
|---|---|
| 0 | 8/16 |
| 1 | 9/16 |
| 2 | 10/16 |
| 3 | 11/16 |
| 4 | 12/16 |
| 5 | 13/16 |
| 6 | 14/16 |
| 7 | 15/16 |

## Examples

The following example specifies parameters for the WRED parameter group called sanjose for the different IP Precedences:

```
random-detect-group sanjose
 precedence 0 32 256 100
 precedence 1 64 256 100
 precedence 2 96 256 100
 precedence 3 128 256 100
 precedence 4 160 256 100
 precedence 5 192 256 100
 precedence 6 224 256 100
 precedence 7 256 256 100
```

## Related Commands

| Command | Description |
|---|---|
| **exponential-weighting-constant** | Configures the exponential weight factor for the average queue size calculation for a WRED parameter group. |
| **random-detect (per VC)** | Enables per-VC WRED or per-VC DWRED. |
| **random-detect-group** | Defines the WRED or DWRED parameter group. |
| **random-detect precedence** | Configures WRED and DWRED parameters for a particular IP Precedence. |
| **show queueing** | Lists all or selected configured queueing strategies. |
| **show queueing interface** | Displays the queueing statistics of an interface or VC. |

# preempt-priority

To specify the Resource Reservation Protocol (RSVP) quality of service (QoS) priorities to be inserted into PATH and RESV messages if they were not signaled from an upstream or downstream neighbor or local client application, use the **preempt-priority** command in local policy configuration mode. To delete the priorities, use the **no** form of this command.

**preempt-priority** [**traffic-eng** *x*] *setup-priority* [ *hold-priority* ]

**no preempt-priority** [**traffic-eng** *x*] *setup-priority* [ *hold-priority* ]

## Syntax Description

| | |
|---|---|
| **traffic-eng** *x* | (Optional) Indicates the upper limit of the priority for Traffic Engineering (TE) reservations. The range of *x*values is 0 to 7 in which the smaller the number, the higher the reservation's priority. For non-TE reservations, the range of *x*values is 0 to 65535 in which the higher the number, the higher the reservation's priority. |
| *setup-priority* | Indicates the priority of a reservation when it is initially installed. Values range from 0 to 7 where 0 is considered the highest priority. For TE reservations, the default value is 7; for non-TE reservations, the default is 0. |
| *hold-priority* | (Optional) Indicates the priority of a reservation after it has been installed. If omitted, this argument defaults to the *setup-priority*. Values range from 0 to 7 where 0 is considered the highest priority. For TE reservations, the default value is 7; for non-TE reservations, the default is 0. |

## Command Default

No RSVP QoS priorities are specified until you configure them.

## Command Modes

Local policy configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |

## Usage Guidelines

Use the **preempt-priority** command to specify the maximum setup or hold priority that RSVP QoS or MPLS/TE sessions can signal. A PATHERROR, RESVERROR, or local application error is returned if these limits are exceeded.

If an incoming message has a preemption priority that requests a priority higher than the policy allows, the message is rejected. Use the tunnel mpls traffic-eng priority command to configure preemption priority for TE tunnels.

A single policy can contain a preempt-priority traffic-eng and a preempt-priority command, which may be useful if the policy is bound to an access control list (ACL) that identifies a subnet containing a mix of TE and non-TE endpoints or midpoints.

When selecting reservations for preemption, RSVP preempts lower-priority reservations before those with higher priority. If there are multiple nonTE reservations with the same preemption priority, RSVP selects the oldest reservations first.

## Examples

The following example has a setup priority of 0 and a hold priority of 5:

```
Router(config-rsvp-local-policy)# preempt-priority 0 5
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp policy local** | Determines how to perform authorization on RSVP requests. |
| **ip rsvp policy preempt** | Enables RSVP to take bandwidth from lower-priority reservations and give it to new, higher-priority reservations. |
| **tunnel mpls traffic-eng priority** | Configures the setup and reservation priorities for an MPLS TE tunnel. |

# priority

To give priority to a class of traffic belonging to a policy map, use the **priority** command in policy-map class configuration mode. To remove a previously specified priority for a class, use the **no** form of this command.

**priority** {*bandwidth-kbps*| **percent** *percentage*} [ *burst* ]

**no priority** {*bandwidth-kbps*| **percent** *percentage*} [ *burst* ]

## Syntax Description

| | |
|---|---|
| *bandwidth-kbps* | Guaranteed allowed bandwidth, in kilobits per second (kbps), for the priority traffic. The amount of guaranteed bandwidth varies according to the interface and platform in use. Beyond the guaranteed bandwidth, the priority traffic will be dropped in the event of congestion to ensure that the nonpriority traffic is not starved. The value must be between 1 and 2,000,000 kbps. |
| **percent** | Specifies that the amount of guaranteed bandwidth will be specified by the percent of available bandwidth. |
| *percentage* | Total available bandwidth to be set aside for the priority class. The percentage can be a number from 1 to 100. |
| *burst* | (Optional) Burst size in bytes. The burst size configures the network to accommodate temporary bursts of traffic. The default burst value, which is computed as 200 milliseconds of traffic at the configured bandwidth rate, is used when theburst argument is not specified. The range of the burst is from 32 to 2000000 bytes. |

## Command Default

No priority is set.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.0(7)T | This command was introduced. |

| Release | Modification |
|---|---|
| 12.0(5)XE5 | This command was integrated into Cisco IOS Release 12.0(5)XE5 and implemented on the Versatile Interface Processor (VIP) as part of the Distributed Low Latency Queueing (Low Latency Queueing for the VIP) feature. |
| 12.0(9)S | This command was integrated into Cisco IOS Release 12.0(9)S and implemented on the VIP as part of the Distributed Low Latency Queueing (Low Latency Queueing for the VIP) feature. |
| 12.1(2)E | This command was modified. The *burst* argument was added. |
| 12.1(3)T | This command was integrated into Cisco IOS Release 12.1(3)T. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T and implemented on the VIP as part of the Distributed Low Latency Queueing (Low Latency Queueing for the VIP) feature. |
| 12.2(2)T | This command was modified. The **percent** keyword and the *percentage* argument were added. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE 2.1 and implemented on Cisco ASR 1000 Series Aggregation Services Routers. |
| 15.1(1)T | This command was modified. The allowed value for the *bandwidth-kbps* argument was changed. The value must be between 8 and 2,000,000 kbps. |
| 15.2(1)T | This command was modified. The allowed value for the *bandwidth-kbps* argument was changed. The value must be between 1 and 2,000,000 kbps. |
| 15.4(1)S | This command was implemented on the Cisco ASR 901 series routers. |

## Usage Guidelines

This command configures low latency queueing (LLQ), providing strict priority queueing (PQ) for class-based weighted fair queueing (CBWFQ). Strict PQ allows delay-sensitive data such as voice to be dequeued and sent before packets in other queues are dequeued.

The **priority** command allows you to set up classes based on a variety of criteria (not just User Datagram Ports [UDP] ports) and assign priority to them, and is available for use on serial interfaces and ATM permanent virtual circuits (PVCs). A similar command, the **iprtppriority**command, allows you to stipulate priority flows based only on UDP port numbers and is not available for ATM PVCs.

When the device is not congested, the priority class traffic is allowed to exceed its allocated bandwidth. When the device is congested, the priority class traffic above the allocated bandwidth is discarded.

The **bandwidth** and **priority** commands cannot be used in the same class, within the same policy map. These commands can be used together in the same policy map, however.

Within a policy map, you can give one or more classes priority status. When multiple classes within a single policy map are configured as priority classes, all traffic from these classes is queued to the same, single, priority queue.

When the policy map containing class policy configurations is attached to the interface to stipulate the service policy for that interface, available bandwidth is assessed. If a policy map cannot be attached to a particular interface because of insufficient interface bandwidth, the policy is removed from all interfaces to which it was successfully attached.

For more information on bandwidth allocation, see the chapter "Congestion Management Overview" in the *Cisco IOS Quality of Service Solutions Configuration Guide.*

**Note** On Cisco ASR 1000 Series Aggregation Services Routers, the use of a conditional priority rate limiter, such as *bandwidth-kbps* or *percentage*, is not supported in the lowest level (i.e. grandchild or leaf) of a three-layer policy map configuration. At the lowest level of a three level policy, the conditional limiter will not be applied. However, priority with a strict policer is supported at this level of the hierarchy. This restriction does not apply to flat or two level hierarchical policy maps.

## Examples

The following example shows how to configure PQ with a guaranteed bandwidth of 50 kbps and a one-time allowable burst size of 60 bytes for the policy map named policy1:

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50 60
```

In the following example, 10 percent of the available bandwidth is reserved for the class named voice on interfaces to which the policy map named policy1 has been attached:

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority percent 10
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map. |
| **ip rtp priority** | Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports. |
| **ip rtp reserve** | Reserves a special queue for a set of RTP packet flows belonging to a range of UDP destination ports. |
| **max-reserved-bandwidth** | Changes the percent of interface bandwidth allocated for CBWFQ, LLQ, and IP RTP Priority. |

| Command | Description |
|---|---|
| **show interfaces fair-queue** | Displays information and statistics about WFQ for a VIP-based interface. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |

# priority (10000 series)

To give priority to a traffic class in a policy map, use the **priority** command in QoS policy-map class configuration mode on Cisco 10000 Series Routers. To remove preferential treatment of a class, use the **no** form of this command.

**priority**

**no priority**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No default behavior or values.

## Command Modes

QoS policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.0(17)SL | This command was introduced. |
| 12.0(20)ST | This command was enhanced to include a percent-based bandwidth rate. |
| 12.0(25)S | This command was modified to provide strict priority queueing on the ESR-PRE1. |
| 12.2(16)BX | This command was implemented on the ESR-PRE2. |
| 12.3(7)XI1 | This command was modified to provide strict priority queueing on the ESR-PRE2. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB. |

## Usage Guidelines

In Cisco IOS Release 12.0(25)S and Release 12.3(7)XI1, and later releases, the priority command provides strict priority queueing. To specify a bandwidth rate in kilobits per second (kbps) or as a percentage of the link bandwidth, use the police or police percent command.

Strict priority queueing guarantees low latency for any packet that enters a priority queue, regardless of the current congestion level on the link.

**Note** In releases prior to Cisco IOS Release 12.0(25)S and Release 12.3(7)XI, use the priority command to specify a bandwidth rate.

The priority command allows you to assign priority to a traffic class in a policy map. Because the router gives preferential treatment to a priority class, priority queueing allows delay-sensitive data such as voice to be dequeued and sent before packets in other queues.

The bandwidth parameter you specify in the police command guarantees bandwidth to the priority class and restricts the flow of packets from the priority class.

The following interfaces support priority queueing using the priority command:

- Physical
- Multilink PPP and multilink Frame Relay
- ATM shaped (peak cell rate is specified) unspecified bit rate (UBR) Permanent Virtual Circuits (PVCs) and point-to-point subinterfaces
- ATM constant bit rate (CBR) PVCs and point-to-point subinterfaces
- ATM variable bit rate (VBR) PVCs and point-to-point subinterfaces
- Label-controlled ATM (LC-ATM) subinterfaces
- Frame Relay PVCs, point-to-point subinterfaces, and map classes
- Ethernet VLANs

The following interfaces do not support priority queueing using the priority command:

- ATM unshaped (no peak cell rate specified) UBR PVCs and point-to-point subinterfaces
- IP tunnel
- Virtual access

**Cisco 10000 Series Router**

The Cisco 10000 series router supports the priority command only on outbound interfaces. It does not support the priority command on inbound interfaces.

**Restrictions and Limitations for Priority Queueing**

- Each policy map can have only one priority class.
- You cannot configure the random-detect or bandwidth commands with a priority service.

## Examples

The following example assigns priority to class-default in policy map policy1:

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# priority
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth (policy-map class)** | Specifies the bandwidth allocated for a class belonging to a policy map. |

| Command | Description |
|---|---|
| **police** | Controls the maximum rate of traffic sent or received on an interface. |
| **police** (percent) | Configures traffic policing on the basis of a percentage of bandwidth available on an interface. |
| **random detect** (perVC) | Enables per-VC WRED or per-VC VIP-distributed WRED. |

# priority (SIP400)

To configure the strict scheduling priority for a class map, use the **priority** command in policy-map class configuration mode. To remove a previously specified priority level for a class, use the **no** form of this command with no arguments.

**priority** [**level** {**1**| **2**}] [*kbps* [ *burst* ]| **percent** *percentage* [ *burst* ]]

**no priority**

## Syntax Description

| | |
|---|---|
| **level** {**1** \| **2** | (Optional) Defines multiple levels of a strict priority service model (1 is high and 2 is lower). When you enable a traffic class with a specific level of priority service, the implication is a single priority queue associated with all traffic enabled with the specified level of priority service. Default: 1. |
| *kbps* | (Optional) Guaranteed allowed bandwidth, in kbps, for the priority traffic. The amount of guaranteed bandwidth varies according to the interface and platform in use. Beyond the guaranteed bandwidth, the priority traffic will be dropped in the event of congestion to ensure that the nonpriority traffic is not starved. Range: 1 to 2480000. |
| *burst* | (Optional) Specifies the burst size in bytes. The burst size configures the network to accommodate temporary bursts of traffic. The default burst value is used when the *burst* argument is not specified. Range: 18 to 2000000. Default: 200 milliseconds of traffic at the configured bandwidth rate. |
| **percent** *percentage* | (Optional) Specifies the percentage of the total available bandwidth to be set aside for the priority class. Range 1 to 100. |

## Command Default

All traffic uses the lower priority queue.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |

## Usage Guidelines

You can enter the **priority** command tocreate two levels of priority queues within a single policy map. The packets from the level 2 priority queue are scheduled to transmit only when the level 1 priority queue is empty.

The priority bandwidth and percentage have the following restrictions:

- Supported in the output direction only.
- Not supported on ATM shared port adapters (SPAs).

The priority level has the following restrictions:

- Only two priority levels are supported: priority or priority level 1 and priority level 2.
- Priority is supported in the output direction only.
- Priority is not supported on ATM SPAs.

You can enter the **showpolicy-mapinterface** command to display the strict level in the priority feature and the counts per level.

The **bandwidth** and **prioritylevel** commands cannot be used in the same class within the same policy map. These commands can be used in the same policy map, however.

The **shape** and **prioritylevel** commands cannot be used in the same class within the same policy map. These commands can be used in the same policy map, however,

Within a policy map, you can give one or more classes priority status. The router associates a single priority queue with all of the traffic enabled with the same priority level and empties the high level priority queues before servicing the next level priority queues and nonpriority queues.

You cannot specify the same priority level for two different classes in the same policy map.

You cannot specify the **priority** command and the **prioritylevel** command for two different classes in the same policy map. For example, you cannot specify the **priority***kbps* or **prioritypercent***percentage* command and the **prioritylevel** command for different classes.

When the **prioritylevel** command is configured with a specific level of priority service, the **queue-limit** and **random-detect** commands can be used if only a single class at that level of priority is configured.

You cannot configure the default queue as a priority queue at any priority level.

## Examples

The following example shows how to configure multilevel priority queues. In the example, the traffic class named Customer1 is given high priority (level 1) and the class named Customer2 is given level 2 priority. To prevent Customer2 traffic from becoming obstructed, Customer1 traffic is policed at 30 percent of the available bandwidth.

```
Router# config terminal
Router(config)# policy-map Business
Router(config-pmap)# class Customer1
Router(config-pmap-c)# priority level 1
Router(config-pmap-c)# police 30
Router(config-pmap-c)# exit
Router(config-pmap)# class Customer2
Router(config-pmap-c)# priority level 2
```

The following example configures a priority queue with a guaranteed bandwidth of 50 kbps and a one-time allowable burst size of 60 bytes for the policy map called policy1:

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50 60
```

In the following example, 10 percent of the available bandwidth is reserved for the class called voice on interfaces to which the policy map called policy1 has been attached:

```
Router(config)# policy-map policy1
Router(config-pmap)# class voice
Router(config-pmap-c)# priority percent 10
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map. |
| **priority** | Assigns priority to a class of traffic. |
| **queue-limit** | Specifies the maximum number of packets a queue can hold for a class policy configured in a policy map. |
| **random-detect** | Enables Weighted Random Early Detection (WRED) on an interface. |
| **shape** | Specifies a maximum data rate for a class of outbound traffic. |
| **show policy-map interface** | Displays the statistics and configurations of the policies attached to an interface. |

# priority-group

**Note** Effective with Cisco IOS Release 15.1(3)T, the **priority-group**command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

To assign the specified priority list to an interface, use the **priority-group** command in interface configuration mode. To remove the specified priority groupassignment, use the **no** form of this command.

**priority-group** *list-number*

**no priority-group** *list-number*

## Syntax Description

| | |
|---|---|
| *list-number* | Priority list number assigned to the interface. Any number from 1 to 16. |

## Command Default

Disabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(3)T | This command was modified. This command was hidden. |

## Usage Guidelines

Only one list can be assigned per interface. Priority output queueing provides a mechanism to prioritize packets sent on an interface.

Use the**showqueueing**and**showinterfaces** commands to display the current status of the output queues.

## Examples

The following example causes packets for transmission on serial interface 0 to be classified by priority list 1:

```
interface serial 0
 priority-group 1
```

The following example shows how to establish queueing priorities based on the address of the serial link on a serial tunnel (STUN) connection. Note that you must use the **priority-group** interface configuration command to assign a priority group to an output interface.

```
stun peer-name 172.16.0.0
stun protocol-group 1 sdlc
!
interface serial 0
! Disable the ip address for interface serial 0:
no ip address
! Enable the interface for STUN:
encapsulation stun
!
stun group 2
stun route address 10 tcp 172.16.0.1 local-ack priority
!
! Assign priority group 1 to the input side of interface serial 0:
priority-group 1
! Assign a low priority to priority list 1 on serial link identified
! by group 2 and address A7:
priority-list 1 stun low address 2 A7
```

## Related Commands

| Command | Description |
|---|---|
| **locaddr-priority-list** | Maps LUs to queueing priorities as one of the steps to establishing queueing priorities based on LU addresses. |
| **priority-list default** | Assigns a priority queue for those packets that do not match any other rule in the priority list. |
| **priority-list interface** | Establishes queueing priorities on packets entering from a given interface. |
| **priority-list protocol** | Establishes queueing priorities based on the protocol type. |
| **priority-list protocol ip tcp** | Establishes BSTUN or STUN queueing priorities based on the TCP port. |
| **priority-list protocol stun address** | Establishes STUN queueing priorities based on the address of the serial link. |
| **priority-list queue-limit** | Specifies the maximum number of packets that can be waiting in each of the priority queues. |
| **show interfaces** | Displays statistics for all interfaces configured on the router or access server. |

| Command | Description |
|---|---|
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# priority level

To configure multiple priority queues, use the **priority level** command in policy-map class configuration mode. To remove a previously specified priority level for a class, use the **no** form of this command.

**priority level** *level*

**no priority level** *level*

## Syntax Description

| | |
|---|---|
| *level* | Defines multiple levels of a strict priority service model. When you enable a traffic class with a specific level of priority service, the implication is a single priority queue associated with all traffic that is enabled with the specified level of priority service.<br>Valid values are from 1 (high priority) to 4 (low priority). Default is 1. For Cisco ASR 1000 Series Routers and the Cisco ASR 903 Series Routers, valid values are from 1 (high priority) to 2 (low priority). Default is 1. |

## Command Default

The priority level has a default level of 1.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.2(31)SB2 | This command was introduced to provide multiple levels of strict priority queuing and implemented on the Cisco 10000 Series Router for the PRE3. |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 Series Routers. |
| Cisco IOS XE Release 3.7S | This command was implemented on Cisco ASR 903 Series Routers. |

## Usage Guidelines

The **bandwidth** and **priority level**commands cannot be used in the same class, within the same policy map. These commands can be used in the same policy map, however.

The **shape** and **priority level** commands cannot be used in the same class, within the same policy map. These commands can be used in the same policy map, however.

Within a policy map, you can give one or more classes priority status. The router associates a single priority queue with all of the traffic enabled with the same priority level and services the high-level priority queues until empty before servicing the next-level priority queues and non-priority queues.

You cannot specify the same priority level for two different classes in the same policy map.

You cannot specify the **priority** command and the **priority level** command for two different classes in the same policy map. For example, you cannot specify the **priority bandwidth** *kbps* or **priority percent** *percentage* command and the **priority level** command for different classes.

When the **priority level** command is configured with a specific level of priority service, the **queue-limit** and **random-detect** commands can be used only if a single class at that level of priority is configured.

You cannot configure the default queue as a priority queue at any priority level.

**Cisco 10000 Series Router, Cisco ASR 1000 Series Router, and Cisco ASR 903 Series Router**

The Cisco 10000 series router, the Cisco ASR 1000 Series Router, and the Cisco ASR 903 Series Router support two levels of priority service: level 1 (high) and level 2 (low). If you do not specify a priority level, the routers use the default level of 1. Level 1 specifies that low-latency behavior must be given to the traffic class. The high-level queues are serviced until empty before the next-level queues and non-priority queues.

## Examples

The following example shows how to configure multi level priority queues. In the example, the traffic class named Customer1 is given high priority (level 1), and the class named Customer2 is given level 2 priority. To prevent Customer2 traffic from becoming starved of bandwidth, Customer1 traffic is policed at 30 percent of the available bandwidth.

```
Router> enable
Router# config terminal
Router(config)# policy-map Business
Router(config-pmap)# class Customer1
Router(config-pmap-c)# priority level 1
Router(config-pmap-c)# police 30
Router(config-pmap-c)# exit
Router(config-pmap)# class Customer2
Router(config-pmap-c)# priority level 2
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map. |
| **priority** | Assigns priority to a class of traffic. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. Displays statistical information for all priority levels configured. |

# priority-list default

To assign a priority queue for those packets that do not match any other rule in the priority list, use the **priority-listdefault** command in global configuration mode. To return to the default or assign **normal** as the default, use the **no** form of this command.

**priority-list** *list-number* **default** {**high**| **medium**| **normal**| **low**}

**no priority-list** *list-number* **default**

## Syntax Description

| | |
|---|---|
| *list-number* | Any number from 1 to 16 that identifies the priority list. |
| **high** \| **medium** \| **normal** \| **low** | Priority queue level. The **normal** queue is used if you use the **no** form of this command. |

## Command Default

This command is not enabled by default.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

When you use multiple rules, remember that the system reads the priority settings in order of appearance. When classifying a packet, the system searches the list of rules specified by **priority-list** commands for a matching protocol or interface type. When a match is found, the system assigns the packet to the appropriate queue. The system searches the list in the order specified, and the first matching rule terminates the search.

## Examples

The following example sets the priority queue for those packets that do not match any other rule in the priority list to a low priority:

```
priority-list 1 default low
```

## Related Commands

| Command | Description |
|---|---|
| **priority-group** | Assigns the specified priority list to an interface. |
| **priority-list interface** | Establishes queueing priorities on packets entering from a given interface. |
| **priority-list protocol** | Establishes queueing priorities based on the protocol type. |
| **priority-list queue-limit** | Specifies the maximum number of packets that can be waiting in each of the priority queues. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# priority-list interface

To establish queueing priorities on packets entering from a given interface, use the **priority-listinterface** command in global configuration mode. To remove an entry from the list, use the **no**form of this command with the appropriate arguments.

**priority-list** *list-number* **interface** *interface-type interface-number* {**high**| **medium**| **normal**| **low**}

**no priority-list** *list-number* **interface** *interface-type interface-number* {**high**| **medium**| **normal**| **low**}

## Syntax Description

| | |
|---|---|
| *list-number* | Any number from 1 to 16 that identifies the priority list. |
| *interface-type* | The type of the interface. |
| *interface-number* | The number of the interface. |
| **high** \| **medium** \| **normal** \| **low** | Priority queue level. |

## Command Default

No queueing priorities are established by default.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

When you use multiple rules, remember that the system reads the priority settings in order of appearance. When classifying a packet, the system searches the list of rules specified by **priority-list** commands for a matching protocol or interface type. When a match is found, the system assigns the packet to the appropriate queue. The system searches the list in the order specified, and the first matching rule terminates the search.

## Examples

The following example assigns a list entering on serial interface 0 to a medium priority queue level:

```
priority-list 3 interface serial 0 medium
```

**Note** This command defines a rule that determines how packets are attached to an interface. Once the rule is defined, the packet is actually attached to the interface using the **priority-group** command.

## Related Commands

| Command | Description |
|---|---|
| **priority-group** | Assigns the specified priority list to an interface. |
| **priority-list default** | Assigns a priority queue for those packets that do not match any other rule in the priority list. |
| **priority-list protocol** | Establishes queueing priorities based on the protocol type. |
| **priority-list queue-limit** | Specifies the maximum number of packets that can be waiting in each of the priority queues. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# priority-list protocol

To establish queueing priorities based upon the protocol type, use the **priority-listprotocol** command in global configuration mode. To remove a priority list entry assigned by protocol type, use the **no** form of this command with the appropriate arguments.

**priority-list** *list-number* **protocol** *protocol-name* {**high| medium| normal| low**} *queue-keyword keyword-value*

**no priority-list** *list-number* **protocol** *protocol-name* {**high| medium| normal| low**} *queue-keyword keyword-value*

## Syntax Description

| | |
|---|---|
| *list-number* | Any number from 1 to 16 that identifies the priority list. |
| *protocol-name* | Protocol type: **aarp**, **appletalk**, **arp**, **bridge** (transparent), **clns**, **clns_es**, **clns_is**, **compressedtcp**, **cmns**, **decnet**, **decnet_node**, **decnet_router-l1**, **decnet_router-l2**, **dlsw**, **ip**, **ipx**, **pad**, **rsrb**, **stun**, and **x25**. |
| **high** \| **medium** \| **normal** \| **low** | Priority queue level. |
| *queue-keyword keyword-value* | Possible keywords are **fragments**, **gt**, **list**, **lt**, **tcp**, and **udp**. For more information about keywords and values, see Table 20 in the "Usage Guidelines" section. |

## Command Default

No queueing priorities are established.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2(13)T | This command was modified. The **apollo**, **vines**, and **xns** keywords were removed from the list of protocol types. These protocols were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems (XNS) were removed in Release 12.2(13)T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

| Release | Modification |
|---|---|
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

When you use multiple rules for a single protocol, remember that the system reads the priority settings in order of appearance. When classifying a packet, the system searches the list of rules specified by **priority-list** commands for a matching protocol type. When a match is found, the system assigns the packet to the appropriate queue. The system searches the list in the order specified, and the first matching rule terminates the search.

The**decnet_router-l1** keyword refers to the multicast address for all level 1 routers, which are intra-area routers, and the **decnet_router-l2** keyword refers to all level 2 routers, which are interarea routers.

The **dlsw**,**rsrb**, and **stun**keywords refer only to direct encapsulation.

Use the tables below to configure the queueing priorities for your system.

***Table 30: Protocol Priority Queue Keywords and Values***

| Option | Description |
|---|---|
| **fragments** | Assigns the priority level defined to fragmented IP packets (for use with IP only). More specifically, this command matches IP packets whose fragment offset field is nonzero. The initial fragment of a fragmented IP packet has a fragment offset of zero, so such packets are not matched by this command.<br>**Note** Packets with a nonzero fragment offset do not contain TCP or User Datagram Protocol (UDP) headers, so other instances of this command that use the **tcp** or **udp** keyword will always fail to match such packets. |
| **gt** *byte-count* | Specifies a greater-than count. The priority level assigned goes into effect when a packet size exceeds the value entered for the *byte-count*argument.<br>**Note** The size of the packet must also include additional bytes because of MAC encapsulation on the outgoing interface. |
| **list** *list-number* | Assigns traffic priorities according to a specified list when used with AppleTalk, bridging, IP, IPX, VINES, or XNS. The *list-number*argument is the access list number as specified by the**access-list** global configuration command for the specified *protocol-name* . For example, if the protocol is AppleTalk, *list-number* should be a valid AppleTalk access list number. |

| Option | Description |
|---|---|
| **lt** *byte-count* | Specifies a less-than count. The priority level assigned goes into effect when a packet size is less than the value entered for the *byte-count* argument.<br>**Note** The size of the packet must also include additional bytes because of MAC encapsulation on the outgoing interface. |
| **tcp** *port* | Assigns the priority level defined to TCP segments originating from or destined to a specified port (for use with IP only). Table 21 lists common TCP services and their port numbers. |
| **udp** *port* | Assigns the priority level defined to UDP packets originating from or destined to a specified port (for use with IP only). Table 22 lists common UDP services and their port numbers. |

***Table 31: Common TCP Services and Their Port Numbers***

| Service | Port |
|---|---|
| FTP data | 20 |
| FTP | 21 |
| Simple Mail Transfer Protocol (SMTP) | 25 |
| Telnet | 23 |

**Note** To display a complete list of TCP services and their port numbers, enter a help string, such as the following example: Router(config)#**prioritylist4protocolipmediumtcp?**

***Table 32: Common UDP Services and Their Port Numbers***

| Service | Port |
|---|---|
| Domain Name System (DNS) | 53 |
| Network File System (NFS) | 2049 |
| remote-procedure call (RPC) | 111 |
| SNMP | 161 |

| Service | Port |
|---|---|
| TFTP | 69 |

**Note** To display a complete list of UDP services and their port numbers, enter a help string, such as the following example: Router(config)#**prioritylist4protocolipmediumudp?**

**Note** The tables above include some of the more common TCP and UDP port numbers. However, you can specify any port number to be prioritized; you are not limited to those listed. For some protocols, such as TFTP and FTP, only the initial request uses port 69. Subsequent packets use a randomly chosen port number. For these types of protocols, the use of port numbers fails to be an effective method to manage queued traffic.

## Examples

The following example shows how to assign 1 as the arbitrary priority list number, specify DECnet as the protocol type, and assign a high-priority level to the DECnet packets sent on this interface:

```
priority-list 1 protocol decnet high
```

The following example shows how to assign a medium-priority level to every DECnet packet with a size greater than 200 bytes:

```
priority-list 2 protocol decnet medium gt 200
```

The following example shows how to assign a medium-priority level to every DECnet packet with a size less than 200 bytes:

```
priority-list 4 protocol decnet medium lt 200
```

The following example shows how to assign a high-priority level to traffic that matches IP access list 10:

```
priority-list 1 protocol ip high list 10
```

The following example shows how to assign a medium-priority level to Telnet packets:

```
priority-list 4 protocol ip medium tcp 23
```

The following example shows how to assign a medium-priority level to UDP DNS packets:

```
priority-list 4 protocol ip medium udp 53
```

The following example shows how to assign a high-priority level to traffic that matches Ethernet type code access list 201:

```
priority-list 1 protocol bridge high list 201
```

The following example shows how to assign a high-priority level to data-link switching plus (DLSw+) traffic with TCP encapsulation:

```
priority-list 1 protocol ip high tcp 2065
```

The following example shows how to assign a high-priority level to DLSw+ traffic with direct encapsulation:

```
priority-list 1 protocol dlsw high
```

**Note** This command define a rule that determines how packets are attached to an interface. Once the rule is defined, the packet is actually attached to the interface using the **priority-group**command.

## Related Commands

| Command | Description |
|---|---|
| **priority-group** | Assigns the specified priority list to an interface. |
| **priority-list default** | Assigns a priority queue for those packets that do not match any other rule in the priority list. |
| **priority-list interface** | Establishes queueing priorities on packets entering from a given interface. |
| **priority-list queue-limit** | Specifies the maximum number of packets that can be waiting in each of the priority queues. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# priority-list queue-limit

To specify the maximum number of packets that can be waiting in each of the priority queues, use the **priority-listqueue-limit** command in global configuration mode. To select the normal queue, use the **no**form of thiscommand.

**priority-list** *list-number* **queue-limit** *high-limit medium-limit normal-limit low-limit*

**no priority-list** *list-number* **queue-limit**

## Syntax Description

| | |
|---|---|
| *list-number* | Any number from 1 to 16 that identifies the priority list. |
| *high-limit medium-limit normal-limit low-limit* | Priority queue maximum length. A value of 0 for any of the four arguments means that the queue can be of unlimited size for that particular queue. For default values for these arguments, see the table below. |

## Command Default

None. See the table below in the “Usage Guidelines” section of this command for a list of the default queue limit arguments.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

If a priority queue overflows, excess packets are discarded and messages can be sent, if appropriate, for the protocol.

The default queue limit values are listed in the table below.

*Table 33: Default Priority Queue Packet Limits*

| Priority Queue Argument | Packet Limits |
|---|---|
| *high-limit* | 20 |
| *medium-limit* | 40 |
| *normal-limit* | 60 |
| *low-limit* | 80 |

**Note** If priority queueing is enabled and there is an active Integrated Services Digital Network (ISDN) call in the queue, changing the configuration of the **priority-listqueue-limit**command drops the call from the queue. For more information about priority queueing, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide.*

## Examples

The following example shows how to set the maximum packets in the priority queue to 10:

```
Router(config)# priority-list 2 queue-limit 10 40 60 80
```

## Related Commands

| Command | Description |
|---|---|
| **priority-group** | Assigns the specified priority list to an interface. |
| **priority-list default** | Assigns a priority queue for those packets that do not match any other rule in the priority list. |
| **priority-list interface** | Establishes queueing priorities on packets entering from a given interface. |
| **priority-list protocol** | Establishes queueing priorities based on the protocol type. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# priority-queue cos-map

To map CoS values to the receive and transmit strict-priority queues in interface configuration command mode, use the **priority-queuecos-map** command. To return to the default mapping, use the **no** form of this command.

**priority-queue cos-map** *queue-id cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [ *cos8* ]]]]]]]

**no priority-queue cos-map**

## Syntax Description

| | |
|---|---|
| *queue-id* | Queue number; the valid value is **1**. |
| *cos1* | CoS value; valid values are from 0 to 7. |
| *. . . cos8* | (Optional) CoS values; valid values are from 0 to 7. |

## Command Default

The default mapping is queue 1 is mapped to CoS 5 for the following receive and transmit strict-priority queues:

- 1p1q4t receive queues
- 1p1q0t receive queues
- 1p1q8t receive queues
- 1p2q2t transmit queues
- 1p3q8t transmit queues
- 1p7q8t transmit queues
- 1p3q1t transmit queues
- 1p2q1t transmit queues

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(50)SY | Support for this command was introduced. |

## Usage Guidelines

**Note** In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

When mapping CoS values to the strict-priority queues, note the following information:

- The queue number is always **1**.
- You can enter up to 8 CoS values to map to the queue.

## Examples

This example shows how to map CoS value 7 to the strict-priority queues on Gigabit Ethernet port 1/1:

```
Router(config-if)# priority-queue cos-map 1 7
Router(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| show queueing interfaces | Displays queueing information. |

# priority-queue queue-limit

To set the priority-queue size on an interface, use the **priority-queuequeue-limit** command in interface configuration mode. To return to the default priority-queue size, use the **no** form of this command.

**priority-queue queue-limit** *percent*

**no priority-queue queue-limit** *percent*

## Syntax Description

| | |
|---|---|
| *percent* | Priority-queue size in percent ; valid values are from 1 to 100. |

## Command Default

When global quality of service (QoS) is enabled the priority-queue size is 15. When global QoS is disabled the priority-queue size is 0.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXF2 | This command was introduced. |
| 12.2(50)SY | Support for this command was introduced. |

## Usage Guidelines

**Note** In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

This command is supported on the following modules:

- WS-X6501-10GE--1p2q1t[9]
- WS-X6148A-GE--1p3q8t[10]
- WS-X6148-45--1p3q8t
- WS-X6148-FE-SFP--1p3q8t
- WS-X6748-SFP--1p3q8t

9 1p2q1t--One strict-priority queue, two standard queues with one WRED drop threshold and one non-configurable (100%) tail-drop threshold per queue.

10 1p3q8t--One strict-priority queue, three standard queues with eight WRED drop thresholds per queue.

- WS-X6724-SFP--1p7q8t [11]
- WS-X6704-10GE--1p7q4t[12]
- WS-SUP32-10GB-3E--1p7q4t
- WS-SUP32-GB-3E--1p3q8t
- WS-X6708-10GE--1p7q4t

## Examples

The following example shows how to set the priority-queue size on an interface:

```
priority-queue queue-limit 15
```

## Related Commands

| Command | Description |
|---|---|
| **show queueing interface** | Displays queueing information. |

11 1p7q8t--One strict-priority queue, seven standard queues with eight WRED drop thresholds per queue.
12 1p7q4t--One strict-priority queue, seven standard queues with four WRED drop thresholds per queue.

# pvc-bundle

To add a virtual circuit (VC) to a bundle as a member of the bundle and enter bundle-vc configuration mode in order to configure that VC bundle member, use the **pvc-bundle** command in bundle configuration mode. To remove the VC from the bundle, use the **no**form of this command.

**pvc-bundle** *pvc-name* [ *vpi/* ] [ *vci* ]

**no pvc-bundle** *pvc-name* [ *vpi/* ] [ *vci* ]

## Syntax Description

| | |
|---|---|
| *pvc-name* | The name of the permanent virtual circuit (PVC) bundle. |
| *vpi* / | (Optional) ATM network virtual path identifier (VPI) for this PVC. The absence of the / and a *vpi* value defaults the *vpi* value to 0.<br>On the Cisco 7200 and 7500 series routers, the value range is from 0 to 255; on the Cisco 4500 and 4700 routers, the value range is from 0 to 1 less than the quotient of 8192 divided by the value set by the **atmvc-per-vp** command.<br>The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0. |
| *vci* | (Optional) ATM network virtual channel identifier (VCI) for this PVC. The value range is from 0 to 1 less than the maximum value set for this interface by the **atmvc-per-vp** command. Typically, lower values 0 to 31 are reserved for specific traffic (F4 Operation, Administration, and Maintenance (OAM), switched virtual circuit (SVC) signaling Integrated Local Management Interface (ILMI), and so on) and should not be used.<br>The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only.<br>The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0. |

## Command Default

None

## Command Modes

Bundle configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.0(26)S | This command was implemented on the Cisco 10000 series router. |
| 12.2(16)BX | This command was implemented on the ESR-PRE2. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Each bundle can contain multiple VCs having different quality of service (QoS) attributes. This command associates a VC with a bundle, making it a member of that bundle. Before you can add a VC to a bundle, the bundle must exist. Use the **bundle** command to create a bundle. You can also use this command to configure a VC that already belongs to a bundle. You enter the command in the same way, giving the name of the VC bundle member.

The **pvc-bundle** command enters bundle-vc configuration mode, in which you can specify VC-specific and VC class attributes for the VC.

## Examples

The following example specifies an existing bundle called bundle1 and enters bundle configuration mode. Then it adds two VCs to the bundle. For each added VC, bundle-vc mode is entered and a VC class is attached to the VC to configure it.

```
bundle bundle1
 pvc-bundle bundle1-control 207
 class control-class
 pvc-bundle bundle1-premium 206
 class premium-class
```

The following example configures the PVC called bundle1-control, an existing member of the bundle called bundle1, to use class-based weighted fair queueing (CBWFQ). The example configuration attaches the policy map called policy1 to the PVC. Once the policy map is attached, the classes comprising policy1 determine the service policy for the PVC bundle1-control.

```
bundle bundle1
 pvc-bundle bundle1-control 207
 class control-class
 service-policy output policy1
```

## Related Commands

| Command | Description |
|---|---|
| **atm vc-per-vp** | Sets the maximum number of VCIs to support per VPI. |

| Command | Description |
|---|---|
| **bump** | Configures the bumping rules for a VC class that can be assigned to a VC bundle. |
| **class-bundle** | Configures a VC bundle with the bundle-level commands contained in the specified VC class. |
| **class-vc** | Assigns a VC class to an ATM PVC, SVC, or VC bundle member. |
| **precedence** | Configures precedence levels for a VC member of a bundle, or for a VC class that can be assigned to a VC bundle. |
| **protect** | Configures a VC class with protected group or protected VC status for application to a VC bundle member. |
| **pvc** | Creates or assigns a name to an ATM PVC, specifies the encapsulation type on an ATM PVC, and enters interface-ATM-VC configuration mode. |
| **ubr** | Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member. |
| **ubr+** | Configures UBR QoS and specifies the output peak cell rate and output minimum guaranteed cell rate for an ATM PVC, SVC, VC class, or VC bundle member. |
| **vbr-nrt** | Configures the VBR-NRT QoS and specifies output peak cell rate, output sustainable cell rate, and output maximum burst cell size for an ATM PVC, SVC, VC class, or VC bundle member. |

# Q through R


- qos police order parent-first, page 917
- qos pre-classify, page 918
- qos shape-timer, page 920
- queue-depth, page 922
- queue-limit, page 924
- queue-limit atm clp, page 929
- queue-list default, page 931
- queue-list interface, page 933
- queue-list lowest-custom, page 935
- queue-list protocol, page 937
- queue-list queue byte-count, page 940
- queue-list queue limit, page 942
- random-detect, page 944
- random-detect (per VC), page 949
- random-detect aggregate, page 953
- random-detect atm-clp-based, page 956
- random-detect clp, page 958
- random-detect cos-based, page 960
- random-detect discard-class, page 962
- random-detect discard-class-based, page 966
- random-detect dscp, page 967
- random-detect dscp (aggregate), page 975
- random-detect ecn, page 980
- random-detect exponential-weighting-constant, page 981

- random-detect flow, page 985
- random-detect flow average-depth-factor, page 987
- random-detect flow count, page 989
- random-detect prec-based, page 991
- random-detect precedence, page 993
- random-detect precedence (aggregate), page 998
- random-detect-group, page 1002
- rate-limit, page 1005
- rcv-queue bandwidth, page 1010
- rcv-queue cos-map, page 1012
- rcv-queue queue-limit, page 1014
- rcv-queue random-detect, page 1016
- rcv-queue threshold, page 1018
- recoverable-loss, page 1021
- redirect interface, page 1023
- refresh max-period, page 1025
- refresh max-time, page 1027
- refresh rtp, page 1029
- rtp, page 1031

# qos police order parent-first

To change the Quality of Service (QoS) policing action from child first, then parent (the default) to parent first, then child, use the **qospoliceorderparent-first** command in global configuration mode. To disable the parent-first order and restore the default behavior, use the **no** form of this command.

**qos police order parent-first**

**no qos police order parent-first**

## Syntax Description

This command has no arguments or keywords.

## Command Default

If the **qospoliceorderparent-first**command is not entered, the child policing action is done first, followed by the parent policing action.

## Command Modes

Global configuration (#)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)S | This command was introduced. |

## Usage Guidelines

Prior to Cisco IOS Release 15.1(1)S, in a hierarchical policing policy map (a parent policy with policing configured under a class that has a child policy also with policing configured), the parent policing action was done first, followed by the child policing action.

Beginning in Cisco IOS Release 15.1(1)S, the order is reversed. By default, the child policing action is done first, followed by the parent policing action. This change applies only to software dataplane policer implementations (Cisco 7200, Cisco 7301, and Cisco 7600 FlexWAN and SIP200 line cards).

This new behavior improves the results for transmit-and-drop actions because the child policing action occurs first. However, if the parent and child policers are performing conflicting mark-and-transmit actions, the parent mark takes effect rather than the child because the parent action happens last.

Use of the **qospoliceorderparent-first** command is necessary only if you need to revert to the police order that was in effect prior to Release 15.1(1)S.

## Examples

The following example shows how to change the police order from child first (default) to parent first, then child:

```
Router# qos police order parent-first
```

# qos pre-classify

To enable quality of service (QoS) preclassification, use the **qospre-classify** command in interface configuration mode. To disable the QoS preclassification feature, use the **no** form of this command.

**qos pre-classify**

**no qos pre-classify**

## Syntax Description

This command has no arguments or keywords.

## Command Default

QoS preclassification is disabled.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)XE3 | This command was introduced. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.2(2)T | This command was implemented on the Cisco 2600 and Cisco 3600 series routers. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers. |

## Usage Guidelines

This command is restricted to tunnel interfaces, virtual templates, and crypto maps. The **qospre-classify** command is unavailable on all other interface types.

You can enable the **qospre-classify** command for IP packets only.

**Note** QoS preclassification is not supported for all fragmented packets. If a packet is fragmented, each fragment might receive different preclassifications.

## Examples

The following example enables the QoS for Virtual Private Networks (VPNs) feature on tunnel interfaces and virtual templates:

```
Router(config-if)# qos pre-classify
```

## Related Commands

| Command | Description |
|---|---|
| **show interfaces** | Displays statistics for the interfaces configured on a router or access server. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |

# qos shape-timer

To specify the Hierarchical Queuing Framework (HQF) shaper-timer interval, use the **qos shape-timer** command in global configuration mode. To remove the shaper-timer interval setting, and restore the default value, use the **no** form of this command.

**qos shape-timer** {**1ms**| **4ms**}

**no qos shape-timer** {**1ms**| **4ms**}

## Syntax Description

| | |
|---|---|
| **1ms** | Sets the HQF shaper timer to 1 millisecond (ms). |
| **4ms** | Sets the HQF shaper timer to the default value of 4 ms. |

## Command Default

The shaper-timer interval is 4-milliseconds.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 15.1(4)M5 | This command was introduced. |

## Usage Guidelines

By default, the shaper timer uses an interval of 4 ms; however, on high-speed interfaces this setting can lead to a burst at the line rate every 4 ms until the token bucket is exhausted. If there is a low-end device immediately downstream, then packets can be dropped during every burst. To eliminate the unwanted burst behavior, you can reduce the token bucket replenish time from 4 ms to 1 ms using the **qos shape-timer** command.

To configure the shape-timer interval, first you use **qos shape-timer** command to set the shaper-timer interval, then you create a QoS service policy that specifies the average shape rate, and finally you apply that policy to an interface. Once the policy has been applied to an interface, the interval that the shaper uses to replenish the token bucket is decided by the parameter you specified using the **qos shape-timer** command.

**Note** The **qos shape-timer** command is available on all Integrated Services Routers (ISRs) that do not have a hardware assisted timer.

## Examples

The following example shows how to create and attach a service policy to an interface and set the shaper-timer interval to 1 ms:

```
Router(config)# policy-map myservicepolicy
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 256000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface gigabitEthernet 0/0
Router(config-if)# service-policy output myservicepolicy
Router(config-if)# exit
Router(config)# qos shape-timer 1ms
```

## Related Commands

| Command | Description |
|---|---|
| **class** | Specifies the name of the class whose policy you want to create or change, or specifies the default class. |
| **policy-map** | Specifies the name of the service policy to configure. |
| **service-policy** | Specifies the name of the service policy to be attached to the interface. |
| **shape** | Specifies average or peak rate traffic shaping. |

# queue-depth

To configure the number of incoming packets that the Open Shortest Path First (OSPF) process can keep in its queue, use the **queue-depth** command in router configuration mode. To set the queue depth to its default value, use the **no** form of the command.

**queue-depth** {**hello**| **update**} {*queue-size*| **unlimited**}

**no queue-depth** {**hello**| **update**}

## Syntax Description

| | |
|---|---|
| **hello** | Specifies the queue depth of the OSPF hello process. |
| **update** | Specifies the queue depth of the OSPF router process queue. |
| *queue-size* | Maximum number of packets in the queue. The range is 1 to 2147483647. |
| **unlimited** | Specifies an infinite queue depth. |

## Command Default

If you do not set a queue size, the OSPF hello process queue depth is unlimited and the OSPF router process (update) queue depth is 200 packets.

## Command Modes

Router configuration (config-router)

## Command History

| Release | Modification |
|---|---|
| 12.2(25)S | This command was introduced. |

## Usage Guidelines

All incoming OSPF packets are initially enqueued in the hello queue. OSPF hello packets are processed directly from this queue, while all other OSPF packet types are subsequently enqueued in the update queue.

If you configure a router with many neighbors and a large database, use the **queue-depth** command to adjust the size of the hello and router queues. Otherwise, packets might be dropped because of queue limits, and OSPF adjacencies may be lost.

## Examples

The following example shows how to configure the OSPF update queue to 1500 packets:

```
Router> enable
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Router(config)# router ospf 1
Router(config-router)# queue-depth update 1500
```

## Related Commands

| Command | Description |
|---|---|
| **queue-limit** | Specifies or modifies the queue limit (size) for a class in bytes, milliseconds (ms), or packets. |
| **queue-list queue limit** | Designates the queue length limit for a queue. |

# queue-limit

To specify or modify the queue limit (size) for a class in bytes, milliseconds (ms), microseconds (us) or packets, use the **queue-limit** command in QoS policy-map class configuration mode. To remove the queue limit from a class, use the **no** form of this command.

**queue-limit** *queue-limit-size* [**bytes**| **ms**| **us**| **packets**]

**no queue-limit**

### Cisco ASR 1000 Series Router

**queue-limit** *queue-limit-size* [**bytes**| **packets**]

**no queue-limit**

### Cisco 7600 Series Routers

**queue-limit** *queue-limit-size* **[packets]**

**no queue-limit**

## Syntax Description

| | |
|---|---|
| *queue-limit-size* | The maximum size of the queue. The maximum varies according to the optional unit of measure keyword specified (**bytes**, **ms**, **us**, or **packets**).<br>**Note** If an optional unit of measure is not specified, the default unit of measure depends on the platform.<br>**Note** For Cisco ASR 1000 Aggregation Services Routers, bytes is the preferred mode. |
| **bytes** | (Optional) Indicates that the unit of measure is bytes. Valid range for bytes is a number from 1 to 8192000.<br>**Note** The **bytes** keyword is not supported on Cisco 7600 series routers.<br>**Note** For Cisco ASR 1000 Series Routers, the valid range for bytes is a number from 1 to 64000000. |
| **ms** | (Optional) Indicates that the unit of measure is milliseconds. Valid range for milliseconds is a number from 1 to 3400.<br>**Note** The **ms** keyword is not supported on Cisco 7600 and Cisco ASR 1000 Series Routers. |
| **us** | (Optional) Indicates that the unit of measure is microseconds. Valid range for microseconds is a number from 1 to 512000. |

| | |
|---|---|
| **packets** | (Optional) Indicates that the unit of measure is packets. Valid range for packets is a number from 1 to 32768 but can also vary by platform and release as follows:<br>• For ESR-PRE1—The queue size limit for packets is a number from 32 to 16384; the number must be a power of 2. If the number that you specify is not a power of 2, the device converts the number to the nearest power of 2.<br>• For Cisco IOS Release 12.2(15)BX and later releases—The queue size limit for packets is a number from 32 to 16384. The number need not be a power of 2.<br>• For Cisco IOS Release 12.2(31)SB2 and later releases—The queue size limit for packets is a number from 16 to 32767.<br>• For Cisco IOS Release 12.3(7)XI and later releases—If the interface has less than 500 MB of memory, the queue size limit for packets is a number from 8 to 4096; the number must be a power of 2. If the interface has more than 500 MB of memory, the queue size limit for packets is a number from 128 to 64000 and must be a power of 2; if it is not, the device converts the number to the nearest power of 2.<br>• For Cisco IOS XE Release 2.1 and later releases—The queue size limit for packets is a number from 1 to 8192000. |

## Command Default

The default behavior of the **queue-limit** command for class queues with and without Weighted Random Early Detection (WRED) is as follows:

- Class queues with WRED—The device uses the default queue limit of two times the largest WRED maximum threshold value, rounded to the nearest power of 2.

**Note** For Cisco IOS Release 12.2(16)BX, the device does not round the value to the nearest power of 2.

- Priority queues and class queues without WRED—The device has buffers for up to 50 ms of 256-byte packets at line rate, but not fewer than 32 packets.

## Command Modes

QoS policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE. Support for VIP-enabled Cisco 7500 Series Routers was added. |
| 12.0(17)SL | This command was implemented on the Cisco 10000 Aggregation Series Router. |
| 12.1(5)T | This command was implemented on the VIP-enabled Cisco 7500 Series Routers. |
| 12.2(16)BX | This command was implemented on the ESR-PRE2. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.3(7)XI | This command was integrated into Cisco IOS Release 12.3(7)XI. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)T | The following argument and keyword combinations were added:<br>• *queue-limit-size* **bytes**<br>• *queue-limit-size* **ms**<br>• *queue-limit-size* **packets**<br>**Note** The **bytes** keyword is not supported on Cisco 7600 Series Routers, and the **ms** keyword is not supported on Cisco 7600 and Cisco ASR 1000 Series Routers. |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 Series Routers. |
| 15.0(1)S1 | This command was modified to improve the qlimit and min/max threshold calculation. |
| 15.0(1)M5 | This command was modified. Hierarchical Queueing Framework (HQF) capability was improved. |
| 15.2(2)T | This command was modified. The **us** keyword was added. The default unit of measure changed from packets to a platform-dependent unit. |
| 15.4(1)S | This command was implemented on the Cisco ASR 901 series routers. |

## Usage Guidelines

### Weighted Fair Queueing

Weighted fair queueing (WFQ) creates a queue for every class for which a class map is defined. Packets that satisfy the match criterion for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the fair queueing process. When the maximum packet threshold that you defined for the class is reached, enqueueing of any further packets to the class queue causes tail drop or, if WRED is configured for the class policy, packet drop to take effect.

**Changes in Cisco IOS Release 15.0(1)S1**

Prior to Cisco IOS Release 15.0(1)S1, if no queue limit was configured, the queue limit for the current class was based on the parent values for available buffers and current class allocated bandwidth. In the implicit WRED min/max scenario, thresholds were calculated from the available buffers.

Thresholds were calculated from the available aggregate queue limit for each class. The WRED min/max threshold values would not be adjusted if there was a user-defined queue-limit configuration. The min/max threshold would still be derived from the "visible_bw" value seen by this traffic class. The WRED functionality could fail because of this inconsistent qlimit and min/max threshold calculation.

Beginning in Cisco IOS Release 15.0(1)S1, the queue limit is always calculated from the parent queue limit and allocated bandwidth in the current class. When you use the **queue-limit** command to explicitly configure the values, these values are used as the definition of the queue limit.

To ensure optimum functionality, use the **queue-limit** command to configure the proper min/max threshold for each WRED class based on the queue-limit configuration.

**Changes in Cisco IOS Release 15.2(2)T**

Prior to Cisco IOS Release 15.2(2)T, if the optional unit of measure was not specified, the unit of measure used was packets. Beginning in Cisco IOS Release 15.2(2)T, if the optional unit of measure is not specified, the unit used depends on the platform.

**Overriding Queue Limits Set by the bandwidth Command**

Use the **bandwidth** command with the modular quality of service (QoS) CLI) (MQC) to specify the bandwidth for a particular class. When used with MQC, the **bandwidth** command has a default queue limit for the class. This queue limit can be modified using the **queue-limit** command, thereby overriding the default set by the **bandwidth** command.

**Note** Using the **queue-limit** command to modify the default queue limit is especially important for higher-speed interfaces, in order to meet the minimum bandwidth guarantees required by the interface.

Prior to the deployment of the Hierarchical Queueing Framework (HQF), the default maximum queue limit on a subinterface was 512 if no hold queue was configured on the main interface.

As part of HQF, this restriction was removed beginning in Cisco IOS Release 15.0(1)M5. Now the maximum queue limit can be set as high as the hold-queue size on the main interface.

If no hold queue is configured on the main interface, the aggregate queue limit can go up to 1000. If the hold-queue is explicitly configured on the main interface, then the aggregate queue limit can go up to the hold-queue value. There is no limit per subinterface.

The maximum configurable hold-queue value of 4096 was increased to 240,000 for users who want to configure higher aggregate queue-limit values. However, configuring high queue-limit and hold-queue values is not recommended.

## Examples

The following example configures a policy map called policy11. The policy11 policy map contains a class called acl203. The policy map for this class is configured so that the queue reserved for the class has a maximum queue size of 40 packets.

```
Device(config)# policy-map policy11
Device(config-pmap)# class acl203
Device(config-pmap-c)# bandwidth 2000
Device(config-pmap-c)# queue-limit 40 packets
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth** | Specifies the maximum aggregate bandwidth for H.323 traffic and verifies the available bandwidth of the destination gatekeeper. |
| **class (policy-map)** | Specifies the name of the class whose policy you want to create or change and the default class (commonly known as the class-default class) before you configure its policy. |
| **class class-default** | Specifies the default traffic class whose bandwidth is to be configured or modified. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **qos default queue-limit** | Configures the default queue limit for all QoS-based classes on a device in bytes, milliseconds (ms), microseconds (us), or packets. |

# queue-limit atm clp

To specify the maximum size (in cells, microseconds, or milliseconds) of a queue for a specific traffic class, use the **queue-limitatmclp** command in policy-map class configuration mode. To remove the queue limit atm cell loss priority (clp) value from a class, use the **no** form of this command.

**queue-limit atm clp** *queue-size* {**cells**| **ms**| **us**}

**no queue-limit atm clp**

## Syntax Description

| | |
|---|---|
| *queue-size* | Threshold value. The range is 1-262144. |
| **cells** \| **ms** \| **us** | Unit of measure for the queue size; ms = milliseconds; us = microseconds. |

## Command Default

No default behavior or values

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.0(30)S | This command was introduced. |

## Usage Guidelines

You can use the **queue-limitatmclp**command only with other queuing features, such as weighted fair queuing (WFQ). WFQ creates a queue for every class for which you define a class map. You can apply the policy map that you created with the atm clp based **queue-limit** command only to ATM interfaces on Cisco 12000 Series Routers.

Use the **queue-limitatmclp** command only after you have issued the **queue-limit**command using the same traffic class.

Use the **noqueue-limit** command to remove both the global queue-limit queue-size value and the queue-limit atm clp queue-size value if you configured it.

Packets satisfying the match criteria for a class accumulate in the queue reserved for the class until they are sent, which occurs when the queue is serviced by the weighted fair queuing process. When the defined maximum packet threshold for the class is reached, enqueuing of additional packets to the class queue causes tail drop.

You can specify the CLP queue-limit threshold in cells, milliseconds (ms), or microseconds (us). However, the unit of measure cannot be mixed. For example, if you specify the CLP queue-limit threshold in milliseconds, then you must also specify the global queue-limit threshold in milliseconds.

**Note** When you specify the queue-limit threshold as cells, milliseconds, or microseconds, it is internally converted to cells by using the visible bandwidth that is available to the class or the ATM virtual circuit (VC).

## Examples

In the following example, a policy map called "POLICY-ATM" has been configured. The "POLICY-ATM" policy map contains a class called "CLASS-ATM". The bandwidth for this class is specified as a percentage (20), and the **queue-limit** command sets the global queue-limit threshold to 1000 cells. The **queue-limitatmclp** command sets the queue-limit threshold for ATM CLP data to 100 cells:

```
Router> enable
Router# configure terminal
Router(config)# policy-map POLICY_ATM
Router(config-pmap)# class CLASS-ATM
Router(config-pmap-c)# bandwidth percent 20
Router(config-pmap-c)# queue-limit 1000 cells
Router(config-pmap-c)# queue-limit atm clp 100 cells
Router(config-pmap-c)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth (policy-map class)** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map. |
| **class class-default** | Specifies the default traffic class whose bandwidth is to be configured or modified. |
| **class (policy-map)** | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **queue-limit** | Specifies or modifies the maximum number of packets the queue can hold for a class configured in a policy map. |

# queue-list default

To assign a priority queue for those packets that do not match any other rule in the queue list, use the **queue-listdefault** command in global configuration mode. To restore the default value, use the **no**form of this command.

**queue-list** *list-number* **default** *queue-number*

**no queue-list** *list-number* **default** *queue-number*

## Syntax Description

| | |
|---|---|
| *list-number* | Number of the queue list. Any number from 1 to 16 that identifies the queue list. |
| *queue-number* | Number of the queue. Any number from 1 to 16. |

## Command Default

Disabled

The default number of the queue list is queue number 1.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

When you use multiple rules, remember that the system reads the **queue-list** commands in order of appearance. When classifying a packet, the system searches the list of rules specified by **queue-list** commands for a matching protocol or interface type. When a match is found, the system assigns the packet to the appropriate queue. The system searches the list in the order specified, and the first matching rule terminates the search.

Queue number 0 is a system queue. It is emptied before any of the other queues are processed. The system enqueues high-priority packets, such as keepalives, to this queue.

Use the**showinterfaces** command to display the current status of the output queues.

## Examples

In the following example, the default queue for list 10 is set to queue number 2:

```
queue-list 10 default 2
```

## Related Commands

| Command | Description |
|---|---|
| **custom-queue-list** | Assigns a custom queue list to an interface. |
| **queue-list interface** | Establishes queueing priorities on packets entering on an interface. |
| **queue-list protocol** | Establishes queueing priority based on the protocol type. |
| **queue-list queue byte-count** | Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle. |
| **queue-list queue limit** | Designates the queue length limit for a queue. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# queue-list interface

To establish queueing priorities on packets entering on an interface, use the**queue-listinterface** command in global configuration mode. To remove an entry from the list, use the **no** form of this command.

**queue-list** *list-number* **interface** *interface-type interface-number queue-number*

**no queue-list** *list-number* **interface** *interface-type interface-number queue-number*

## Syntax Description

| | |
|---|---|
| *list-number* | Number of the queue list. Any number from 1 to 16 that identifies the queue list. |
| *interface-type* | Type of the interface. |
| *interface-number* | Number of the interface. |
| *queue-number* | Number of the queue. Any number from 1 to 16. |

## Command Default

No queueing priorities are established.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

When you use multiple rules, remember that the system reads the **queue-list** commands in order of appearance. When classifying a packet, the system searches the list of rules specified by **queue-list** commands for a matching protocol or interface type. When a match is found, the system assigns the packet to the appropriate queue. The list is searched in the order specified, and the first matching rule terminates the search.

## Examples

In the following example, queue list 4 establishes queueing priorities for packets entering on interface tunnel 3. The queue number assigned is 10.

```
queue-list 4 interface tunnel 3 10
```

## Related Commands

| Command | Description |
|---|---|
| **custom-queue-list** | Assigns a custom queue list to an interface. |
| **queue-list default** | Assigns a priority queue for those packets that do not match any other rule in the queue list. |
| **queue-list protocol** | Establishes queueing priority based on the protocol type. |
| **queue-list queue byte-count** | Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle. |
| **queue-list queue limit** | Designates the queue length limit for a queue. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# queue-list lowest-custom

To set the lowest number for a queue to be treated as a custom queue, use the **queue-listlowest-custom**command in global configuration mode. To restore the default value, use the **no**form of this command.

**queue-list** *list-number* **lowest-custom** *queue-number*

**no queue-list** *list-number* **lowest-custom** *queue-number*

## Syntax Description

| | |
|---|---|
| *list-number* | Number of the queue list. Any number from 1 to 16 that identifies the queue list. |
| *queue-number* | Number of the queue. Any number from 1 to 16. |

## Command Default

The default number of the lowest custom queue is 1.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.0 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

All queues from queue 0 to the queue prior to the one specified in the **queue-listlowest-custom** command use the priority queue. (Queue 0 has the highest priority.)

All queues from the one specified in the **queue-listlowest-custom** command to queue 16 use a round-robin scheduler.

Use the**showqueueingcustom**command to display the current custom queue configuration.

## Examples

In the following example, the lowest custom value is set to 2 for queue list 4:

```
queue-list 4 lowest-custom 2
```

## Related Commands

| Command | Description |
|---|---|
| **custom-queue-list** | Assigns a custom queue list to an interface. |
| **queue-list interface** | Establishes queueing priorities on packets entering on an interface. |
| **queue-list protocol** | Establishes queueing priority based on the protocol type. |
| **queue-list queue byte-count** | Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle. |
| **queue-list queue limit** | Designates the queue length limit for a queue. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# queue-list protocol

To establish queueing priority based upon the protocol type, use the **queue-listprotocol** command in global configuration mode. To remove an entry from the list, use the **no**form of this command.

**queue-list** *list-number* **protocol** *protocol-name queue-number queue-keyword keyword-value*

**no queue-list** *list-number* **protocol** *protocol-name queue-number queue-keyword keyword-value*

## Syntax Description

| | |
|---|---|
| *list-number* | Number of the queue list. Any number from 1 to 16. |
| *protocol-name* | Protocol type: **aarp**, **appletalk**, **arp**, **bridge** (transparent), **clns**, **clns_es**, **clns_is**, **cmns**, **compressedtcp**, **decnet**, **decnet_node**, **decnet_routerl1**, **decnet_routerl2**, **dlsw**, **ip**, **ipx**, **pad**, **rsrb**, **stun** and **x25**. |
| *queue-number* | Number of the queue. Any number from 1 to 16. |
| *queue-keyword keyword-value* | Possible keywords are **fragments,gt,list,lt,tcp**, and **udp**. See the **priority-listprotocol** command for more information about this keyword. |

## Command Default

No queueing priorities are established.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2(13)T | This command was modified to remove apollo, vines, and xns from the list of protocol types. These protocols were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems (XNS) were removed in Release 12.2(13)T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

When you use multiple rules for a single protocol, remember that the system reads the **queue-list** commands in order of appearance. When classifying a packet, the system searches the list of rules specified by **queue-list** commands for a matching protocol. When a match is found, the system assigns the packet to the appropriate queue. The system searches the list in the order specified, and the first matching rule terminates the search.

The **decnet_router-l1** keyword refers to the multicast address for all level 1 routers, which are intra-area routers, and the **decnet_router-l2** keyword refers to all level 2 routers, which are interarea routers.

The **dlsw**,**rsrb**, and **stun**keywords refer only to direct encapsulation.

Use the tables listed in the **priority-listprotocol** command documention to configure the queueing priorities for your system.

## Examples

The following example assigns 1 as the custom queue list, specifies DECnet as the protocol type, and assigns 3 as a queue number to the packets sent on this interface:

```
queue-list 1 protocol decnet 3
```

The following example assigns DECnet packets with a size greater than 200 bytes to queue number 2:

```
queue-list 2 protocol decnet 2 gt 200
```

The following example assigns DECnet packets with a size less than 200 bytes to queue number 2:

```
queue-list 4 protocol decnet 2 lt 200
```

The following example assigns traffic that matches IP access list 10 to queue number 1:

```
queue-list 1 protocol ip 1 list 10
```

The following example assigns Telnet packets to queue number 2:

```
queue-list 4 protocol ip 2 tcp 23
```

The following example assigns User Datagram Protocol (UDP) Domain Name Service packets to queue number 2:

```
queue-list 4 protocol ip 2 udp 53
```

The following example assigns traffic that matches Ethernet type code access list 201 to queue number 1:

```
queue-list 1 protocol bridge 1 list 201
```

## Related Commands

| Command | Description |
|---|---|
| **custom-queue-list** | Assigns a custom queue list to an interface. |
| **queue-list default** | Assigns a priority queue for those packets that do not match any other rule in the queue list. |
| **queue-list queue byte-count** | Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle. |
| **queue-list queue limit** | Designates the queue length limit for a queue. |

| Command | Description |
|---|---|
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# queue-list queue byte-count

To specify how many bytes the system allows to be delivered from a given queue during a particular cycle , use the **queue-listqueuebyte-count** command in global configuration mode. To return the byte count to the default value, use the **no** form of this command.

**queue-list** *list-number* **queue** *queue-number* **byte-count** *byte-count-number*

**no queue-list** *list-number* **queue** *queue-number* **byte-count** *byte-count-number*

## Syntax Description

| | |
|---|---|
| *list-number* | Number of the queue list. Any number from 1 to 16. |
| *queue-number* | Number of the queue. Any number from 1 to 16. |
| *byte-count-number* | The average number of bytes the system allows to be delivered from a given queue during a particular cycle. |

## Command Default

This command is disabled by default. The default byte count is 1500 bytes.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Examples

In the following example, queue list 9 establishes the byte count as 1400 for queue number 10:

```
queue-list 9 queue 10 byte-count 1400
```

## Related Commands

| Command | Description |
|---|---|
| **custom-queue-list** | Assigns a custom queue list to an interface. |

| Command | Description |
|---|---|
| **queue-list default** | Assigns a priority queue for those packets that do not match any other rule in the queue list. |
| **queue-list interface** | Establishes queueing priorities on packets entering on an interface. |
| **queue-list protocol** | Establishes queueing priority based on the protocol type. |
| **queue-list queue byte-count** | Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle. |
| **queue-list queue limit** | Designates the queue length limit for a queue. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# queue-list queue limit

To designate the queue length limit for a queue, use the **queue-listqueuelimit** command in global configuration mode. To return the queue length to the default value, use the **no** form of this command.

**queue-list** *list-number* **queue** *queue-number* **limit** *limit-number*

**no queue-list** *list-number* **queue** *queue-number* **limit** *limit-number*

## Syntax Description

| | |
|---|---|
| *list-number* | Number of the queue list. Any number from 1 to 16. |
| *queue-number* | Number of the queue. Any number from 1 to 16. |
| *limit-number* | Maximum number of packets that can be enqueued at any time. The range is from 0 to 32767 queue entries. A value of 0 means that the queue can be of unlimited size. |

## Command Default

The default queue length limit is 20 entries.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Examples

In the following example, the queue length of queue 10 is increased to 40:

```
queue-list 5 queue 10 limit 40
```

## Related Commands

| Command | Description |
|---|---|
| **custom-queue-list** | Assigns a custom queue list to an interface. |

| Command | Description |
|---|---|
| **queue-list default** | Assigns a priority queue for those packets that do not match any other rule in the queue list. |
| **queue-list interface** | Establishes queueing priorities on packets entering on an interface. |
| **queue-list protocol** | Establishes queueing priority based on the protocol type. |
| **queue-list queue byte-count** | Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# random-detect

**Note** Effective with Cisco IOS Release 15.0(1)S and Cisco IOS Release 15.1(3)T, the **random-detect** command is hidden in interface configuration mode. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you enter a question mark at the command line. This command will be completely removed from interface configuration mode in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

To enable Weighted Random Early Detection (WRED) or distributed WRED (dWRED) on an interface, use the **random-detect** command in interface configuration mode. To configure WRED for a class in a policy map, use the **random-detect** command in QoS policy-map class configuration mode. To disable WRED or dWRED, use the **no** form of this command.

**random-detect** [**dscp-based**| **prec-based**]

**no random-detect**

## Syntax Description

| | |
|---|---|
| **dscp-based** | (Optional) Specifies that WRED is to use the differentiated services code point (DSCP) value when it calculates the drop probability for a packet. |
| **prec-based** | (Optional) Specifies that WRED is to use the IP Precedence value when it calculates the drop probability for a packet. |

## Command Default

WRED and dWRED are disabled by default.

## Command Modes

Interface configuration (config-if) QoS policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 11.1CC | This command was introduced. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. Arguments were added to support Differentiated Services (DiffServ) and Assured Forwarding (AF) Per Hop Behavior (PHB). |

| Release | Modification |
|---|---|
| 12.1(5a)E | This command was integrated into Cisco IOS Release 12.1(5a)E in policy map class configuration mode only. This command was implemented on Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers and Catalyst 6000 family switches with a FlexWAN module. |
| 12.0(15)S | This command was integrated into Cisco IOS Release 12.0(15)S in QoS policy-map class configuration mode only. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.0(28)S | This command was integrated into Cisco IOS Release 12.0(28)S in QoS policy map class configuration mode. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB in QoS policy map class configuration mode. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)T | Support was added for hierarchical queueing framework (HQF) using the modular quality of service (QoS) CLI (MQC). |
| 15.0(1)S | This command was modified. This command was hidden in interface configuration mode. |
| 15.1(3)T | This command was modified. This command was hidden in interface configuration mode. |
| Cisco IOS XE 3.6S | This command was modified. Support was added for the Cisco ASR 903 router. |

## Usage Guidelines

### Keywords

If you choose not to use either the **dscp-based** or the **prec-based** keyword, WRED uses the IP Precedence value (the default method) to calculate the drop probability for the packet.

### Availability

The **random-detect** command is not available at the interface level for Cisco IOS Releases 12.1E or 12.0S. The **random-detect** command is available in policy-map class configuration mode only for Cisco IOS Releases 12.1E, 12.0S, and later releases.

### WRED Functionality

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. dWRED is similar to WRED but uses the Versatile Interface Processor (VIP) instead of the Route Switch Processor (RSP). WRED and dWRED are most useful with protocols such as Transport Control Protocol (TCP) that respond to dropped packets by decreasing the transmission rate.

The router automatically determines parameters to use in the WRED calculations. To change these parameters, use the **random-detect precedence** command.

### Platform Support for dWRED

The dWRED feature is supported only on Cisco 7000 series routers with an RSP7000 card and Cisco 7500 series routers with a VIP2-40 or higher interface processor. A VIP2-50 interface processor is strongly recommended when the aggregate line rate of the port adapters on the VIP is greater than DS3. A VIP2-50 interface processor is required for OC-3 rates.

To use dWRED, distributed Cisco Express Forwarding switching must first be enabled on the interface. For more information on distributed Cisco Express Forwarding, refer to the *Cisco IOS Switching Services Configuration Guide* and the *Cisco IOS Switching Services Command Reference* .

### WRED in a Policy Map

You can configure WRED as part of the policy map for a standard class or the default class. The WRED **random-detect** command and the weighted fair queueing (WFQ) **queue-limit** command are mutually exclusive. If you configure WRED, its packet drop capability is used to manage the queue when packets exceeding the configured maximum count are enqueued. If you configure the WFQ **queue-limit** command, tail drop is used.

To configure a policy map and create class policies, use the **policy-map** and **class** (policy-map) commands. When creating a class within a policy map, you can use the **random-detect** command with either of the following commands:

- **bandwidth** (policy-map class)
- **fair-queue** (class-default)--for the default class only

**Note** If you use WRED packet drop instead of tail drop for one or more classes in a policy map, you must ensure that WRED is not configured on the interface to which you attach that policy map.

**Note** dWRED is not supported for classes in a policy map.

### Two Methods for Calculating the Drop Probability of a Packet

This command includes two optional keywords, **dscp-based** and **prec-based**, that determine the method WRED uses to calculate the drop probability of a packet.

Note the following points when deciding which method to instruct WRED to use:

- With the **dscp-based** keyword, WRED uses the DSCP value (that is, the first six bits of the IP type of service (ToS) byte) to calculate the drop probability.
- With the **prec-based** keyword, WRED will use the IP Precedence value to calculate the drop probability.

- The **dscp-based** and **prec-based** keywords are mutually exclusive.
- If neither argument is specified, WRED uses the IP Precedence value to calculate the drop probability (the default method).

## Examples

The following example configures WRED on the High-Speed Serial Interface (HSSI) 0/0/0 interface:

```
interface Hssi0/0/0
 random-detect
```

The following example configures the policy map called policy1 to contain policy specification for the class called class1. During times of congestion, WRED packet drop is used instead of tail drop.

```
! The following commands create the class map called class1:
class-map class1
 match input-interface fastethernet0/1
! The following commands define policy1 to contain policy specification for class1:
policy-map policy1
 class class1
  bandwidth 1000
  random-detect
```

The following example enables WRED to use the DSCP value 8. The minimum threshold for the DSCP value 8 is 24 and the maximum threshold is 40. This configuration was performed at the interface level.

```
Router(config)# interface serial0/0
Router(config-if)# random-detect dscp-based
Router(config-if)# random-detect dscp 8 24 40
```

The following example enables WRED to use the DSCP value 8 for class c1. The minimum threshold for DSCP value 8 is 24 and the maximum threshold is 40. The last line attaches the service policy to the output interface or virtual circuit (VC) p1.

```
Router(config-if)# class-map c1
Router(config-cmap)# match access-group 101
Router(config-if)# policy-map p1
Router(config-pmap)# class c1
Router(config-pmap-c)# bandwidth 48
Router(config-pmap-c)# random-detect dscp-based
Router(config-pmap-c)# random-detect dscp 8 24 40
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial0/0
Router(config-if)# service-policy output p1
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map or enables ATM overhead accounting. |
| **class** | Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before configuring its policy. |

| Command | Description |
|---|---|
| **fair-queue** | Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy. |
| **policy-map** | Creates a policy map that defines a Control Plane Policing and Protection (CoPP) per-user policy. |
| **queue-limit** | Specifies or modifies the queue limit (size) for a class in bytes, milliseconds (ms), microseconds (us) or packets. |
| **random-detect dscp** | Changes the minimum and maximum packet thresholds for the DSCP value. |
| **random-detect exponential-weighting-constant** | Configures the WRED and dWRED exponential weight factor for the average queue size calculation. |
| **random-detect flow** | Enables flow-based WRED. |
| **random-detect precedence** | Configures WRED and dWRED parameters for a particular IP Precedence. |
| **show interfaces** | Displays statistics for all interfaces configured on the router or access server. |
| **show queueing** | Lists all or selected configured queueing strategies. |
| **show tech-support rsvp** | Generates a report of all RSVP-related information. |

# random-detect (per VC)

**Note** Effective with Cisco IOS Release 15.1(3)T, the **random-detect**(per VC) command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release. For more information, see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

To enable per-virtual circuit (VC) Weighted Random Early Detection ( WRED) or per-VC VIP-distributed WRED ( DWRED), use the **random-detect**command in VC submode mode. To disable per-VC WRED and per-VC DWRED, use the **no** form of this command.

**random-detect** [**attach** *group-name*]

**no random-detect** [**attach** *group-name*]

## Syntax Description

| | | |
|---|---|---|
| **attach** | *group-name* | (Optional) Name of the WRED or DWRED group. |

## Command Default

WRED and DWRED are disabled by default.

## Command Modes

VC submode

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(3)T | This command was modified. This command was hidden. |

## Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. DWRED is similar to WRED but uses the Versatile Interface Processor (VIP) instead of the Route Switch Processor (RSP). WRED and DWRED are most useful with protocols like TCP that respond to dropped packets by decreasing the transmission rate.

WRED and DWRED are configurable at the interface and per-VC levels. The VC-level WRED or DWRED configuration will override the interface-level configuration if WRED or DWRED is also configured at the interface level.

Use this command to configure a single ATM VC or a VC that is a member of a bundle.

Note the following points when using the **random-detect**(per VC) command:

- If you use this command without the optional **attach** keyword, default WRED or DWRED parameters (such as minimum and maximum thresholds) are used.
- If you use this command with the optional **attach** keyword, the parameters defined by the specified WRED or DWRED parameter group are used. (WRED or DWRED parameter groups are defined through the **random-detect-group** command.) If the specified WRED or DWRED group does not exist, the VC is configured with default WRED or DWRED parameters.

When this command is used to configure an interface-level WRED or DWRED group to include per-VC WRED or DWRED as a drop policy, the configured WRED or DWRED group parameters are inherited under the following conditions:

- All existing VCs--including Resource Reservation Protocol (RSVP) switched virtual circuits (SVCs) that are not specifically configured with a VC-level WRED or DWRED group--will inherit the interface-level WRED or DWRED group parameters.
- Except for the VC used for signalling and the Interim Local Management Interface (ILMI) VC, any VCs created after the configuration of an interface-level DWRED group will inherit the parameters.

When an interface-level WRED or DWRED group configuration is removed, per-VC WRED or DWRED parameters are removed from any VC that inherited them from the configured interface-level WRED or DWRED group.

When an interface-level WRED or DWRED group configuration is modified, per-VC WRED or DWRED parameters are modified accordingly if the WRED or DWRED parameters were inherited from the configured interface-level WRED or DWRED group configuration.

This command is only supported on interfaces that are capable of VC-level queueing. The only currently supported interface is the Enhanced ATM port adapter (PA-A3).

The DWRED feature is only supported on Cisco 7000 series routers with an RSP7000 card and Cisco 7500 series routers with a VIP2-40 or greater interface processor. A VIP2-50 interface processor is strongly recommended when the aggregate line rate of the port adapters on the VIP is greater than DS3. A VIP2-50 interface processor is required for OC-3 rates.

To use DWRED, distributed Cisco Express Forwarding (dCEF) switching must first be enabled on the interface. For more information on dCEF, refer to the Cisco IOS Switching Services Configuration Guide and the Cisco IOS Switching Services Command Reference.

## Examples

The following example configures per-VC WRED for the permanent virtual circuit (PVC) called cisco. Because the **attach** keyword was not used, WRED uses default parameters.

```
pvc cisco 46
 random-detect
```

The following example creates a DWRED group called Rome and then applies the parameter group to an ATM PVC:

```
! The following commands create the DWRED parameter group Rome:
random-detect-group Rome
```

```
 precedence rsvp 46 50 10
 precedence 1 32 50 10
 precedence 2 34 50 10
 precedence 3 36 50 10
 precedence 4 38 50 10
 precedence 5 40 50 10
 precedence 6 42 50 10
 precedence 7 44 50 10
 exit
exit
! The following commands create a PVC on an ATM interface and then apply the
! DWRED group Rome to that PVC:
interface ATM2/0.23 point-to-point
 ip address 10.9.23.10 255.255.255.0
 no ip mroute-cache
 pvc vc1 201/201
  random-detect attach Rome
  vbr-nrt 2000 1000 200
  encapsulation aal5snap
```

The following **showqueueing** command displays the current settings for each of the IP Precedences following configuration of per-VC DWRED:

```
Router# show queueing random-detect interface atm2/0.23 vc 201/201
random-detect group Rome:
exponential weight 9
class    min-threshold    max-threshold    mark-probability
----------------------------------------------------------
0        30               50               1/10
1        32               50               1/10
2        34               50               1/10
3        36               50               1/10
4        38               50               1/10
5        40               50               1/10
6        42               50               1/10
7        44               50               1/10
rsvp     46               50               1/10
```

## Related Commands

| Command | Description |
|---|---|
| **class (policy-map)** | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy. |
| **random-detect exponential-weighting-constant** | Configures the WRED and DWRED exponential weight factor for the average queue size calculation. |
| **random-detect-group** | Defines the WRED or DWRED parameter group. |
| **random-detect precedence** | Configures WRED and DWRED parameters for a particular IP Precedence. |
| **show interfaces** | Displays the statistical information specific to a serial interface. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# random-detect aggregate

To enable aggregate Weighted Random Early Detection (WRED), use the **random-detectaggregate**command in policy-map class configuration mode. To disable aggregate WRED, use the **no** form of this command.

**random-detect** [**precedence-based**| **dscp-based**] **aggregate** [**minimum-thresh** *min-thresh* **maximum-thresh** *max-thresh* **mark-probability** *mark-prob*]

**no random-detect** [**precedence-based**| **dscp-based**] **aggregate**

## Syntax Description

| | |
|---|---|
| **precedence-based** | (Optional) Enables aggregate WRED based on IP precedence values. This is the default. |
| **dscp-based** | (Optional) Enables aggregate WRED based on differentiated services code point (DSCP) values. |
| **minimum-thresh** *min-thresh* | (Optional) Default minimum threshold (in number of packets) to be used for all subclasses (IP precedence or DSCP values) that have not been specifically configured. Valid values are from 1 to 12288. |
| **maximum-thresh** *max-thresh* | (Optional) Default maximum threshold (in number of packets) to be used for all subclasses (IP precedence or DSCP values) that have not been specifically configured. Valid values are from the minimum threshold argument to 12288. |
| **mark-probability** *mark-prob* | (Optional) Default denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. This value is used for all subclasses (IP precedence or DSCP values) that have not been specifically configured. Valid values are from 1 to 255. |

## Command Default

If no **precedence-based** or **dscp-based**keyword is specified in the command, the default is **precedence-based**.

If optional parameters for a default aggregate class are not defined, all subclass values that are not explicitly configured will use plain (non-weighted) RED drop behavior. This is different from standard random-detect configuration where the default is to always use WRED behavior.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXE | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2 on the Cisco 10000 series router for the PRE3. |

## Usage Guidelines

For ATM interfaces, the Aggregate WRED feature requires that the ATM SPA cards are installed in a Cisco 7600 SIP-200 carrier card or a Cisco 7600 SIP-400 carrier card.

To configure WRED on an ATM interface, you must use the random-detect aggregate commands; the standard random-detect commands are no longer supported on ATM interfaces.

The **precedence-based** and **dscp-based** keywords are mutually exclusive. If you do not specify either keyword, **precedence-based** is the default.

Defining WRED profile parameter values for the default aggregate class is optional. If defined, WRED profile parameters applied to the default aggregate class will be used for all subclasses that have not been explicitly configured. If all possible IP precedence or DSCP values are defined as subclasses, a default specification is unnecessary. If the optional parameters for a default aggregate class are not defined and packets with an unconfigured IP precedence or DSCP value arrive at the interface, plain (non-weighted) RED drop behavior will be used.

Use this command with a **random-detectprecedence**(aggregate) or **random-detectdscp**(aggregate) command within a policy map configuration to configure aggregate Weighted Random Early Detection (WRED) parameters for specific IP precedence or DSCP value(s).

After the policy map is defined, the policy map must be attached at the VC level.

Use the **showpolicy-mapinterface** command to display the statistics for aggregated subclasses.

## Examples

The following example shows a precedence-based aggregate WRED configuration for an ATM interface. Note that first a policy map named prec-aggr-wred is defined for the default class, then precedence-based Aggregate WRED is enabled with the **random-detectaggregate** command, then subclasses and WRED parameter values are assigned in a series of **random-detectprecedence**(aggregate)commands, and, finally, the policy map is attached at the ATM VC level using the **interface**and **service-policy** commands.

```
Router (config)# policy-map prec-aggr-wred
Router (config-pmap)# class class-default
Router (config-pmap-c)# random-detect aggregate
Router (config-pmap-c)# random-detect precedence values 0 1 2 3 minimum thresh 10
maximum-thresh 100 mark-prob 10
Router (config-pmap-c)# random-detect precedence values 4 5 minimum-thresh 40 maximum-thresh
 400 mark-prob 10
Router (config-pmap-c)# random-detect precedence values 6 minimum-thresh 60 maximum-thresh
 600 mark-prob 10
Router (config-pmap-c)# random-detect precedence values 7 minimum-thresh 70 maximum-thresh
 700 mark-prob 10
Router (config-pmap-c)# interface ATM4/1/0.10 point-to-point
Router (config-subif)# ip address 10.0.0.2 255.255.255.0
```

```
Router (config-subif)# pvc 10/110
Router (config-subif)# service-policy output prec-aggr-wred
```

The following example shows a DSCP-based aggregate WRED configuration for an ATM interface. Note that first a policy map named dscp-aggr-wred is defined for the default class, then dscp-based Aggregate WRED is enabled with the **random-detectdscp-basedaggregate** command, then subclasses and WRED parameter values are assigned in a series of **random-detectdscp** (aggregate) commands, and, finally, the policy map is attached at the ATM VC level using the **interface**and **service-policy** commands.

```
Router (config)# policy-map dscp-aggr-wred
Router (config-pmap)# class class-default
Router (config-pmap-c)# random-detect dscp-based aggregate minimum-thresh 1 maximum-thresh
 10 mark-prob 10
Router (config-pmap-c)# random-detect dscp values 0 1 2 3 4 5 6 7 minimum-thresh 10
maximum-thresh 20 mark-prob 10
Router (config-pmap-c)# random-detect dscp values 8 9 10 11 minimum-thresh 10 maximum-thresh
 40 mark-prob 10
Router (config)# interface ATM4/1/0.11 point-to-point
Router (config-subif)# ip address 10.0.0.2 255.255.255.0
Router (config-subif)# pvc 11/101
Router (config-subif)# service-policy output dscp-aggr-wred
```

## Related Commands

| Command | Description |
|---|---|
| **class (policy-map)** | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy. |
| **interface** | Configures an interface type and enters interface configuration mode. |
| **policy-map** | Creates a policy map that can be attached to one or more interfaces to specify a service policy. |
| **random-detect precedence (aggregate)** | Configures aggregate WRED parameters for specific IP precedence values. |
| **random-detect dscp (aggregate)** | Configures aggregate WRED parameters for specific DSCP values. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

# random-detect atm-clp-based

To enable weighted random early detection (WRED) on the basis of the ATM cell loss priority (CLP) of a packet, use the **random-detectatm-clp-based** command in policy-map class configuration mode. To disable WRED, use the **no** form of this command.

**random-detect atm-clp-based** *clp-value*

**no random-detect atm-clp-based**

**Cisco 10000 Series Router**

**random-detect atm-clp-based** *min-thresh-value max-thresh-value mark-probability-denominator-value*

**no random-detect atm-clp-based**

## Syntax Description

| | |
|---|---|
| *clp-value* | CLP value. Valid values are 0 or 1. |
| *min-thresh-value* | Minimum threshold in number of packets. Valid values are 1 to 4096. |
| *max-thresh-value* | Maximum threshold in number of packets. Valid values are 1 to 4096. |
| *max-probability-denominator-value* | Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. Valid values are 1 to 65535. |

## Command Default

When WRED is configured, the default minimum and maximum thresholdsare determined on the basis of output buffering capacity and the transmission speed for the interface.

The default maximum probability denominator is 10.

On the Cisco 10000 series router, the default is disabled.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.0(28)S | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SB | This command was introduced on the PRE3 and PRE4 for the Cisco 10000 series router. |

| Release | Modification |
|---|---|
| 12.4(20)T | Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC). |

## Usage Guidelines

You cannot use the **random-detectatm-clp-based** command with the **random-detectcos-based** command in the same HQF configuration. You must use the **norandom-detectcos-based** command to disable it before you configure the **random-detectatm-clp-based** command.

## Examples

In the following example, WRED is configured on the basis of the ATM CLP. In this configuration, the **random-detectatm-clp-based**command has been configured and an ATM CLP of 1 has been specified.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policymap1
Router(config-pmap)# class class1
Router(config-pmap-c)# random-detect atm-clp-based 1
Router(config-pmap-c)#

end
```

## Related Commands

| Command | Description |
|---|---|
| **random-detect clp** | Specifies the ATM CLP value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling WRED. |
| **random-detect cos** | Specifies the CoS value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling WRED. |
| **random-detect cos-based** | Enables WRED on the basis of the CoS value of a packet. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# random-detect clp

To specify the ATM cell loss priority (CLP) value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling weighted random early detection (WRED), use the **random-detect clp** command in policy-map class configuration mode. To reset the thresholds and maximum probability denominator to the default values for the specified ATM CLP, use the **no** form of this command.

**random-detect clp** *clp-value min-threshold max-threshold max-probability-denominator*

**no random-detect clp** *clp-value min-threshold max-threshold max-probability-denominator*

## Syntax Description

| | |
|---|---|
| *clp-value* | CLP value. Valid values are 0 or 1. |
| *min-threshold* | Minimum threshold in number of packets. Valid values are in the range 1 to 512000000. |
| *max-threshold* | Maximum threshold in number of packets. Valid values are in the range 1 to 512000000. |
| *max-probability-denominator* | Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. Valid values are 1 to 65535. |

## Command Default

The default values for the *min-threshold* and *max-threshold* arguments are based on the output buffering capacity and the transmission speed for the interface.

The default for the *max-probability-denominator* argument is 10; that is, 1 out of every 10 packets is dropped at the maximum threshold.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.0(28)S | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 15.2(2)T | This command was modified. The maximum and minimum threshold ranges were changed. |

## Usage Guidelines

Note the following points when using the **random-detect clp** command:

- When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified IP precedence.
- When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified IP precedence.
- While the range of values for the *min-threshold* and *max-threshold* arguments is from 1 to 512000000, the actual values that you can specify depend on the type of random detect you are configuring. For example, the maximum threshold value cannot exceed the queue limit.
- The *max-probability-denominator* argument is the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold.

## Examples

In the following example, WRED has been enabled using the **random-detect clp** command. With the **random-detect clp** command, the ATM CLP has been specified, along with the minimum and maximum thresholds, and the maximum probability denominator.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policymap1
Router(config-pmap)# class class1
Router(config-pmap-c)# random-detect clp 1 12 25 1/10
Router(config-pmap-c)# end
```

## Related Commands

| Command | Description |
|---|---|
| **random-detect atm-clp-based** | Enables WRED on the basis of the ATM CLP of a packet. |
| **random-detect cos** | Specifies the CoS value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling WRED. |
| **random-detect cos-based** | Enables WRED on the basis of the CoS value of a packet. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# random-detect cos-based

To enable weighted random early detection (WRED) on the basis of the class of service (CoS) value of a packet, use the **random-detectcos-based** command in policy-map class configuration mode. To disable WRED, use the **no** form of this command.

**random-detect cos-based** *cos-value*

**no random-detect cos-based**

## Syntax Description

| | |
|---|---|
| *cos-value* | Specific IEEE 802.1Q CoS values from 0 to 7. |

## Command Default

When WRED is configured, the default minimum and maximum thresholds are determined on the basis of output buffering capacity and the transmission speed for the interface.

The default maximum probability denominator is 10.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.0(28)S | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.4(20)T | Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC). |

## Usage Guidelines

You cannot use the **random-detectcos-based** command with the **random-detectatm-clp-based** command in the same HQF configuration. You must use the **norandom-detectatm-clp-based** command to disable it before you configure the **random-detectcos-based** command.

## Examples

In the following example, WRED is configured on the basis of the CoS value. In this configuration, the **random-detectcos-based**command has been configured and a CoS value of 2 has been specified.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policymap1
Router(config-pmap)# class class1
Router(config-pmap-c)# random-detect cos-based 2
Router(config-pmap-c)#

end
```

## Related Commands

| Command | Description |
|---|---|
| **random-detect atm-clp-based** | Enables WRED on the basis of the ATM CLP of a packet. |
| **random-detect clp** | Specifies the ATM CLP value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling WRED. |
| **random-detect cos** | Specifies the CoS value of a packet, the minimum and maximum thresholds, and the maximum probability denominator used for enabling WRED. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# random-detect discard-class

To configure the weighted random early detection (WRED) parameters for a discard-class value for a class policy in a policy map, use the **random-detectdiscard-class** command in policy-map class configuration mode. To disable the discard-class values, use the **no** form of this command.

**random-detect discard-class** *value min-threshold max-threshold max-probability-denominator*

**no random-detect discard-class** *value min-threshold max-threshold max-probability-denominator*

## Syntax Description

| | |
|---|---|
| *value* | Discard class. This is a number that identifies the drop eligibility of a packet. Valid values are 0 to 7. |
| *min-threshold* | Specifies the minimum number of packets allowed in the queue. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified DSCP, IP precedence, or discard-class value. Valid minimum threshold values are 1 to 512000000. |
| *max-threshold* | Specifies the maximum number of packets allowed in the queue. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified DSCP, IP precedence, or discard-class value. Valid maximum threshold values are 1 to 512000000. |
| *max-probability-denominator* | Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. Valid values are 1 to 65535. |

## Command Default

For all precedence levels, the *max-probability-denominator* default is 10 packets; that is, 1 out of every 10 packets is dropped at the maximum threshold.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. |

| Release | Modification |
|---|---|
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router. |
| 15.2(2)T | This command was modified. The maximum and minimum threshold ranges were changed. |

## Usage Guidelines

When you configure the **random-detect discard-class** command on an interface, packets are given preferential treatment based on the discard class of the packet. Use the **random-detect discard-class** command to adjust the discard class for different discard-class values.

**Note** While the range of values for the *min-threshold* and *max-threshold* arguments is from 1 to 512000000, the actual values that you can specify depend on the type of random detect you are configuring. For example, the maximum threshold value cannot exceed the queue limit.

### Cisco 10000 Series Router

You must first enable the drop mode using the **random-detect discard-class-based** command. You can then set the drop probability profile using the **random-detect discard-class** command.

The table below lists the default drop thresholds for WRED based on differentiated services code point (DSCP), IP precedence, and discard class. The drop probability indicates that the router drops one packet for every 10 packets.

***Table 34: WRED Default Drop Thresholds***

| DSCP, Precedence, and Discard-Class Values | Minimum Threshold (Times the Queue Size) | Maximum Threshold (Times the Queue Size) | Drop Probability |
|---|---|---|---|
| All DSCPs | 1/4 | 1/2 | 1/10 |
| 0 | 1/4 | 1/2 | 1/10 |
| 1 | 9/32 | 1/2 | 1/10 |
| 2 | 5/16 | 1/2 | 1/10 |
| 3 | 11/32 | 1/2 | 1/10 |
| 4 | 3/8 | 1/2 | 1/10 |
| 5 | 13/32 | 1/2 | 1/10 |
| 6 | 7/16 | 1/2 | 1/10 |
| 7 | 15/32 | 1/2 | 1/10 |

## Examples

The following example shows how to configure discard class 2 to randomly drop packets when the average queue reaches the minimum threshold of 100 packets and 1 in 10 packets are dropped when the average queue is at the maximum threshold of 200 packets:

```
policy-map set-MPLS-PHB
 class IP-AF11
  bandwidth percent 40
  random-detect discard-class-based
  random-detect-discard-class 2 100 200 10
```

## Examples

The following example shows how to enable discard-class-based WRED. In this example, the configuration of the class map named Silver indicates to classify traffic based on discard class 3 and 5. Traffic that matches discard class 3 or 5 is assigned to the class named Silver in the policy map named Premium. The Silver configuration includes WRED packet dropping based on discard class 5 with a minimum threshold of 500, maximum threshold of 1500, and a mark-probability-denominator of 200. The QoS policy is applied to PVC 1/81 on point-to-point ATM subinterface 2/0/0.2 in the outbound direction.

```
Router(config)# class-map Silver
Router(config-cmap)# match discard-class 3 5
Router(config-cmap)# exit
Router(config)# policy-map Premium
Router(config-pmap)# class Silver
Router(config-pmap-c)# bandwidth percent 30
Router(config-pmap-c)# random-detect discard-class-based
Router(config-pmap-c)# random-detect discard-class 5 500 1500 200
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm 2/0/0
Router(config-if)# atm pxf queuing
Router(config-if)# interface atm 2/0/0.2 point-to-point
Router(config-subif)# pvc 1/81
Router(config-subif-atm-vc)# ubr 10000
Router(config-subif-atm-vc)# service-policy output Premium
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth (policy-map class)** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map. |
| **match discard-class** | Matches packets of a certain discard-class. |
| **random-detect discard-class-based** | Bases WRED on the discard class value of a packet. |
| **random-detect exponential-weighting-constant** | Configures the WRED and DWRED exponential weight factor for the average queue size calculation. |
| **random-detect precedence** | Configures WRED and DWRED parameters for a particular IP precedence. |

| Command | Description |
|---|---|
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

# random-detect discard-class-based

To base weighted random early detection (WRED) on the discard class value of a packet, use the **random-detectdiscard-class-based** command in policy-map class configuration mode. To disable this feature, use the **no** form of this command.

**random-detect discard-class-based**

**no random-detect discard-class-based**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The defaults are router-dependent.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |

## Usage Guidelines

Enter this command so that WRED is based on the discard class instead of on the IP precedence field.

## Examples

The following example shows that random detect is based on the discard class value of a packet:

```
policy-map name
 class-name
  bandwidth percent 40
  random-detect discard-class-based
```

## Related Commands

| Command | Description |
|---|---|
| **match discard-class** | Matches packets of a certain discard class. |

# random-detect dscp

**Note** Effective with Cisco IOS Release 15.1(3)T, the **random-detect dscp** command is hidden in interface configuration mode. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you enter a question mark at the command line. This command will be completely removed from interface configuration mode in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

To change the minimum and maximum packet thresholds for the differentiated services code point (DSCP) value, use the **random-detect dscp** command in interface or QoS policy-map class configuration mode. To return the minimum and maximum packet thresholds to the default for the DSCP value, use the **no** form of this command.

**random-detect dscp** *dscp-value min-threshold max-threshold* [ *mark-probability-denominator* ]

**no random-detect dscp** *dscp-value min-threshold max-threshold* [ *mark-probability-denominator* ]

## Syntax Description

| | |
|---|---|
| *dscp-value* | The DSCP value. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs7**, **ef**, or **rsvp**. |
| *min-threshold* | Minimum threshold in number of packets. The value range of this argument is from 1 to 512000000. When the average queue length reaches the minimum threshold, Weighted Random Early Detection (WRED) or distributed WRED (dWRED) randomly drop some packets with the specified DSCP value. |
| *max-threshold* | Maximum threshold in number of packets. The value range of this argument is from the value of the *min-threshold* argument to 512000000. When the average queue length exceeds the maximum threshold, WRED or dWRED drop all packets with the specified DSCP value. |

| | |
|---|---|
| *mark-probability-denominator* | (Optional) Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. The value range is from 1 to 65536. The default is 10; that is, 1 out of every 10 packets is dropped at the maximum threshold. |

## Command Default

The default values for the **random-detect dscp** command are different on Versatile Interface Processor (VIP)-enabled Cisco 7500 series routers and Catalyst 6000 family switches with a FlexWAN module (dWRED). All other platforms running WRED have another set of default values. For more information about **random-detect dscp** defaults, see the "Usage Guidelines" section.

## Command Modes

Interface configuration (config-if) QoS policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.1(5)T | This command was introduced. |
| 12.1(5a)E | This command was integrated into Cisco IOS Release 12.1(5a)E in policy-map class configuration mode only. This command was implemented on VIP-enabled Cisco 7500 series routers and Catalyst 6000 family switches with a FlexWAN module. |
| 12.0(15)S | This command was integrated into Cisco IOS Release 12.0(15)S in QoS policy-map class configuration mode. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(3)T | This command was modified. This command was hidden in interface configuration mode. |
| 15.2(2)T | This command was modified. The maximum and minimum threshold ranges were changed. |
| Cisco IOS XE Release 3.6S | This command was modified. Support was added for the Cisco ASR 903 router. |

## Usage Guidelines

Use the **random-detect dscp** command in conjunction with the **random-detect** command in interface configuration mode.

The **random-detect dscp** command is available only if you specified the *dscp-based* argument when using the **random-detect** command in interface configuration mode.

**Note** The **random-detect dscp** command is not available at the interface level for Cisco IOS Release 12.1E or Release 12.0S. The **random-detect dscp** command is available only in QoS policy-map class configuration mode in Cisco IOS Release 12.1E.

### Defaults for VIP-Enabled Cisco 7500 Series Routers and Catalyst 6000 Family Switches with a FlexWAN Module

For all IP precedence values, the default *mark-probability-denominator* is 10, and the *max-threshold* value is based on the output buffering capacity and the transmission speed of the interface.

The default *min-threshold* value depends on the IP precedence value. The *min-threshold* value for IP precedence 0 corresponds to half of the *max-threshold* value. The values for the remaining IP precedence values fall between half the *max-threshold* value and the *max-threshold* value at even intervals.

**Note** Although the range of values for the *min-threshold* and *max-threshold* arguments is from 1 to 512000000, the actual values that you can specify depend on the type of random detect you are configuring. For example, the maximum threshold value cannot exceed the queue limit.

Unless the maximum and minimum threshold values for the DSCP values are configured by the user, all DSCP values have the same minimum threshold and maximum threshold values as the value specified for precedence 0.

### Specifying the DSCP Value

The **random-detect dscp** command allows you to specify the DSCP value per traffic class. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs7**, **ef**, or **rsvp**.

On a particular traffic class, eight DSCP values can be configured per traffic class. Overall, 29 values can be configured on a traffic class: 8 precedence values, 12 Assured Forwarding (AF) code points, 1 Expedited Forwarding code point, and 8 user-defined DSCP values.

### Assured Forwarding Code Points

The AF code points provide a means for a domain to offer four different levels (four different AF classes) of forwarding assurances for IP packets received from other (such as customer) domains. Each one of the four AF classes is allocated a certain amount of forwarding services (buffer space and bandwidth).

Within each AF class, IP packets are marked with one of three possible drop precedence values (binary 2{010}, 4{100}, or 6{110}), which exist as the three lowest bits in the DSCP header. In congested network environments, the drop precedence value of the packet determines the importance of the packet within the AF class. Packets with higher drop precedence values are discarded before packets with lower drop precedence values.

The upper three bits of the DSCP value determine the AF class; the lower three values determine the drop probability.

### Expedited Forwarding Code Points

The EF code point is usually used to mark high-priority, time-sensitive data. The EF code point marking is equal to the highest precedence value; therefore, the EF code point is always equal to precedence value 7.

### Class Selector Values

The Class Selector (CS) values are equal to IP precedence values (for instance, cs1 is the same as IP precedence 1).

### Default Values

The table below lists the default WRED minimum threshold value for each IP precedence value on the distributed platforms.

***Table 35: Default WRED Minimum Threshold Values for the Distributed Platforms***

| IP (Precedence) | Class Selector (CS) Value | Minimum Threshold Value (Fraction of Maximum Threshold Value) | Notes About the Value |
|---|---|---|---|
| 0 | cs0 | 8/16 | All DSCP values that are not configured by the user will have the same threshold values as IP precedence 0. |
| 1 | cs1 | 9/16 | -- |
| 2 | cs2 | 10/16 | -- |
| 3 | cs3 | 11/16 | -- |
| 4 | cs4 | 12/16 | -- |
| 5 | cs5 | 13/16 | -- |
| 6 | cs6 | 14/16 | -- |
| 7 | cs7 | 15/16 | The EF code point will always be equal to IP precedence 7. |

### Defaults for Non-VIP-Enabled Cisco 7500 Series Routers and Catalyst 6000 Family Switches with a FlexWAN Module

All platforms except the VIP-enabled Cisco 7500 series router and the Catalyst 6000 have the default values shown in the table below.

If WRED is using the DSCP value to calculate the drop probability of a packet, all 64 entries of the DSCP table are initialized with the default settings shown in the table below.

***Table 36: random-detect dscp Default Settings***

| DSCP (Precedence) | Minimum Threshold | Maximum Threshold | Mark Probability |
|---|---|---|---|
| 0 (0) | 20 | 40 | 1/10 |
| 1 | 22 | 40 | 1/10 |
| 2 | 24 | 40 | 1/10 |
| 3 | 26 | 40 | 1/10 |
| 4 | 28 | 40 | 1/10 |
| 5 | 30 | 40 | 1/10 |
| 6 | 32 | 40 | 1/10 |
| 7 | 34 | 40 | 1/10 |
| 8 (1) | 22 | 40 | 1/10 |
| 9 | 22 | 40 | 1/10 |
| 10 | 24 | 40 | 1/10 |
| 11 | 26 | 40 | 1/10 |
| 12 | 28 | 40 | 1/10 |
| 13 | 30 | 40 | 1/10 |
| 14 | 32 | 40 | 1/10 |
| 15 | 34 | 40 | 1/10 |
| 16 (2) | 24 | 40 | 1/10 |
| 17 | 22 | 40 | 1/10 |
| 18 | 24 | 40 | 1/10 |

| DSCP (Precedence) | Minimum Threshold | Maximum Threshold | Mark Probability |
|---|---|---|---|
| 19 | 26 | 40 | 1/10 |
| 20 | 28 | 40 | 1/10 |
| 21 | 30 | 40 | 1/10 |
| 22 | 32 | 40 | 1/10 |
| 23 | 34 | 40 | 1/10 |
| 24 (3) | 26 | 40 | 1/10 |
| 25 | 22 | 40 | 1/10 |
| 26 | 24 | 40 | 1/10 |
| 27 | 26 | 40 | 1/10 |
| 28 | 28 | 40 | 1/10 |
| 29 | 30 | 40 | 1/10 |
| 30 | 32 | 40 | 1/10 |
| 31 | 34 | 40 | 1/10 |
| 32 (4) | 28 | 40 | 1/10 |
| 33 | 22 | 40 | 1/10 |
| 34 | 24 | 40 | 1/10 |
| 35 | 26 | 40 | 1/10 |
| 36 | 28 | 40 | 1/10 |
| 37 | 30 | 40 | 1/10 |
| 38 | 32 | 40 | 1/10 |
| 39 | 34 | 40 | 1/10 |
| 40 (5) | 30 | 40 | 1/10 |
| 41 | 22 | 40 | 1/10 |
| 42 | 24 | 40 | 1/10 |

| DSCP (Precedence) | Minimum Threshold | Maximum Threshold | Mark Probability |
|---|---|---|---|
| 43 | 26 | 40 | 1/10 |
| 44 | 28 | 40 | 1/10 |
| 45 | 30 | 40 | 1/10 |
| 46 | 36 | 40 | 1/10 |
| 47 | 34 | 40 | 1/10 |
| 48 (6) | 32 | 40 | 1/10 |
| 49 | 22 | 40 | 1/10 |
| 50 | 24 | 40 | 1/10 |
| 51 | 26 | 40 | 1/10 |
| 52 | 28 | 40 | 1/10 |
| 53 | 30 | 40 | 1/10 |
| 54 | 32 | 40 | 1/10 |
| 55 | 34 | 40 | 1/10 |
| 56 (7) | 34 | 40 | 1/10 |
| 57 | 22 | 40 | 1/10 |
| 58 | 24 | 40 | 1/10 |
| 59 | 26 | 40 | 1/10 |
| 60 | 28 | 40 | 1/10 |
| 61 | 30 | 40 | 1/10 |
| 62 | 32 | 40 | 1/10 |
| 63 | 34 | 40 | 1/10 |
| rsvp | 36 | 40 | 1/10 |

## Examples

The following example enables WRED to use the DSCP value 8. The minimum threshold for the DSCP value 8 is 20, the maximum threshold is 40, and the mark probability is 1/10.

```
random-detect dscp 8 20 40 10
```

## Related Commands

| Command | Description |
|---|---|
| **random-detect** | Enables WRED or dWRED. |
| **show queueing** | Lists all or selected configured queueing strategies. |
| **show queueing interface** | Displays the queueing statistics of an interface or VC. |

# random-detect dscp (aggregate)

To configure aggregate Weighted Random Early Detection (WRED) parameters for specific differentiated services code point (DSCP) value, use the **random-detectdscpvalues(aggregate)**command in QoS policy-map class configuration mode. To disable configuration of aggregate WRED DSCP values, use the **no** form of this command.

**random-detect dscp** *sub-class-val1 sub-class-val2 sub-class-val3 sub-class-val4 min-thresh max-thresh mark-prob*

**no random-detect dscp** *sub-class-val1 sub-class-val2 sub-class-val3 sub-class-val4 min-thresh max-thresh mark-prob*

### Cisco 10000 Series Router (PRE3)

**random-detect dscp values sub-class-val1** [... **[sub-class-val8]**] **minimum-thresh** *min-thresh-value* **maximum-thresh** *max-thresh-value* **mark-prob** *mark-prob-value*

**no random-detect dscp values sub-class-val1** [... **[sub-class-val8]**] **minimum-thresh** *min-thresh-value* **maximum-thresh** *max-thresh-value* **mark-prob** *mark-prob*

## Syntax Description

| | |
|---|---|
| *sub-class-val1*<br>*sub-class-val2*<br>*sub-class-val3*<br>*sub-class-val4* | DSCP value(s) to which the following WRED profile parameter specifications are to apply. A maximum of eight subclasses (DSCP values) can be specified per command-line interface (CLI) entry. See the "Usage Guidelines" for a list of valid DSCP values. |
| *min-thresh* | The minimum number of packets allowed in the queue. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified DSCP value. Valid minimum threshold values are 1 to 16384. |
| *max-thresh* | The maximum number of packets allowed in the queue. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified DSCP value. Valid maximum threshold values are 1 to 16384. |
| *mark-prob* | The denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. Valid values are 1 to 65535. |
| **Cisco 10000 Series Router** | |

| | |
|---|---|
| **values** *sub-class-val1* [...[*subclass-val8*]] | DSCP value(s) to which the following WRED profile parameter specifications are to apply. A maximum of 8 subclasses (DSCP values) can be specified per CLI entry. The DSCP value can be a number from 0 to 63, or it can be one of the following keywords: **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, or **cs7**. |
| **minimum-thresh** *min-thresh* | Specifies the minimum number of packets allowed in the queue. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified DSCP value. Valid minimum threshold values are 1 to 16384. |
| **maximum-thresh** *max-thresh* | Specifies the maximum number of packets allowed in the queue. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified DSCP value. Valid maximum threshold values are 1 to 16384. |
| **mark-probability** *mark-prob* | Specifies the denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. Valid values are 1 to 65535. |

## Command Default

For all precedence levels, the mark-prob default value is 10 packets.

## Command Modes

QoS policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXE | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2 and implemented on the Cisco 10000 series router. |

## Usage Guidelines

For ATM interfaces, the Aggregate WRED feature requires that the ATM SPA cards are installed in a Cisco 7600 SIP-200 carrier card or a Cisco 7600 SIP-400 carrier card.

To configure WRED on an ATM interface, you must use the**random-detectaggregate**commands; the standard random-detect commands are no longer supported on ATM interfaces.

Use this command with a **random-detectaggregate** command within a policy map configuration.

Repeat this command for each set of DSCP values that share WRED parameters.

After the policy map is defined, the policy map must be attached at the virtual circuit (VC) level.

The set of subclass (DSCP precedence) values defined on a **random-detectdscp(aggregate)**CLI will be aggregated into a single hardware WRED resource. The statistics for these subclasses will also be aggregated.

Use the **showpolicy-mapinterface** command to display the statistics for aggregated subclasses.

**Cisco 10000 Series Router**

For the PRE2, the random-detect command specifies the default profile for the queue. For the PRE3, the aggregate random-detect command is used instead to configure aggregate parameters for WRED. The PRE3 accepts the PRE2 random-detect command as a hidden command.

On the PRE2, accounting for the default profile is per precedence. On the PRE3, accounting and configuration for the default profile is per class map.

On the PRE2, the default threshold is per precedence for a DSCP or precedence value without an explicit threshold configuration. On the PRE3, the default threshold is to have no WRED configured.

On the PRE2, the drop counter for each precedence belonging to the default profile only has a drop count that matches the specific precedence value. Because the PRE2 has a default threshold for the default profile, the CBQOSMIB displays default threshold values. On the PRE3, the drop counter for each precedence belonging to the default profile has the aggregate counter of the default profile and not the individual counter for a specific precedence. The default profile on the PRE3 does not display any default threshold values in the CBQOSMIB if you do not configure any threshold values for the default profile.

**DSCP Values**

You must enter one or more differentiated service code point (DSCP) values. The command may include any combination of the following:

- numbers (0 to 63) representing differentiated services code point values
- af numbers (for example, af11) identifying specific AF DSCPs
- cs numbers (for example, cs1) identifying specific CS DSCPs
- **default** --Matches packets with the default DSCP.
- **ef** --Matches packets with EF DSCP.

For example, if you wanted the DCSP values of 0, 1, 2, 3, 4, 5, 6, or 7 (note that only one of the IP DSCP values must be a successful match criterion, not all of the specified DSCP values), enter the **matchdscp01234567** command.

## Examples

The following example shows how to create a class map named map1 and associate it with the policy map named map2. The configuration enables WRED to drop map1 packets based on DSCP 8 with a minimum threshold of 24 and a maximum threshold of 40. The map2 policy map is attached to the outbound ATM interface 1/0/0.

```
Router(config-if)# class-map map1
Router(config-cmap)# match access-group 10
Router(config-cmap)# exit
Router(config)# policy-map map2
```

```
Router(config-pmap)# class map1
Router(config-pmap-c)# bandwidth 48
Router(config-pmap-c)# random-detect dscp-based
Router(config-pmap-c)# random-detect dscp 8 24 40
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm 1/0/0
Router(config-if)# service-policy output map2
```

The following example shows a DSCP-based aggregate WRED configuration for an ATM interface. Note that first a policy map named dscp-aggr-wred is defined for the default class, then dscp-based aggregate WRED is enabled with the **random-detectdscp-basedaggregate** command, then subclasses and WRED parameter values are assigned in a series of **random-detectdscp(aggregate)**commands, and, finally, the policy map is attached at the ATM VC level using the **interface**and **service-policy** commands.

```
Router(config)# policy-map dscp-aggr-wred
Router(config-pmap)# class class-default
Router(config-pmap-c)# random-detect dscp-based aggregate minimum-thresh 1 maximum-thresh
10 mark-prob 10
!
! Define an aggregate subclass for packets with DSCP values of 0-7 and assign the WRED
! profile parameter values for this subclass
Router(config-pmap-c)# random-detect dscp 0 1 2 3 4 5 6 7 minimum-thresh 10 maximum-thresh
 20 mark-prob 10
Router(config-pmap-c) random-detect dscp 8 9 10 11 minimum-thresh 10 maximum-thresh 40
mark-prob 10
Router(config)# interface ATM4/1/0.11 point-to-point
Router(config-subif)# ip address 10.0.0.2 255.255.255.0
Router(config-subif) pvc 11/101
Router(config-subif)# service-policy output dscp-aggr-wred
```

## Examples

The following example shows how to create a class map named Gold and associate it with the policy map named Business. The configuration enables WRED to drop Gold packets based on DSCP 8 with a minimum threshold of 24 and a maximum threshold of 40. The Business policy map is attached to the outbound ATM interface 1/0/0.

```
Router(config-if)# class-map Gold
Router(config-cmap)# match access-group 10
Router(config-cmap)# exit
Router(config)# policy-map Business
Router(config-pmap)# class Gold
Router(config-pmap-c)# bandwidth 48
Router(config-pmap-c)# random-detect dscp-based
Router(config-pmap-c)# random-detect dscp values 8 minimum-thresh 24 maximum-thresh 40
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm 1/0/0
Router(config-if)# service-policy output Business
```

## Related Commands

| Command | Description |
|---|---|
| **class (policy-map)** | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy. |
| **interface** | Configures an interface type and enters interface configuration mode. |

| Command | Description |
|---|---|
| **policy-map** | Creates a policy map that can be attached to one or more interfaces to specify a service policy. |
| **random-detect aggregate** | Enables aggregate WRED and optionally specifies default WRED parameter values for a default aggregate class. This default class will be used for all subclasses that have not been explicitly configured. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

# random-detect ecn

To enable explicit congestion notification (ECN), use the **random-detectecn**command in policy-map class configuration mode. To disable ECN, use the **no** form of this command.

**random-detect ecn**

**no random-detect ecn**

## Syntax Description

This command has no arguments or keywords.

## Command Default

By default, ECN is disabled.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(8)T | This command was introduced. |

## Usage Guidelines

If ECN is enabled, ECN can be used whether Weighted Random Early Detection (WRED) is based on the IP precedence value or the differentiated services code point (DSCP) value.

## Examples

The following example enables ECN in a policy map called “pol1”:

```
Router(config)# policy-map pol1
Router(config-pmap)# class class-default
Router(config-pmap)# bandwidth per 70
Router(config-pmap-c)# random-detect
Router(config-pmap-c)# random-detect ecn
```

## Related Commands

| Command | Description |
|---|---|
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# random-detect exponential-weighting-constant

**Note** Effective with Cisco IOS Release 15.0(1)S and Cisco IOS Release 15.1(3)T, the **random-detectexponential-weighting-constant**command is hidden in interface configuration mode. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed from interface configuration mode in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

To configure the Weighted Random Early Detection (WRED) and distributed WRED (DWRED) exponential weight factor for the average queue size calculation for the queue, use the **random-detectexponential-weighting-constant**command in interface configuration mode. To configure the exponential weight factor for the average queue size calculation for the queue reserved for a class, use the **random-detectexponential-weighting-constant**command in policy-map class configuration mode. To return the value to the default, use the **no** form of this command.

**random-detect exponential-weighting-constant** *exponent*

**no random-detect exponential-weighting-constant**

## Syntax Description

| | |
|---|---|
| *exponent* | Exponent from 1 to 16 used in the average queue size calculation. |

## Command Default

The default exponential weight factor is 9.

## Command Modes

Interface configuration when used on an interface Policy-map class configuration when used to specify class policy in a policy map or when used in the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC)

## Command History

| Release | Modification |
|---|---|
| 11.1CC | This command was introduced. |
| 12.0(5)T | This command was made available as a QoS policy-map class configuration command. |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE and implemented on Versatile Interface Processor (VIP) enabled Cisco 7500 series routers. |

| Release | Modification |
|---|---|
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T and implemented on VIP-enabled Cisco 7500 series routers. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.0(1)S | This command was modified. This command was hidden in interface configuration mode. |
| 15.1(3)T | This command was modified. This command was hidden in interface configuration mode. |

## Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. DWRED is similar to WRED but uses the VIP instead of the Route Switch Processor (RSP). WRED and DWRED are most useful with protocols like TCP that respond to dropped packets by decreasing the transmission rate.

Use this command to change the exponent used in the average queue size calculation for the WRED and DWRED services. You can also use this command to configure the exponential weight factor for the average queue size calculation for the queue reserved for a class.

**Note** The default WRED or DWRED parameter values are based on the best available data. We recommend that you do not change the parameters from their default values unless you have determined that your applications would benefit from the changed values.

The DWRED feature is not supported for class policy.

The DWRED feature is supported only on Cisco 7000 series routers with an RSP7000 card and Cisco 7500 series routers with a VIP2-40 or greater interface processor. A VIP2-50 interface processor is strongly recommended when the aggregate line rate of the port adapters on the VIP is greater than DS3. A VIP2-50 interface processor is required for OC-3 rates.

To use DWRED, distributed Cisco Express Forwarding (dCEF) switching must first be enabled on the interface. For more information on dCEF, refer to the Cisco IOS IP Switching Configuration Guide and the Cisco IOS IP Switching Command Reference.

## Examples

The following example configures WRED on an interface with a weight factor of 10:

```
interface Hssi0/0/0
 description 45Mbps to R1
 ip address 10.200.14.250 255.255.255.252
```

```
 random-detect
 random-detect exponential-weighting-constant 10
```

The following example configures the policy map called policy1 to contain policy specification for the class called class1. During times of congestion, WRED packet drop is used instead of tail drop. The weight factor used for the average queue size calculation for the queue for class1 is 12.

```
! The following commands create the class map called class1:
class-map class1
 match input-interface FE0/1
! The following commands define policy1 to contain policy specification for class1:
policy-map policy1
 class class1
 bandwidth 1000
 random-detect
 random-detect exponential-weighting-constant 12
```

The following example configures policy for a traffic class named int10 to configure the exponential weight factor as 12. This is the weight factor used for the average queue size calculation for the queue for traffic class int10. WRED packet drop is used for congestion avoidance for traffic class int10, not tail drop.

```
policy-map policy12
 class int10
 bandwidth 2000
 random-detect exponential-weighting-constant 12
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth (policy-map class)** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map. |
| **exponential-weighting-constant** | Configures the exponential weight factor for the average queue size calculation for a WRED parameter group. |
| **fair-queue (class-default)** | Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy. |
| **precedence** | Configures precedence levels for a VC or PVC class that can be assigned to a VC or PVC bundle and thus applied to all of the members of that bundle. |
| **precedence (WRED group)** | Configures a WRED group for a particular IP Precedence. |
| **random-detect dscp** | Changes the minimum and maximum packet thresholds for the DSCP value. |
| **random-detect (per VC)** | Enables per-VC WRED or per-VC DWRED. |
| **random-detect precedence** | Configures WRED and DWRED parameters for a particular IP Precedence. |

| Command | Description |
|---|---|
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# random-detect flow

**Note** Effective with Cisco IOS Release 15.1(3)T, the **random-detectflow**command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release. For more information, see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

To enable flow-based Weighted Random Early Detection ( WRED), use the **random-detectflow**command in interface configuration mode. To disable flow-based WRED, use the **no** form of this command.

**random-detect flow**

**no random-detect flow**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Flow-based WRED is disabled by default.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(3)T | This command was modified. This command was hidden. |

## Usage Guidelines

You must use this command to enable flow-based WRED before you can use the **random-detectflowaverage-depth-factor** and **random-detectflowcount** commands to further configure the parameters of flow-based WRED.

Before you can enable flow-based WRED, you must enable and configure WRED. For complete information, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide* .

## Examples

The following example enables flow-based WRED on serial interface 1:

```
interface Serial1
 random-detect
 random-detect flow
```

## Related Commands

| Command | Description |
|---|---|
| **random-detect dscp** | Changes the minimum and maximum packet thresholds for the DSCP value. |
| **random-detect exponential-weighting-constant** | Configures the WRED and DWRED exponential weight factor for the average queue size calculation. |
| **random-detect flow average-depth-factor** | Sets the multiplier to be used in determining the average depth factor for a flow when flow-based WRED is enabled. |
| **random-detect flow count** | Sets the flow count for flow-based WRED. |
| **random-detect precedence** | Configures WRED and DWRED parameters for a particular IP Precedence. |
| **show interfaces** | Displays the statistical information specific to a serial interface. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# random-detect flow average-depth-factor

**Note** Effective with Cisco IOS Release 15.1(3)T, the **random-detectflowaverage-depth-factor**command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release. For more information, see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

To set the multiplier to be used in determining the average depth factor for a flow when flow-based Weighted Random Early Detection (WRED) is enabled, use the **random-detectflowaverage-depth-factor**command in interface configuration mode. To remove the current flow average depth factor value, use the **no** form of this command.

**random-detect flow average-depth-factor** *scaling-factor*

**no random-detect flow average-depth-factor** *scaling-factor*

## Syntax Description

| | |
|---|---|
| *scaling-factor* | The scaling factor can be a number from 1 to 16. |

## Command Default

The default average depth factor is 4.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(3)T | This command was modified. This command was hidden. |

## Usage Guidelines

Use this command to specify the scaling factor that flow-based WRED should use in scaling the number of buffers available per flow and in determining the number of packets allowed in the output queue for each active flow. This scaling factor is common to all flows. The outcome of the scaled number of buffers becomes the per-flow limit.

If this command is not used and flow-based WRED is enabled, the average depth scaling factor defaults to 4.

A flow is considered nonadaptive--that is, it takes up too much of the resources--when the average flow depth times the specified multiplier (scaling factor) is less than the depth for the flow, for example:

average-flow-depth * (scaling factor) < flow-depth

Before you use this command, you must use the **random-detectflow** command to enable flow-based WRED for the interface. To configure flow-based WRED, you may also use the **random-detectflowcount** command.

## Examples

The following example enables flow-based WRED on serial interface 1 and sets the scaling factor for the average flow depth to 8:

```
interface Serial1
 random-detect
 random-detect flow
 random-detect flow average-depth-factor 8
```

## Related Commands

| Command | Description |
|---|---|
| **random-detect dscp** | Changes the minimum and maximum packet thresholds for the DSCP value. |
| **random-detect exponential-weighting-constant** | Configures the WRED and DWRED exponential weight factor for the average queue size calculation. |
| **random-detect flow** | Enables flow-based WRED. |
| **random-detect flow count** | Sets the flow count for flow-based WRED. |
| **random-detect precedence** | Configures WRED and DWRED parameters for a particular IP Precedence. |
| **show interfaces** | Displays the statistical information specific to a serial interface. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# random-detect flow count

**Note** Effective with Cisco IOS Release 15.1(3)T, the **random-detectflowcount**command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release. For more information, see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

To set the flow count for flow-based Weighted Random Early Detection (WRED), use the **random-detectflowcount**command in interface configuration mode. To remove the current flow count value, use the **no** form of this command.

**random-detect flow count** *number*

**no random-detect flow count** *number*

## Syntax Description

| | |
|---|---|
| *number* | Specifies a value from 16 to 215 (32768). |

## Command Default

256

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(3)T | This command was modified. This command was hidden. |

## Usage Guidelines

Before you use this command, you must use the **random-detectflow** command to enable flow-based WRED for the interface.

## Examples

The following example enables flow-based WRED on serial interface 1 and sets the flow threshold constant to 16:

```
interface Serial1
 random-detect
 random-detect flow
 random-detect flow count 16
```

## Related Commands

| Command | Description |
|---|---|
| **random-detect dscp** | Changes the minimum and maximum packet thresholds for the DSCP value. |
| **random-detect exponential-weighting-constant** | Configures the WRED and DWRED exponential weight factor for the average queue size calculation. |
| **random-detect flow** | Enables flow-based WRED. |
| **random-detect precedence** | Configures WRED and DWRED parameters for a particular IP Precedence. |
| **show interfaces** | Displays the statistical information specific to a serial interface. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# random-detect prec-based

**Note** Effective with Cisco IOS Release 12.4(20)T, the **random-detectprec-based**command**isreplacedbytherandom-detectprecedence-basedcommand.Seetherandom-dete formoreinformation.**

To base weighted random early detection (WRED) on the precedence value of a packet, use the **random-detectprec-based** command in policy-map class configuration mode. To disable this feature, use the **no** form of this command.

**random-detect prec-based**

**no random-detect prec-based**

## Syntax Description

This command has no arguments or keywords.

## Command Default

WRED is disabled by default.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.0(28)S | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.4(20)T | This command was replaced by the **random-detectprecedence-based** command within a policy map. |

## Usage Guidelines

With the **random-detectprec-based** command, WRED is based on the IP precedence value of the packet.

Use the **random-detectprec-based** command before configuring the **random-detectprecedence** command.

Beginning with Cisco IOS Release 12.4(20)T, use the **random-detectprecedence** command when you configure a policy map.

## Examples

The following example shows that random detect is based on the precedence value of a packet:

```
Router> enable
Router# configure terminal
Router(config)#

policy-map policy1
Router(config-pmap)# class class1
```

```
Router(config-pmap-c)# bandwidth percent 80
Router(config-pmap-c)# random-detect precedence-based
Router(config-pmap-c)# random-detect precedence 2 500 ms 1000 ms
Router(config-pmap-c)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **random-detect** | Enables WRED or DWRED. |
| **random-detect precedence** | Configures the WRED and DWRED parameters for a particular IP precedence; configures WRED parameters for a particular IP precedence for a class policy in a policy map. |

# random-detect precedence

**Note** Effective with Cisco IOS Release 15.0(1)S and Cisco IOS Release 15.1(3)T, the **random-detect precedence** command is hidden in interface configuration mode. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you enter a question mark at the command line. This command will be completely removed from interface configuration mode in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

To configure Weighted Random Early Detection (WRED) and distributed WRED (dWRED) parameters for a particular IP precedence, use the **random-detect precedence** command in interface configuration mode. To configure WRED parameters for a particular IP precedence for a class policy in a policy map, use the **random-detect precedence** command in QoS policy-map class configuration mode. To return the values to the default for the precedence, use the **no** form of this command.

**random-detect precedence** {*precedence*| **rsvp**} *min-threshold max-threshold mark-probability-denominator*

**no random-detect precedence**

## Syntax Description

| | |
|---|---|
| *precedence* | IP precedence number. The value range is from 0 to 7. For Cisco 7000 series routers with an RSP7000 interface processor and Cisco 7500 series routers with a VIP2-40 interface processor (the VIP2-50 interface processor is strongly recommended), the precedence value range is from 0 to 7; see Table 1 in the "Usage Guidelines" section. |
| **rsvp** | Indicates Resource Reservation Protocol (RSVP) traffic. |
| *min-threshold* | Minimum threshold in number of packets. The value range of this argument is from 1 to 512000000. When the average queue length reaches the minimum threshold, WRED or dWRED randomly drop some packets with the specified IP precedence. |
| *max-threshold* | Maximum threshold in number of packets. The value range of this argument is from the value of the *min-threshold* argument to 512000000. When the average queue length exceeds the maximum threshold, WRED or dWRED drop all packets with the specified IP precedence. |

| | |
|---|---|
| *mark-probability-denominator* | Denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. The value range is from 1 to 65536. The default is 10; that is 1 out of every 10 packets is dropped at the maximum threshold. |

## Command Default

For all precedences, the *mark-probability-denominator* default value is 10, and the *max-threshold* value is based on the output buffering capacity and the transmission speed for the interface.

The default *min-threshold* value depends on the precedence. The *min-threshold* value for IP precedence 0 corresponds to half of the *max-threshold* value. The values for the remaining precedences fall between half the *max-threshold* value and the *max-threshold* value at evenly spaced intervals. See the table in the "Usage Guidelines" section of this command for a list of the default minimum threshold values for each IP precedence.

## Command Modes

Interface configuration (config-if)

QoS policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 11.1CC | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)T | Support was added for hierarchical queueing framework (HQF) using the modular quality of service (QoS) CLI (MQC).<br>**Note** This command replaces the **random-detect prec-based** command in QoS policy-map configuration mode. |
| 15.0(1)S | This command was modified. This command was hidden in interface configuration mode. |
| 15.1(3)T | This command was modified. This command was hidden in interface configuration mode. |
| 15.2(2)T | This command was modified. The maximum and minimum threshold ranges were changed. |
| Cisco IOS XE Release 3.6S | This command was modified. Support was added for the Cisco ASR 903 router. |

## Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when congestion exists. dWRED is similar to WRED but uses the Versatile Interface Processor (VIP) instead of the Route Switch Processor (RSP).

When you configure the **random-detect** command on an interface, packets are given preferential treatment based on the IP precedence of the packet. Use the **random-detect precedence** command to adjust the treatment for different precedences.

If you want WRED or dWRED to ignore the precedence when determining which packets to drop, enter this command with the same parameters for each precedence. Remember to use appropriate values for the minimum and maximum thresholds.

Note that if you use the **random-detect precedence** command to adjust the treatment for different precedences within class policy, you must ensure that WRED is not configured for the interface to which you attach that service policy.

**Note** Although the range of values for the *min-threshold* and *max-threshold* arguments is from 1 to 512000000, the actual values that you can specify depend on the type of random detect you are configuring. For example, the maximum threshold value cannot exceed the queue limit.

The table below lists the default minimum threshold value for each IP precedence.

***Table 37: Default WRED and dWRED Minimum Threshold Values***

| | **Minimum Threshold Value (Fraction of Maximum Threshold Value)** | |
|---|---|---|
| IP Precedence | WRED | dWRED |
| 0 | 9/18 | 8/16 |
| 1 | 10/18 | 9/16 |
| 2 | 11/18 | 10/16 |
| 3 | 12/18 | 11/16 |
| 4 | 13/18 | 12/16 |
| 5 | 14/18 | 13/16 |
| 6 | 15/18 | 14/16 |
| 7 | 16/18 | 15/16 |
| rsvp | 17/18 | — |

**Note** The default WRED or dWRED parameter values are based on the best available data. We recommend that you do not change the parameters from their default values unless you have determined that your applications would benefit from the changed values.

The dWRED feature is supported only on Cisco 7000 series routers with an RSP7000 card and Cisco 7500 series routers with a VIP2-40 or higher interface processor. A VIP2-50 interface processor is strongly recommended when the aggregate line rate of the port adapters on the VIP is greater than DS3. A VIP2-50 interface processor is required for OC-3 rates.

To use dWRED, distributed Cisco Express Forwarding (dCEF) switching must first be enabled on the interface. For more information on dCEF, refer to the *Cisco IOS IP Switching Configuration Guide* and the *Cisco IOS IP Switching Command Reference*.

**Note** The dWRED feature is not supported in a class policy.

## Examples

The following example shows the configuration to enable WRED on the interface and to specify parameters for the different IP precedences:

```
interface Hssi0/0/0
 description 45Mbps to R1
 ip address 10.200.14.250 255.255.255.252
 random-detect
 random-detect precedence 0 32 256 100
 random-detect precedence 1 64 256 100
 random-detect precedence 2 96 256 100
 random-detect precedence 3 120 256 100
 random-detect precedence 4 140 256 100
 random-detect precedence 5 170 256 100
 random-detect precedence 6 290 256 100
 random-detect precedence 7 210 256 100
 random-detect precedence rsvp 230 256 100
```

The following example shows the configuration for the policy for a class called acl10 included in a policy map called policy10. Class acl101 has these characteristics: a minimum of 2000 kb/s of bandwidth are expected to be delivered to this class in the event of congestion and a weight factor of 10 is used to calculate the average queue size. For congestion avoidance, WRED packet drop is used, not tail drop. IP precedence is reset for levels 0 through 4.

```
policy-map policy10
class acl10
 bandwidth 2000
 random-detect
 random-detect exponential-weighting-constant 10
 random-detect precedence 0 32 256 100
 random-detect precedence 1 64 256 100
 random-detect precedence 2 96 256 100
 random-detect precedence 3 120 256 100
 random-detect precedence 4 140 256 100
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth (policy-map class)** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map. |

| Command | Description |
|---|---|
| **fair-queue (class-default)** | Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy. |
| **random-detect (per VC)** | Enables per-VC WRED or per-VC dWRED. |
| **random-detect dscp** | Changes the minimum and maximum packet thresholds for the DSCP value. |
| **random-detect exponential-weighting-constant** | Configures the WRED and dWRED exponential weight factor for the average queue size calculation. |
| **random-detect flow count** | Sets the flow count for flow-based WRED. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queuing** | Lists all or selected configured queuing strategies. |

# random-detect precedence (aggregate)

To configure aggregate Weighted Random Early Detection (WRED) parameters for specific IP precedence value(s), use the **random-detectprecedence**(aggregate)command in policy-map class configuration mode. To disable configuration of aggregate WRED precedence values, use the **no** form of this command.

**random-detect precedence** *sub-class-val1* [*sub-class-val2 sub-class-val3* **sub-class-val4**] *min-thresh max-thresh mark-prob*

**no random-detect precedence** *sub-class-val1* [*sub-class-val2 sub-class-val3 sub-class-val4*]

## Syntax Description

| | |
|---|---|
| **s** *ub-class-val 1 sub-class-val 2* **s** *ub-class-val 3* **s** *ub-class-val 4* | IP precedence value to which the following WRED profile parameter specifications are to apply. Up to four subclasses (IP precedence values) can be specified per command line interface (CLI) entry. The value range is from 0 to 7. |
| *min-thresh* | Minimum threshold (in number of packets) for the subclass(es). Valid values are from 1 to 12288. |
| *max-thresh* | Specifies the maximum threshold (in number of packets) for the subclass(es). Valid values are from the minimum threshold argument to 12288. |
| *mark-prob* | Specifies the denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold for the subclass(es). Valid values are from 1 to 255. |
| **Cisco 10000 Series Router** | |
| **s** *ub-class-val 1* [*...*[*subclass-val8*]] | IP precedence value(s) to which the following WRED profile parameter specifications are to apply. A maximum of 8 subclasses (IP precedence values) can be specified per CLI entry. The value range is from 0 to 7. |
| **minimum-thresh** min-thresh | Specifies the minimum number of packets allowed in the queue. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified IP precedence value. Valid minimum threshold values are 1 to 16384. |
| **maximum-thresh** max-thresh | Specifies the maximum number of packets allowed in the queue. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified IP precedence value. Valid maximum threshold values are 1 to 16384. |

| | |
|---|---|
| **mark-probability** mark-prob | Specifies the denominator for the fraction of packets dropped when the average queue depth is at the maximum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the maximum threshold. Valid values are 1 to 65535. |

## Command Default

For all precedence levels, the mark-prob default is 10 packets.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(17)SL | This command was introduced on the Cisco 10000 series router. |
| 12.2(18)SXE | This command was introduced. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router for the PRE3. |

## Usage Guidelines

For ATM interfaces, the Aggregate WRED feature requires that the ATM SPA cards are installed in a Cisco 7600 SIP-200 carrier card or a Cisco 7600 SIP-400 carrier card.

To configure WRED on an ATM interface, you must use the random-detect aggregate commands; the standard random-detect commands are no longer supported on ATM interfaces

Use this command with a **random-detectaggregate** command within a policy map configuration.

Repeat this command for each set of IP precedence values that share WRED parameters.

After the policy map is defined, the policy map must be attached at the VC level.

The set of subclass (IP precedence) values defined on a **random-detectprecedence**(aggregate)CLI will be aggregated into a single hardware WRED resource. The statistics for these subclasses will also be aggregated.

Use the **showpolicy-mapinterface** command to display the statistics for aggregated subclasses.

**Cisco 10000 Series Router**

The table below lists the default drop thresholds for WRED based on DSCP, IP precedence, and discard-class. The drop probability indicates that the router drops one packet for every 10 packets.

*Table 38: WRED Default Drop Thresholds*

| DSCP, Precedence, and Discard-Class Values | Minimum Threshold (times the queue size) | Maximum Threshold (times the queue size) | Drop Probability |
|---|---|---|---|
| All DSCPs | 1/4 | 1/2 | 1/10 |
| 0 | 1/4 | 1/2 | 1/10 |
| 1 | 9/32 | 1/2 | 1/10 |
| 2 | 5/16 | 1/2 | 1/10 |
| 3 | 11/32 | 1/2 | 1/10 |
| 4 | 3/8 | 1/2 | 1/10 |
| 5 | 13/32 | 1/2 | 1/10 |
| 6 | 7/16 | 1/2 | 1/10 |
| 7 | 15/32 | 1/2 | 1/10 |

For the PRE2, the random-detect command specifies the default profile for the queue. For the PRE3, the aggregate random-detect command is used instead to configure aggregate parameters for WRED. The PRE3 accepts the PRE2 random-detect command as a hidden CLI.

On the PRE2, accounting for the default profile is per precedence. On the PRE3, accounting and configuration for the default profile is per class map.

On the PRE2, the default threshold is per precedence for a DSCP or precedence value without an explicit threshold configuration. On the PRE3, the default threshold is to have no WRED configured.

On the PRE2, the drop counter for each precedence belonging to the default profile only has a drop count that matches the specific precedence value. Because the PRE2 has a default threshold for the default profile, the CBQOSMIB displays default threshold values. On the PRE3, the drop counter for each precedence belonging to the default profile has the aggregate counter of the default profile and not the individual counter for a specific precedence. The default profile on the PRE3 does not display any default threshold values in the CBQOSMIB if you do not configure any threshold values for the default profile.

## Examples

## Examples

The following example shows how to enable IP precedence-based WRED on the Cisco 10000 series router. In this example, the configuration of the class map named Class1 indicates to classify traffic based on IP precedence 3, 4, and 5. Traffic that matches IP precedence 3, 4, or 5 is assigned to the class named Class1 in the policy map named Policy1. WRED-based packet dropping is configured for Class1 and is based on IP precedence 3 with a minimum threshold of 500, maximum threshold of 1500, and a mark-probability-denominator of 200. The QoS policy is applied to PVC 1/32 on the point-to-point ATM subinterface 1/0/0.1.

```
Router(config)# class-map Class1
```

```
Router(config-cmap)# match ip precedence 3 4 5
Router(config-cmap)# exit
Router(config)# policy-map Policy1
Router(config-pmap)# class Class1
Router(config-pmap-c)# bandwidth 1000
Router(config-pmap-c)# random-detect prec-based
Router(config-pmap-c)# random-detect precedence 3 500 1500 200
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface atm 1/0/0
Router(config-if)# atm pxf queuing
Router(config-if)# interface atm 1/0/0.1 point-to-point
Router(config-subif)# pvc 1/32
Router(config-subif-atm-vc)# ubr 10000
Router(config-subif-atm-vc)# service-policy output policy1
```

## Related Commands

| Command | Description |
|---|---|
| **class (policy-map)** | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy. |
| **interface** | Configures an interface type and enters interface configuration mode. |
| **policy-map** | Creates a policy map that can be attached to one or more interfaces to specify a service policy. |
| **random-detect aggregate** | Enables aggregate WRED and optionally specifies default WRED parameter values for a default aggregate class. This default class will be used for all subclasses that have not been explicitly configured. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

# random-detect-group

**Note** Effective with Cisco IOS Release 15.0(1)S and Cisco IOS Release 15.1(3)T, the **random-detect-group**command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release. For more information, see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

To define the Weighted Random Early Detection (WRED) or distributed WRED (DWRED) parameter group, use the **random-detect-group**command in global configuration mode. To delete the WRED or DWRED parameter group, use the **no** form of this command.

**random-detect-group** *group-name* [**dscp-based**| **prec-based**]

**no random-detect-group** *group-name* [**dscp-based**| **prec-based**]

## Syntax Description

| | |
|---|---|
| *group-name* | Name for the WRED or DWRED parameter group. |
| **dscp-based** | (Optional) Specifies that WRED is to use the differentiated services code point (DSCP) value when it calculates the drop probability for a packet. |
| **prec-based** | (Optional) Specifies that WRED is to use the IP Precedence value when it calculates the drop probability for a packet. |

## Command Default

No WRED or DWRED parameter group exists.

If you choose not to use either the **dscp-based** or the **prec-based** keywords, WRED uses the IP Precedence value (the default method) to calculate drop probability for the packet.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 11.1(22)CC | This command was introduced. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. Keywords **dscp-based** and **prec-based** were added to support Differentiated Services (DiffServ) and Assured Forwarding (AF) Per Hop Behavior (PHB). |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

| Release | Modification |
|---|---|
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.0(1)S | This command was modified. This command was hidden. |
| 15.1(3)T | This command was modified. This command was hidden. |

## Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when there is congestion. DWRED is similar to WRED but uses the Versatile Interface Processor (VIP) instead of the Route Switch Processor (RSP). WRED and DWRED are most useful when the traffic uses protocols such as TCP that respond to dropped packets by decreasing the transmission rate.

The router automatically determines parameters to use in the WRED calculations. If you want to change these parameters for a group, use the **exponential-weighting-constant**or **precedence** command.

**Two Methods for Calculating the Drop Probability of a Packet**

This command includes two optional arguments, **dscp-based** and **prec-based**, that determine the method WRED uses to calculate the drop probability of a packet.

Note the following points when deciding which method to instruct WRED to use:

- With the **dscp-based**keyword, WRED uses the DSCP value (that is, the first six bits of the IP type of service (ToS) byte) to calculate the drop probability.
- With the **prec-based** keyword, WRED will use the IP Precedence value to calculate the drop probability.
- The **dscp-based** and **prec-based** keywords are mutually exclusive.
- If neither argument is specified, WRED uses the IP Precedence value to calculate the drop probability (the default method).

## Examples

The following example defines the WRED parameter group called sanjose:

```
random-detect-group sanjose
 precedence 0 32 256 100
 precedence 1 64 256 100
 precedence 2 96 256 100
 precedence 3 128 256 100
 precedence 4 160 256 100
 precedence 5 192 256 100
 precedence 6 224 256 100
 precedence 7 256 256 100
```

The following example enables WRED to use the DSCP value 9. The minimum threshold for the DSCP value 9 is 20 and the maximum threshold is 50. This configuration can be attached to other virtual circuits (VCs) as required.

```
Router(config)# random-detect-group sanjose dscp-based
Router(cfg-red-grp)# dscp 9 20 50
Router(config-subif-vc)# random-detect attach sanjose
```

## Related Commands

| Command | Description |
|---|---|
| **dscp** | Changes the minimum and maximum packet thresholds for the DSCP value. |
| **exponential-weighting-constant** | Configures the exponential weight factor for the average queue size calculation for a WRED parameter group. |
| **precedence (WRED group)** | Configures a WRED group for a particular IP Precedence. |
| **random-detect (per VC)** | Enables per-VC WRED or per-VC VIP-distributed WRED. |
| **show queueing** | Lists all or selected configured queueing strategies. |
| **show queueing interface** | Displays the queueing statistics of an interface or VC. |

# rate-limit

To configure committed access rate (CAR) and distributed committed access rate (DCAR) policies, use the **rate-limit** command in interface configuration mode. To remove the rate limit from the configuration, use the **no** form of this command.

**rate-limit** {**input**| [**output** *acl-index* | **[rate-limit]** *rate-limit-acl-index* |**dscp***dscp-value* **qos-group** *qos-group-number*]}*burst-normal burst-max* **conform-action***conform-action* **exceed-action***exceed-action*

**no rate-limit** {**input**| [**output** *acl-index* | **[rate-limit]** *rate-limit-acl-index* |**dscp***dscp-value* **qos-group** *qos-group-number*]}*burst-normal burst-max* **conform-action***conform-action* **exceed-action***exceed-action*

## Syntax Description

| | |
|---|---|
| **input** | Applies this CAR traffic policy to packets received on this input interface. |
| **output** | Applies this CAR traffic policy to packets sent on this output interface. |
| *bps* | Average rate, in bits per second (bps). The value must be in increments of 8 kbps. The value is a number from 8000 to 2000000000. |
| **access-group** | (Optional) Applies this CAR traffic policy to the specified access list. |
| *acl-index* | (Optional) Access list number. Values are numbers from 1 to 2699. |
| **rate-limit** | (Optional) The access list is a rate-limit access list. |
| *rate-limit-acl-index* | (Optional) Rate-limit access list number. Values are numbers from 0 to 99. |
| **dscp** | (Optional) Allows the rate limit to be applied to any packet matching a specified differentiated services code point (DSCP). |
| *dscp-value* | (Optional) The DSCP number. Values are numbers from 0 to 63. |
| **qos-group** | (Optional) Allows the rate limit to be applied to any packet matching a specified qos-group number. Values are numbers from 0 to 99. |
| *qos-group-number* | (Optional) The qos-group number. Values are numbers from 0 to 99. |

| | |
|---|---|
| *burst-normal* | Normal burst size, in bytes. The minimum value is bps divided by 2000. The value is a number from 1000 to 512000,000. |
| *burst-max* | Excess burst size, in bytes. The value is a number from 2000 to 1024000000. |
| **conform-action** *conform-action* | Action to take on packets that conform to the specified rate limit. Specify one of the following keywords:<br>• **continue** --Evaluate the next **rate-limit** command.<br>• **drop** --Drop the packet.<br>• **set-dscp-continue** --Set the differentiated services codepoint (DSCP) (0 to 63) and evaluate the next **rate-limit** command.<br>• **set-dscp-transmit** --Transmit the DSCP and transmit the packet.<br>• **set-mpls-exp-imposition-continue** --Set the Multiprotocol Label Switching (MPLS) experimental bits (0 to 7) during imposition and evaluate the next **rate-limit** command.<br>• **set-mpls-exp-imposition-transmit** --Set the MPLS experimental bits (0 to 7) during imposition and transmit the packet.<br>• **set-prec-continue** --Set the IP precedence (0 to 7) and evaluate the next **rate-limit** command.<br>• **set-prec-transmit** --Set the IP precedence (0 to 7) and transmit the packet.<br>• **set-qos-continue** --Set the quality of service (QoS) group ID (1 to 99) and evaluate the next **rate-limit** command.<br>• **set-qos-transmit** --Set the QoS group ID (1 to 99) and transmit the packet.<br>• **transmit** --Transmit the packet. |

| | |
|---|---|
| **exceed-action** *exceed-action* | Action to take on packets that exceed the specified rate limit. Specify one of the following keywords:<br>• **continue** --Evaluate the next **rate-limit** command.<br>• **drop** --Drop the packet.<br>• **set-dscp-continue** --Set the DSCP (0 to 63) and evaluate the next **rate-limit** command.<br>• **set-dscp-transmit** --Transmit the DSCP and transmit the packet.<br>• **set-mpls-exp-imposition-continue** --Set the MPLS experimental bits (0 to 7) during imposition and evaluate the next **rate-limit** command.<br>• **set-mpls-exp-imposition-transmit** --Set the MPLS experimental bits (0 to 7) during imposition and transmit the packet.<br>• **set-prec-continue** --Set the IP precedence (0 to 7) and evaluate the next **rate-limit** command.<br>• **set-prec-transmit** --Set the IP precedence (0 to 7) and transmit the packet.<br>• **set-qos-continue** --Set the QoS group ID (1 to 99) and evaluate the next **rate-limit** command.<br>• **set-qos-transmit** --Set the QoS group ID (1 to 99) and transmit the packet.<br>• **transmit** --Transmit the packet. |

**Command Default**

CAR and DCAR are disabled.

**Command Modes**

Interface configuration

**Command History**

| Release | Modification |
|---|---|
| 11.1 CC | This command was introduced. |
| 12.1(5)T | The **conform** and **exceed** keywords for the MPLS experimental field were added. |
| 12.2(4)T | This command was implemented on the Cisco MGX 8850 switch and the MGX 8950 switch with a Cisco MGX RPM-PR card. |

| Release | Modification |
|---|---|
| 12.2(4)T2 | This command was implemented on the Cisco 7500 series routers. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use this command to configure your CAR policy on an interface. To specify multiple policies, enter this command once for each policy.

CAR and DCAR can be configured on an interface or subinterface.

**Policing Traffic with CAR**

CAR embodies a rate-limiting feature for policing traffic. When policing traffic with CAR, Cisco recommends the following values for the normal and extended burst parameters:

normal burst (in bytes) = configured rate (in bits per second) * (1 byte)/(8 bits) * 1.5 seconds

17.000.000 * (1 byte)/(8 bits) * 1.5 seconds = 3.187.500 bytes

extended burst = 2 * normal burst

2 * 3.187.500 = 6.375.000 bytes

With the listed choices for parameters, extensive test results have shown CAR to achieve the configured rate. If the burst values are too low, then the achieved rate is often much lower than the configured rate.

For more information about using CAR to police traffic, see the “Policing with CAR” section of the “Policing and Shaping Overview” in the *Cisco IOS Quality of Service Solutions Configuration Guide* .

## Examples

In the following example, the recommended burst parameters for CAR are used:

```
Router(config)# interface serial6/1/0
Router(config-if)#
rate-limitinputaccess-group11700000031875006375000conform-actiontransmitexceed-actiondrop
```

In the following example, the rate is limited by the application in question:

- All World Wide Web traffic is transmitted. However, the MPLS experimental field for web traffic that conforms to the first rate policy is set to 5. For nonconforming traffic, the IP precedence is set to 0 (best effort). See the following commands in the example:

```
rate-limit input rate-limit access-group 101 20000000 24000 32000 conform-action
set-mpls-exp-transmit 5 exceed-action set-mpls-exp-transmit 0
access-list 101 permit tcp any any eq www
```

- FTP traffic is transmitted with an MPLS experimental field value of 5 if it conforms to the second rate policy. If the FTP traffic exceeds the rate policy, it is dropped. See the following commands in the example:

```
rate-limit input access-group 102 10000000 24000 32000
```

```
conform-action set-mpls-exp-transmit 5 exceed-action drop
access-list 102 permit tcp any any eq ftp
```

- Any remaining traffic is limited to 8 Mbps, with a normal burst size of 1,500,000 bytes and an excess burst size of 3,000,000 bytes. Traffic that conforms is sent with an MPLS experimental field of 5. Traffic that does not conform is dropped. See the following command in the example:

```
rate-limit input 8000000 1500000 3000000 conform-action set-mpls-exp-transmit 5
exceed-action drop
```

Notice that two access lists are created to classify the web and FTP traffic so that they can be handled separately by the CAR feature.

```
Router(config)# interface Hssi0/0/0
Router(config-if)# description 45Mbps to R2
Router(config-if)# rate-limit input rate-limit access-group 101 20000000 3750000 7500000
conform-action set-mpls-exp-transmit 5 exceed-action set-mpls-exp-transmit 0
Router(config-if)# rate-limit input access-group 102 10000000 1875000 3750000
conform-action set-mpls-exp-transmit 5 exceed-action drop
Router(config-if)# rate-limit input 8000000 1500000 3000000 conform-action
set-mpls-exp-transmit 5 exceed-action drop
Router(config-if)# ip address 10.1.1.1 255.255.255.252
!
Router(config-if)# access-list 101 permit tcp any any eq www
Router(config-if)# access-list 102 permit tcp any any eq ftp
```

In the following example, the MPLS experimental field is set, and the packet is transmitted:

```
Router(config)# interface FastEthernet1/1/0
Router(config-if)# rate-limit input 8000 1500 3000 access-group conform-action
set mpls-exp-transmit 5 exceed-action set-mpls-exp-transmit 5
```

In the following example, any packet with a DSCP of 1 can apply the rate limit:

```
Router(config)# interface serial6/1/0
Router(config-if)# rate-limit output dscp 1 8000 1500 3000 conform-action transmit
exceed-action drop
```

## Related Commands

| Command | Description |
|---|---|
| **access-list rate-limit** | Configures an access list for use with CAR policies. |
| **show access-lists rate-limit** | Displays information about rate-limit access lists. |
| **show interfaces rate-limit** | Displays information about CAR for a specified interface. |

# rcv-queue bandwidth

To define the bandwidths for ingress (receive) WRR queues through scheduling weights in interface configuration command mode, use the **rcv-queuebandwidth**command. To return to the default settings, use the **no** form of this command.

**rcv-queue bandwidth** *weight-1 ... weight-n*

**no rcv-queue bandwidth**

## Syntax Description

| | |
|---|---|
| *weight-1 ... weight-n* | WRR weights; valid values are fr om 0 to 255. |

## Command Default

The defaults are as follows:

- QoS enabled--4:255
- QoS disabled--255:1

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(17a)SX | This command was introduced on the Supervisor Engine 720. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(50)SY | Support for this command was introduced. |

## Usage Guidelin

**Note** In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

This command is not supported on Cisco 7600 series router that are configured with a Supervisor Engine 2.

This command is supported on 2q8t and 8q8t ports only.

You can configure up to seven queue weights.

## Examples

This example shows how to allocate a three-to-one bandwidth ratio:

```
Router(config-if)# rcv-queue bandwidth 3 1
```

```
Router(config-if)#
```

## Related Commands

| Command | Description |
|---|---|
| **rcv-queue queue-limit** | Sets the size ratio between the strict-priority and standard receive queues. |
| **show queueing interface** | Displays queueing information. |

# rcv-queue cos-map

To map the class of service (CoS) values to the standard receive-queue drop thresholds, use the **rcv-queuecos-map** command in interface configuration mode. To remove the mapping, use the **no** form of this command.

**rcv-queue cos-map** *queue-id threshold-id cos-1 cos-n*

**no rcv-queue cos-map** *queue-id threshold-id*

## Syntax Description

| | |
|---|---|
| *queue-id* | Queue ID; the valid value is 1 . |
| *threshold-id* | Threshold ID; valid values are from 1 to 4. |
| *cos-1 ... cos-n* | CoS values; valid values are from 0 to 7. |

## Command Default

The defaults are listed in the table below.

***Table 39: CoS-to-Standard Receive Queue Map Defaults***

| queue | threshold | cos-map | queue | threshold | cos-map |
|---|---|---|---|---|---|
| With QoS Disabled | With QoS Enabled | | | | |
| 1 | 1 | 0,1, 2,3,4,5,6,7 | 1 | 1 | 0,1 |
| 1 | 2 | | 1 | 2 | 2,3 |
| 1 | 3 | | 1 | 3 | 4 |
| 1 | 4 | | 1 | 4 | 6,7 |
| 2 | 1 | 5 | 2 | 1 | 5 |

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(50)SY | Support for this command was introduced. |

## Usage Guidelin

**Note** In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

The *cos-n value* is defined by the module and port type. When you enter the cos-n value, note that the higher values indicate higher priorities.

Use this command on trusted ports only.

## Examples

This example shows how to map the CoS values 0 and 1 to threshold 1 in the standard receive queue:

```
Router (config-if)# rcv-queue cos-map 1 1 0 1
  cos-map configured on:  Gi1/1 Gi1/2
```

## Related Commands

| Command | Description |
|---|---|
| **show queueing interface** | Displays queueing information. |

# rcv-queue queue-limit

To set the size ratio between the strict-priority and standard receive queues, use the **rcv-queuequeue-limit** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

**rcv-queue queue-limit** *q-limit-1 q-limit-2*

**no rcv-queue queue-limit**

## Syntax Description

| | |
|---|---|
| *q-limit-1* | Standard queue weight; valid values are from 1 and 100 pe rcent. |
| *q-limit-2* | Strict-priority queue weight; see the “Usage Guidelines” section for valid values. |

## Command Default

The defaults are as follows:

- 80 percent is for low priority.
- 20 percent is for strict priority.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(50)SY | Support for this command was introduced. |

## Usage Guidelin

**Note** In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

Valid strict-priority weight values are fro m 1 to 100 percent, excep t on 1p1q8t ingress LAN ports, where valid values for the strict-priority queue are from 3 to 100 perce nt.

The **rcv-queuequeue-limit** command configures ports on a per-ASIC basis.

Estimate the mix of strict-priority-to-standard traffic on your network (for example, 80-percent standard traffic and 20-percent strict-priority traffic) and use the estimated percentages as queue weights.

## Examples

This example shows how to set the receive-queue size ratio for Gigabit Ethernet interface 1/2:

```
Router# configure terminal
Router(config)# interface gigabitethernet 1/2
Router(config-if)# rcv-queue queue-limit 75 15

Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **show queueuing interface** | Displays queueing information. |

# rcv-queue random-detect

To specify the minimum and maximum threshold for the specified receive queues, use the **rcv-queuerandom-detect** command in interface configuration mode. To return to the det fault settings, use the **no** form of this command.

**rcv-queue random-detect** {**max-threshold**| **min-threshold**} *queue-id threshold-percent-1 threshold-percent-n*

**no rcv-queue random-detect** {**max-threshold**| **min-threshold**} *queue-id*

## Syntax Description

| | |
|---|---|
| **max-threshold** | Specifies the maximum threshold. |
| **min-threshold** | Specifies the minimum threshold. |
| *queue-id* | Queue ID; the valid value is 1 . |
| *threshold-percent-1 threshold-percent-n* | Threshold weights; valid values are from 1 to 100 percent. |

## Command Default

The defaults are as follows:

- min-threshold -- 80 percent
- max-threshold -- 20 percent

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(17a)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(50)SY | Support for this command was introduced. |

## Usage Guidelines

**Note** In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

This command is supported on 1p1q8t and 8q8t ports only.

The 1p1q8t interface indicates one strict queue and one standard queue with eight thresholds. The 8q8t interface indicates eight standard queues with eight thresholds. The threshold in the strict-priority queue is not configurable.

Each threshold has a low- and a high-threshold value. The threshold values are a percentage of the receive-queue capacity.

For additional information on configuring receive-queue thresholds, refer to the "QoS" chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*.

## Examples

This example shows how to configure the low-priority receive-queue thresholds:

```
Router (config-if)# rcv-queue random-detect max-threshold 1 60 100
```

## Related Commands

| Command | Description |
|---|---|
| **show queueing interface** | Displays queueing information. |

# rcv-queue threshold

To configure the drop-threshold percentages for the standard receive queues on 1p1q4t and 1p1q0t interfaces, use the **rcv-queuethreshold** command in interface configuration mode. To return the thresholds to the default settings, use the **no** form of this command.

**rcv-queue threshold** *queue-id threshold-percent-1 threshold-percent-n*

**no rcv-queue threshold**

## Syntax Description

| | |
|---|---|
| *queue-id* | Queue ID; the valid value is 1. |
| *threshold- percent-1 ... threshold- percent-n* | Threshold ID; valid values are from 1 to 100 percent . |

## Command Default

The defaults for the 1p1q4t and 1p1q0t configurations are as follows:

- Quality of service (QoS) assigns all traffic with class of service (CoS) 5 to the strict-priority queue.
- QoS assigns all other traffic to the standard queue.

The default for the 1q4t configuration is that QoS assigns all traffic to the standard queue.

If you enable QoS, the following default thresholds apply:

- 1p1q4t interfaces have this default drop-threshold configuration:
  - Frames with CoS 0, 1, 2, 3, 4, 6, or 7 go to the standard receive queue.
  - Using standard receive-queue drop threshold 1, the Cisco 7600 series router drops incoming frames with CoS 0 or 1 when the receive-queue buffer is 50 percent or more full.
  - Using standard receive-queue drop threshold 2, the Cisco 7600 series router drops incoming frames with CoS 2 or 3 when the receive-queue buffer is 60 percent or more full.
  - Using standard receive-queue drop threshold 3, the Cisco 7600 series router drops incoming frames with CoS 4 when the receive-queue buffer is 80 percent or more full.
  - Using standard receive-queue drop threshold 4, the Cisco 7600 series router drops incoming frames with CoS 6 or 7 when the receive-queue buffer is 100 percent full.
  - Frames with CoS 5 go to the strict-priority receive queue (queue 2), where the Cisco 7600 series router drops incoming frames only when the strict-priority receive-queue buffer is 100 percent full.
- 1p1q0t interfaces have this default drop-threshold configuration:
  - Frames with CoS 0, 1, 2, 3, 4, 6, or 7 go to the standard receive queue. The Cisco 7600 series router drops incoming frames when the receive-queue buffer is 100 percent full.

- Frames with CoS 5 go to the strict-priority receive queue (queue 2), where the Cisco 7600 series router drops incoming frames only when the strict-priority receive-queue buffer is 100 percent full.

**Note** The 100-percent threshold may be actually changed by the module to 98 percent to allow Bridge Protocol Data Unite (BPDU) traffic to proceed. The BPDU threshold is factory set at 100 percent.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(50)SY | Support for this command was introduced. |

## Usage Guidelines

**Note** In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

The *queue-id* value is always 1.

A value of 10 indicates a threshold when the buffer is 10 percent full.

Always set threshold 4 to 100 percent.

Receive thresholds take effect only on ports whose trust state is trust cos.

Configure the 1q4t receive-queue tail-drop threshold percentages with the **wrr-queuethreshold**command.

## Examples

This example shows how to configure the receive-queue drop thresholds for Gigabit Ethernet interface 1/1:

```
Router(config-if)# rcv-queue threshold 1 60 75 85 100
```

## Related Commands

| Command | Description |
|---|---|
| **show queueing interface** | Displays queueing information. |

| Command | Description |
|---|---|
| **wrr-queue threshold** | Configures the drop-threshold percentages for the standard receive and transmit queues on 1q4t and 2q2t interfaces. |

# recoverable-loss

To enable Enhanced Compressed Real-Time Transport Protocol (ECRTP), use the **recoverable-loss** command in IPHC-profile configuration mode. To disable ECRTP, use the **no** form of this command.

**recoverable-loss** {**dynamic**| *packet-drops*}

**no recoverable-loss**

## Syntax Description

| | |
|---|---|
| **dynamic** | Indicates that the dynamic recoverable loss calculation is used. |
| *packet-drops* | Maximum number of consecutive packet drops. Range is from 1 to 8. |

## Command Default

ECRTP is disabled.

## Command Modes

IPHC-profile configuration (config-iphcp)

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |
| 12.4(11)T | Support was added for Frame Relay encapsulation. |

## Usage Guidelines

The **recoverable-loss** command is part of the ECRTP feature.

**ECRPT Functionality**

ECRTP reduces corruption by managing the way the compressor updates the context information at the decompressor. The compressor sends updated context information periodically to keep the compressor and decompressor synchronized. By repeating the updates, the probability of context corruption because of packet loss is minimized.

The synchronization of context information between the compressor and the decompressor can be performed dynamically (by specifying the **dynamic** keyword) or whenever a specific number of packets are dropped (by using the *packet-drops*argument).

The number of packet drops represents the quality of the link between the hosts. The lower the number of packet drops, the higher the quality of the link between the hosts.

The packet drops value is maintained independently for each context and does not have to be the same for all contexts.

**Note** If you specify the number of packet drops with the *packet-drops* argument, the **recoverable-loss**command automatically enables ECRTP.

**Intended for Use with IPHC Profiles**

The **recoverable-loss**command is intended for use as part of an IP Header Compression (IPHC) profile. An IPHC profile is used to enable and configure header compression on a network. For more information about using IPHC profiles to configure header compression, see the "Header Compression" module and the "Configuring Header Compression Using IPHC Profiles" module of the *Cisco IOS Quality of Service Solutions Configuration Guide* , Release 12.4T.

## Examples

The following example shows how to configure an IPHC profile called profile2. In this example, ECRTP is enabled with a maximum number of five consecutive packet drops.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# recoverable-loss 5
Router(config-iphcp)# end
```

## Related Commands

| Command | Description |
|---|---|
| **iphc-profile** | Creates an IPHC profile. |

# redirect interface

To configure a traffic class to redirect packets belonging to a specific class to the interface that is specified in the command, use the redirect interface command in policy-map class configuration mode. To prevent the packets from getting redirected, use the no form of this command

**redirect interface** *interface* **type number**

**no redirect interface interface type number**

## Syntax Description

| | |
|---|---|
| *interface type number* | The type and number of the interface to which the packets need to be redirected. |

## Command Default

If this command is not specified, the packets are not redirected to an interface

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.2(18)ZYA1 | This command was introduced. |

## Usage Guidelines

Use this command to redirect packets to a predefined interface. You can also configure the redirect interface command with the log command but not with a drop or copy interface command. This command cannot be configured with a service policy for a stack class. The packets can be redirected only to the following interfaces:

- Ethernet
- Fast Ethernet
- Gigabit Ethernet
- Ten Gigabit Ethernet

## Examples

In the following example, a traffic class called cmtest has been created and configured for use in a policy map called pmtest. The policy map (service policy) is attached to Fast Ethernet interface 4/15. All packets in the cmtest are redirected to FastEthernet interface 4/18.

```
Router(config)# policy-map type access-control pmtest
Router(config-pmap)# class cmtest
Router(config-pmap-c)# redirect interface FastEthernet 4/18
Router(config-pmap-c)# log
Router(config-pmap-c)# exit
Router(config)# interface FastEthernet 4/18
Router(config-if)# service-policy input pmtest
```

## Related Commands

| Command | Description |
|---|---|
| **log** | Generates a log of messages in the policy-map class configuration mode or class-map configuration mode. |
| **show class-map** | Displays all class maps and their matching criteria. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# refresh max-period

To set the number of packets sent between full-header refresh occurrences, use the **refreshmax-period**command in IPHC-profile configuration mode. To use the default number of packets, use the **no** form of this command.

**refresh max-period** {*number-of-packets*| **infinite**}

**no refresh max-period**

## Syntax Description

| | |
|---|---|
| *number-of-packets* | Number of packets sent between full-header refresh occurrences. Range is from 0 to 65535. Default is 256. |
| **infinite** | Indicates no limitation on the number of packets sent between full-header refresh occurrences. |

## Command Default

The number of packets sent between full-header refresh occurrences is 256.

## Command Modes

IPHC-profile configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

Use the **refreshmax-period** command to set the number of non-TCP packets sent between full-header refresh occurrences. The **refreshmax-period** command also allows you to specify no limitation on the number of packets sent between full-header refresh occurrences. To specify no limitation on the number of packets sent, use the **infinite** keyword.

**Prerequisite**

Before you use the **refreshmax-period**command, you must enable non-TCP header compression by using the**non-tcp** command.

**Intended for Use with IPHC Profiles**

The **refreshmax-period**command is intended for use as part of an IPHC profile. An IPHC profile is used to enable and configure header compression on your network. For more information about using IPHC profiles to configure header compression, see the "Header Compression" module and the "Configuring Header Compression Using IPHC Profiles" module of the *Cisco IOS Quality of Service Solutions Configuration Guide* , Release 12.4T.

## Examples

The following is an example of an IPHC profile called profile2. In this example, the number of packets sent before a full-header refresh occurrence is 700 packets.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp
Router(config-iphcp)# refresh max-period 700
Router(config-iphcp)# end
```

## Related Commands

| Command | Description |
|---|---|
| **iphc-profile** | Creates an IPHC profile. |
| **non-tcp** | Enables non-TCP header compression within an IPHC profile. |

# refresh max-time

To set the amount of time to wait before a full-header refresh occurrence, use the **refreshmax-time**command in IPHC-profile configuration mode. To use the default time, use the **no** form of this command.

**refresh max-time** {*seconds*| **infinite**}

**no refresh max-time**

## Syntax Description

| | |
|---|---|
| *seconds* | Length of time, in seconds, to wait before a full-header refresh occurrence. Range is from 0 to 65535. Default is 5. |
| **infinite** | Indicates no limitation on the time between full-header refreshes. |

## Command Default

The amount of time to wait before a full-header refresh occurrence is set to 5 seconds.

## Command Modes

IPHC-profile configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

Use the **refreshmax-time**command to set the maximum amount of time to wait before a full-header refresh occurs. The **refreshmax-time** command also allows you to indicate no limitation on the time between full-header refresh occurrences. To specify no limitation on the time between full-header refresh occurrences, use the **infinite** keyword.

**Prerequisite**

Before you use the **refreshmax-time** command, you must enable non-TCP header compression by using the **non-tcp** command.

**Intended for Use with IPHC Profiles**

The **refreshmax-time**command is intended for use as part of an IPHC profile. An IPHC profile is used to enable and configure header compression on your network. For more information about using IPHC profiles to configure header compression, see the "Header Compression" module and the "Configuring Header Compression Using IPHC Profiles" module of the *Cisco IOS Quality of Service Solutions Configuration Guide* , Release 12.4T.

## Examples

The following is an example of an IPHC profile called profile2. In this example, the maximum amount of time to wait before a full-header refresh occurs is 500 seconds.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# non-tcp
Router(config-iphcp)# refresh max-time 500
Router(config-iphcp)# end
```

## Related Commands

| Command | Description |
|---|---|
| **iphc-profile** | Creates an IPHC profile. |
| **non-tcp** | Enables non-TCP header compression within an IPHC profile. |

# refresh rtp

To enable a context refresh occurrence for Real-Time Transport Protocol (RTP) header compression, use the **refreshrtp** command in IPHC-profile configuration mode. To disable a context refresh occurrence for RTP header compression, use the **no** form of this command.

**refresh rtp**

**no refresh rtp**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Context refresh occurrences for RTP header compression are disabled.

## Command Modes

IPHC-profile configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

Use the **refreshrtp** command to enable a context refresh occurrence for RTP header compression. A context is the state that the compressor uses to compress a header and that the decompressor uses to decompress a header. The context is the uncompressed version of the last header sent and includes information used to compress and decompress the packet.

**Prerequisite**

Before you use the **refreshrtp**command, you must enable RTP header compression by using the **rtp**command.

**Intended for Use with IPHC Profiles**

The **refreshrtp**command is intended for use as part of an IP header compression (IPHC) profile. An IPHC profile is used to enable and configure header compression on your network. For more information about using IPHC profiles to configure header compression, see the "Header Compression" module and the "Configuring Header Compression Using IPHC Profiles" module of the *Cisco IOS Quality of Service Solutions Configuration Guide* , Release 12.4T.

## Examples

The following is an example of an IPHC profile called profile2. In this example, the **refreshrtp** command is used to enable a context refresh occurrence for RTP header compression.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# rtp
Router(config-iphcp)# refresh rtp
Router(config-iphcp)# end
```

## Related Commands

| Command | Description |
|---|---|
| **iphc-profile** | Creates an IPHC profile. |
| **rtp** | Enables RTP header compression within an IPHC profile. |

# rtp

To enable Real-Time Transport Protocol (RTP) header compression within an IP Header Compression (IPHC) profile, use the **rtp** command in IPHC-profile configuration mode. To disable RTP header compression within an IPHC profile, use the **no** form of this command.

**rtp**

**no rtp**

## Syntax Description

This command has no arguments or keywords.

## Command Default

RTP header compression is enabled.

## Command Modes

IPHC-profile configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

The **rtp** command enables RTP header compression and automatically enables non-TCP header compression (the equivalent of using the **non-tcp** command).

### Intended for Use with IPHC Profiles

The **rtp**command is intended for use as part of an IP Header Compression (IPHC) profile. An IPHC profile is used to enable and configure header compression on a network. For more information about using IPHC profiles to configure header compression, see the "Header Compression" module and the "Configuring Header Compression Using IPHC Profiles" module of the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4T.

## Examples

The following example shows how to configure an IPHC profile called profile2. In this example, RTP header compression is configured.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 ietf
Router(config-iphcp)# rtp
Router(config-iphcp)# end
```

## Related Commands

| Command | Description |
|---|---|
| **iphc-profile** | Creates an IPHC profile. |

| Command | Description |
| --- | --- |
| **non-tcp** | Enables non-TCP header compression within an IPHC profile. |

# send qdm message through show atm bundle svc statistics


- send qdm message, page 1035
- service-group, page 1037
- service-policy, page 1038
- service-policy (class-map), page 1048
- service-policy (control-plane), page 1050
- service-policy (policy-map class), page 1053
- service-policy (service group), page 1056
- service-policy type qos, page 1057
- set atm-clp, page 1059
- set cos, page 1061
- set cos cos-inner (policy-map configuration), page 1065
- set cos-inner, page 1068
- set cos-inner cos, page 1070
- set discard-class, page 1072
- set dscp, page 1074
- set fr-de, page 1078
- set ip dscp, page 1080
- set ip dscp (policy-map configuration), page 1081
- set ip dscp tunnel, page 1084
- set ip precedence (policy-map configuration), page 1086
- set ip precedence (policy-map), page 1089
- set ip precedence (route-map), page 1090
- set ip precedence tunnel, page 1093

- set ip tos (route-map), page 1095
- set precedence, page 1098
- set qos-group, page 1102
- set vlan inner, page 1106
- shape, page 1107
- shape (percent), page 1110
- shape (policy-map class), page 1114
- shape adaptive, page 1120
- shape fecn-adapt, page 1122
- shape max-buffers, page 1124
- show access-lists rate-limit, page 1126
- show atm bundle, page 1128
- show atm bundle stat, page 1130
- show atm bundle svc, page 1132
- show atm bundle svc stat, page 1134

# send qdm message

To send a text message to all Quality Device Manager (QDM) clients, use the **sendqdmmessage**command in EXEC mode.

**send qdm** [**client** *client-id*] **message** *message-text*

## Syntax Description

| | |
|---|---|
| **client** | (Optional) Specifies a QDM client to receive the message. |
| *client-id* | (Optional) Specifies the QDM identification of the client that will receive the text message. |
| **message** | Specifies that a message will be sent. |
| *message-text* | The actual text of the message. |

## Command Default

No text messages are sent.

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1(1)E | This command was introduced. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **sendqdm**command to send a message to a specific QDM client. For example, entering the**sendqdmclient9messagehello** command will send the message “hello” to client ID 9.

Use the **sendqdmmessage***message-text* command to send a message to all QDM clients. For example, entering the **sendqdmmessagehello** command sends the message “hello” to all open QDM clients.

## Examples

The following example sends the text message “how are you?” to client ID 12:

```
send qdm client 12 message how are you?
```

The following example sends the text message “how is everybody?” to all QDM clients connected to the router:

```
send qdm message how is everybody?
```

## Related Commands

| Command | Description |
|---|---|
| **show qdm status** | Displays the status of connected QDM clients. |

# service-group

To create a service group, use the service-group command in global configuration mode. To remove a service group, use the **no** form of this command.

**service-group service-group-identifier**

**no service-group service-group-identifier**

## Syntax Description

| | |
|---|---|
| *service-group-identifier* | Service-group number. A valid entry is a number between 1 and the maximum number of groups that can be supported by the router. For more information, use the question mark (?) online help function and see "Usage Guidelines." |

## Command Default

A service group is not created.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRE | This command was introduced. |

## Usage Guidelines

The maximum number of service groups that are supported on a router is determined by the router at system-startup time. For the Cisco 7600 series router, the valid entry range for the *service-group-identifier* argument is 1 to 32768.

## Examples

In the following example, service group 750 is created.

```
Router> enable
Router# configure terminal
Router(config)# service-group 750
Router(config)# end
```

# service-policy

To attach a policy map to an input interface, a virtual circuit (VC), an output interface, or a VC that will be used as the service policy for the interface or VC, use the **service-policy** command in the appropriate configuration mode. To remove a service policy from an input or output interface or from an input or output VC, use the **no** form of this command.

**service-policy** [**type access-control**] {**input| output**} *policy-map-name*

**no service-policy** [**type access-control**] {**input| output**} *policy-map-name*

### Cisco 10000 Series and Cisco 7600 Series Routers

**service-policy** [**history**| {**input| output**} *policy-map-name*| **type control** *control-policy-name*]

**no service-policy** [**history**| {**input| output**} *policy-map-name*| **type control** *control-policy-name*]

## Syntax Description

| | |
|---|---|
| **type access-control** | (Optional) Determines the exact pattern to look for in the protocol stack of interest. |
| **input** | Attaches the specified policy map to the input interface or input VC. |
| **output** | Attaches the specified policy map to the output interface or output VC. |
| *policy-map-name* | The name of a service policy map (created using the **policy-map** command) to be attached. The name can be a maximum of 40 alphanumeric characters in length. |
| **history** | (Optional) Maintains a history of quality of service (QoS) metrics. |
| **type control** *control-policy-name* | (Optional) Creates a Class-Based Policy Language (CPL) control policy map that is applied to a context. |

## Command Default

No service policy is specified. A control policy is not applied to a context. No policy map is attached.

## Command Modes

ATM VC bundle configuration (config-atm-bundle)

ATM PVP configuration (config-if-atm-l2trans-pvp)

ATM VC configuration mode (config-if-atm-vc)

Ethernet service configuration (config-if-srv)

Global configuration (config)

Interface configuration (config-if)

Static maps class configuration (config-map-class)

ATM PVC-in-range configuration (cfg-if-atm-range-pvc)

Subinterface configuration (config-subif)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE. |
| 12.0(7)S | This command was integrated into Cisco IOS Release 12.0(7)S. |
| 12.0(17)SL | This command was implemented on the Cisco 10000 series routers. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(2)T | This command was modified to enable low latency queueing (LLQ) on Frame Relay VCs. |
| 12.2(14)SX | Support for this command was implemented on Cisco 7600 series routers. Support was added for output policy maps. |
| 12.2(15)BX | This command was implemented on the ESR-PRE2. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(2)T | This command was modified. Support was added for subinterface configuration mode and for ATM PVC-in-range configuration mode to extend policy map functionality on an ATM VC to the ATM VC range. |
| 12.4(4)T | The **type stack** and **type control** keywords were added to support flexible packet matching (FPM). |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.3(7)XI2 | This command was modified to support subinterface configuration mode and ATM PVC-in-range configuration mode for ATM VCs on the Cisco 10000 series router and the Cisco 7200 series router. |
| 12.2(18)ZY | The **type stack** and **type control** keywords were integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA). |

| Release | Modification |
|---|---|
| 12.2(33)SRC | Support for this command was enhanced on Cisco 7600 series routers. |
| 12.2(33)SB | This command was modified. The command was implemented on the Cisco 10000 series router for the PRE3 and PRE4. |
| Cisco IOS XE Release 2.3 | This command was modified to support ATM PVP configuration mode. |
| 12.4(18e) | This command was modified to prevent simultaneous configuration of legacy traffic-shaping and Cisco Modular QoS CLI (MQC) shaping on the same interface. |
| Cisco IOS XE Release 3.3S | This command was modified to support Ethernet service configuration mode. |
| Cisco IOS XE Release 3.5S | This command was modified. An error displays if you try to configure the **service-policy input** or **service-policy output** command when the **ip subscriber interface** command is already configured on the interface. |
| 15.2(1)S | This command was modified to allow simultaneous nonqueueing policies to be enabled on subinterfaces. |

## Usage Guidelines

The table below shows which configuration mode to choose based on the intended use of the command.

***Table 40: Configuration Modes Based on Command Application***

| Application | Mode |
|---|---|
| Standalone VC | ATM VC submode |
| ATM VC bundle members | ATM VC Bundle configuration |
| A range of ATM PVCs | Subinterface configuration |
| Individual PVC within a PVC range | ATM PVC-in-range configuration |
| Frame Relay VC | Static maps class configuration |
| Ethernet services, Ethernet VCs (EVCs) | Ethernet service configuration |

You can attach a single policy map to one or more interfaces or to one or more VCs to specify the service policy for those interfaces or VCs.

A service policy specifies class-based weighted fair queueing (CBWFQ). The class policies that make up the policy map are then applied to packets that satisfy the class map match criteria for the class.

Before you can attach a policy map to an interface or ATM VC, the aggregate of the configured minimum bandwidths of the classes that make up the policy map must be less than or equal to 75 percent (99 percent on the Cisco 10008 router) of the interface bandwidth or the bandwidth allocated to the VC.

Before you can enable low latency queueing (LLQ) for Frame Relay (priority queueing [PQ]/CBWFQ), you must first enable Frame Relay traffic shaping (FRTS) on the interface using the **frame-relay traffic-shaping** command in interface configuration mode. You then attach an output service policy to the Frame Relay VC using the **service-policy** command in Static maps class configuration mode.

To attach a policy map to an interface or ATM VC, the aggregate of the configured minimum bandwidths of the classes that make up the policy map must be less than or equal to 75 percent of the interface bandwidth or the bandwidth allocated to the VC. For a Frame Relay VC, the total amount of bandwidth allocated must not exceed the minimum committed information rate (CIR) configured for the VC less any bandwidth reserved by the **frame-relay voice bandwidth** or **frame-relay ip rtp priority** Static maps class configuration mode commands. If these values are not configured, the minimum CIR defaults to half of the CIR.

Configuring CBWFQ on a physical interface is possible only if the interface is in the default queueing mode. Serial interfaces at E1 (2.048 Mbps) and below use weighted fair queueing (WFQ) by default. Other interfaces use first-in first-out (FIFO) by default. Enabling CBWFQ on a physical interface overrides the default interface queueing method. Enabling CBWFQ on an ATM permanent virtual circuit (PVC) does not override the default queueing method.

When you attach a service policy with CBWFQ enabled to an interface, commands related to fancy queueing such as those pertaining to fair queueing, custom queueing, priority queueing, and Weighted Random Early Detection (WRED) are available using the modular quality of service CLI (MQC). However, you cannot configure these features directly on the interface until you remove the policy map from the interface.

**Note** Beginning in Cisco IOS Release 12.4(18e), you cannot configure the traffic-shape rate and MQC shaping on the same interface at the same time. You must remove the traffic-shape rate configured on the interface before you attach the service policy. For example, if you try to enter the **service-policy** {**input** | **output**} *policy-map-name* command when the **traffic-shape rate** command is already in effect, this message is displayed:

```
Remove traffic-shape rate configured on the interface before attaching the service-policy.
```

If the MQC shaper is attached first, and you enter the legacy **traffic-shape rate** command on the same interface, the command is rejected and an error message is displayed.

You can modify a policy map attached to an interface or VC, changing the bandwidth of any of the classes that make up the map. Bandwidth changes that you make to an attached policy map are effective only if the aggregate of the bandwidth amount for all classes that make up the policy map, including the modified class bandwidth, is less than or equal to 75 percent of the interface bandwidth or the VC bandwidth. If the new aggregate bandwidth amount exceeds 75 percent of the interface bandwidth or VC bandwidth, the policy map is not modified.

After you apply the **service-policy** command to set a class of service (CoS) bit to an Ethernet interface, the policy remains active as long as there is a subinterface that is performing 8021.Q or Inter-Switch Link (ISL) trunking. Upon reload, however, the service policy is removed from the configuration with the following error message:

```
Process "set" action associated with class-map voip failed: Set cos supported only with
IEEE 802.1Q/ISL interfaces.
```

**Note** The **service-policy input** and **service-policy output** commands cannot be configured if the **ip subscriber interface** command is already configured on the interface; these commands are mutually exclusive.

### Simultaneous Nonqueueing QoS Policies

Beginning in Cisco IOS Release 15.2(1)S, you can configure simultaneous nonqueueing QoS policies on an ATM subinterface and ATM PVC, or on a Frame Relay (FR) subinterface and data-link connection identifier (DLCI). However, simultaneous queueing policies are still not allowed, because they create hierarchical queueing framework layer contention. If you try to configure simultaneous queueing policies, the policies are rejected and the router displays an error message.

**Note** If both the PVC or DLCI and subinterface policies are applied under the same subinterface, the policy under the PVC or DLCI takes precedence and the subinterface policy has no effect.

### Cisco 10000 Series Router Usage Guidelines

The Cisco 10000 series router does not support applying CBWFQ policies to unspecified bit rate (UBR) VCs.

To attach a policy map to an interface or a VC, the aggregate of the configured minimum bandwidth of the classes that make up the policy map must be less than or equal to 99 percent of the interface bandwidth or the bandwidth allocated to the VC. If you attempt to attach a policy map to an interface when the sum of the bandwidth assigned to classes is greater than 99 percent of the available bandwidth, the router logs a warning message and does not allocate the requested bandwidth to all of the classes. If the policy map is already attached to other interfaces, it is removed from them.

The total bandwidth is the speed (rate) of the ATM layer of the physical interface. The router converts the minimum bandwidth that you specify to the nearest multiple of 1/255 (ESR-PRE1) or 1/65,535 (ESR-PRE2) of the interface speed. When you request a value that is not a multiple of 1/255 or 1/65,535, the router chooses the nearest multiple.

The bandwidth percentage is based on the interface bandwidth. In a hierarchical policy, the bandwidth percentage is based on the nearest parent shape rate.

By default, a minimum bandwidth guaranteed queue has buffers for up to 50 milliseconds of 256-byte packets at line rate, but not less than 32 packets.

For Cisco IOS Release 12.0(22)S and later releases, to enable LLQ for Frame Relay (priority queueing (PQ)/CBWFQ) on the Cisco 10000 series router, first create a policy map and then assign priority to a defined traffic class using the **priority** command. For example, the following sample configuration shows how to configure a priority queue with a guaranteed bandwidth of 8000 kb/s. In the example, the Business class in the policy map named “map1” is configured as the priority queue. The map1 policy also includes the Non-Business class with a minimum bandwidth guarantee of 48 kb/s. The map1 policy is attached to serial interface 2/0/0 in the outbound direction.

```
class-map Business
 match ip precedence 3
policy-map map1
 class Business
 priority
 police 8000
 class Non-Business
 bandwidth 48
interface serial 2/0/0
 frame-relay encapsulation
 service-policy output map1
```

On the PRE2, you can use the **service-policy** command to attach a QoS policy to an ATM subinterface or to a PVC. However, on the PRE3, you can attach a QoS policy only to a PVC.

### Cisco 7600 Series Routers

The **output** keyword is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Do not attach a service policy to a port that is a member of an EtherChannel.

Although the CLI allows you to configure QoS based on policy feature cards (PFCs) on the WAN ports on the OC-12 ATM optical services modules (OSM) and on the WAN ports on the channelized OSMs, PFC-based QoS is not supported on the WAN ports on these OSMs. OSMs are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

PFC QoS supports the optional **output** keyword only on VLAN interfaces. You can attach both an input policy map and an output-policy map to a VLAN interface.

### Cisco 10000 Series Routers Control Policy Maps

Activate a control policy map by applying it to a context. A control policy map can be applied to one or more of the following types of contexts, which are listed in order of precedence:

1. Global
2. Interface
3. Subinterface
4. Virtual template
5. VC class
6. PVC

In general, control policy maps that are applied to more specific contexts take precedence over policy maps applied to more general contexts. In the list, the context types are numbered in order of precedence. For example, a control policy map that is applied to a permanent virtual circuit (PVC) takes precedence over a control policy map that is applied to an interface.

Control policies apply to all sessions hosted on the context. Only one control policy map can be applied to a given context.

### Abbreviated Form of the service-policy Command

In Cisco IOS Release 12.2(33)SB and later releases, the router does not accept the abbreviated form (ser) of the **service-policy** command. Instead, you must spell out the command name **service-** before the router accepts the command. For example, the following error message displays when you attempt to use the abbreviated form of the **service-policy** command:

```
interface GigabitEthernet1/1/0
 ser out ?
% Unrecognized command
 ser ?
% Unrecognized command
```

As shown in the following example, when you enter the command as **service-** followed by a space, the router parses the command as **service-policy**. Entering the question mark causes the router to display the command options for the **service-policy** command.

```
service- ?
input Assign policy-map to the input of an interface
output Assign policy-map to the output of an interface
type Configure CPL Service Policy
```

In releases prior to Cisco IOS Release 12.2(33)SB, the router accepts the abbreviated form of the **service-policy** command. For example, the router accepts the following commands:

```
interface GigabitEthernet1/1/0
 ser out test
```

## Examples

The following example shows how to attach a policy map to a Fast Ethernet interface:

```
interface fastethernet 5/20
 service-policy input pmap1
```

The following example shows how to attach the service policy map named “policy9” to DLCI 100 on output serial interface 1 and enables LLQ for Frame Relay:

```
interface Serial1/0.1 point-to-point
 frame-relay interface-dlci 100
 class fragment
 map-class frame-relay fragment
 service-policy output policy9
```

The following example shows how to attach the service policy map named “policy9” to input serial interface 1:

```
interface Serial1
 service-policy input policy9
```

The following example attaches the service policy map named “policy9” to the input PVC named “cisco”:

```
pvc cisco 0/34
service-policy input policy9
vbr-nt 5000 3000 500
precedence 4-7
```

The following example shows how to attach the policy named “policy9” to output serial interface 1 to specify the service policy for the interface and enable CBWFQ on it:

```
interface serial1
 service-policy output policy9
```

The following example attaches the service policy map named “policy9” to the output PVC named "cisco":

```
pvc cisco 0/5
service-policy output policy9
vbr-nt 4000 2000 500
precedence 2-3
```

## Examples

The following example shows how to attach the service policy named “userpolicy” to DLCI 100 on serial subinterface 1/0/0.1 for outbound packets:

```
interface serial 1/0/0.1 point-to-point
 frame-relay interface-dlci 100
 service-policy output userpolicy
```

**Note** You must be running Cisco IOS Release 12.0(22)S or a later release to attach a policy to a DLCI in this way. If you are running a release prior to Cisco IOS Release 12.0(22)S, attach the service policy as described in the previous configuration examples using the legacy Frame Relay commands, as shown in the example “how to attach the service policy map named “policy9” to DLCI 100 on output serial interface 1 and enable LLQ for Frame Relay”.

The following example shows how to attach a QoS service policy named “map2” to PVC 0/101 on the ATM subinterface 3/0/0.1 for inbound traffic:

```
interface atm 3/0/0
 atm pxf queueing
interface atm 3/0/0.1
 pvc 0/101
 service-policy input map2
```

**Note** The **atm pxf queueing** command is not supported on the PRE3 or PRE4.

The following example shows how to attach a service policy named “myQoS” to physical Gigabit Ethernet interface 1/0/0 for inbound traffic. VLAN 4, configured on Gigabit Ethernet subinterface 1/0/0.3, inherits the service policy of physical Gigabit Ethernet interface 1/0/0.

```
interface GigabitEthernet 1/0/0
 service-policy input myQoS
interface GigabitEthernet 1/0/0.3
 encapsulation dot1q 4
```

The following example shows how to apply the policy map named “policy1” to the virtual template named “virtual-template1” for all inbound traffic. In this example, the virtual template configuration also includes Challenge Handshake Authentication Protocol (CHAP) authentication and PPP authorization and accounting.

```
interface virtual-template1
 ip unnumbered Loopback1
 no peer default ip address
 ppp authentication chap vpn1
 ppp authorization vpn1
 ppp accounting vpn1
 service-policy input policy1
```

The following example shows how to attach the service policy map named “voice” to ATM VC 2/0/0 within a PVC range of a total of three PVCs and enable subinterface configuration mode where a point-to-point subinterface is created for each PVC in the range. Each PVC created as part of the range has the voice service policy attached to it.

```
configure terminal
 interface atm 2/0/0
 range pvc 1/50 1/52
 service-policy input voice
```

The following example shows how to attach the service policy map named “voice” to ATM VC 2/0/0 within a PVC range, where every VC created as part of the range has the voice service policy attached to it. The exception is PVC 1/51, which is configured as an individual PVC within the range and has a different service policy named “data” attached to it in ATM PVC-in-range configuration mode.

```
configure terminal
 interface atm 2/0/0
 range pvc 1/50 1/52
 service-policy input voice
 pvc-in-range 1/51
 service-policy input data
```

The following example shows how to configure a service group named “PREMIUM-SERVICE” and apply the input policy named “PREMIUM-MARK-IN” and the output policy named “PREMIUM-OUT” to the service group:

```
policy-map type service PREMIUM-SERVICE
 service-policy input PREMIUM-MARK-IN
 service-policy output PREMIUM-OUT
```

The following example shows a policy map and interface configuration that supported simultaneous nonqueueing policies:

```
Policy-map p-map
class c-map
set mpls experimental imposition 4

interface ATM1/0/0.1 multipoint
no atm enable-ilmi-trap
xconnect 10.1.1.1 100001 encapsulation mpls
service-policy input p-map
pvc 1/41 l2transport
no epd
!
pvc 1/42 l2transport
no epd
!
pvc 1/43 l2transport
no epd
interface ATM1/0/0.101 multipoint
no atm enable-ilmi-trap
pvc 9/41 l2transport
xconnect 10.1.1.1 1001011 encapsulation mpls
service-policy input p-map
!
pvc 10/41 l2transport
xconnect 10.1.1.1 1001012 encapsulation mpls
!
```

The following example shows how to attach simultaneous nonqueueing QoS policies on an ATM subinterface and ATM PVC:

```
interface atm 1/0/0.101
pvc 9/41
service-policy input p-map
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Accesses QoS class-map configuration mode to configure QoS class maps. |
| **frame-relay ip rtp priority** | Reserves a strict priority queue on a Frame Relay PVC for a set of RTP packet flows belonging to a range of UDP destination ports, |
| **frame-relay traffic-shaping** | Enables both traffic shaping and per-virtual-circuit queueing for all PVCs and SVCs on a Frame Relay interface. |
| **frame-relay voice bandwidth** | Specifies the amount of bandwidth to be reserved for voice traffic on a specific DLCI. |
| **ip subscriber interface** | Creates an ISG IP interface session. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **priority** | Gives priority to a class of traffic belonging to a policy map. |

| Command | Description |
|---|---|
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |
| **traffic-shape rate** | Enables traffic shaping for outbound traffic on an interface. |

# service-policy (class-map)

To attach a policy map to a class, use the **service-policy**command in class-map configuration mode. To remove a service policy from a class, use the **no** form of this command.

**service-policy** *policy-map*

**no service-policy**

## Syntax Description

| | |
|---|---|
| *policy-map* | The name of a service policy map (created using the **policy-map** command) to be attached. The name can be a maximum of 40 alphanumeric characters. |

## Command Default

No service policy is specified.

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(2)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

You can attach a single policy map to one or more classes to specify the service policy for those classes. This command is only available for the output interface, which is assumed.

## Examples

In the following example, three policy maps are defined--cust1-classes, cust2-classes, and cust-policy. The policy maps cust1-classes and cust2-classes have three classes defined--gold, silver, and bronze.

For cust1-classes, gold is configured to use 50 percent of the bandwidth. Silver is configured to use 20 percent of the bandwidth, and bronze is configured to use 15 percent of the bandwidth.

For cust2-classes, gold is configured to use 30 percent of the bandwidth. Silver is configured to use 15 percent of the bandwidth, and bronze is configured to use 10 percent of the bandwidth.

The policy map cust-policy specifies average rate shaping of 384 kbps and assigns the service policy called cust1-classes to the policy map called cust1-classes. The policy map called cust-policy specifies peak rate shaping of 512 kbps and assigns the service policy called cust2-classes to the policy map called cust2-classes.

To configure classes for cust1-classes, use the following commands:

```
Router(config)# policy-map cust1-classes
Router(config-pmap)# class gold
Router(config-pmap-c)# bandwidth percent 50
Router(config-pmap-c)# exit
Router(config-pmap)# class silver
Router(config-pmap-c)# bandwidth percent 20
Router(config-pmap-c)# exit
Router(config-pmap)# class bronze
Router(config-pmap-c)# bandwidth percent 15
```

To configure classes for cust2, use the following commands:

```
Router(config)# policy-map cust2-classes
Router(config-pmap)# class gold
Router(config-pmap-c)# bandwidth percent 30
Router(config-pmap-c)# exit
Router(config-pmap)# class silver
Router(config-pmap-c)# bandwidth percent 15
Router(config-pmap-c)# exit
Router(config-pmap)# class bronze
Router(config-pmap-c)# bandwidth percent 10
```

To define the customer policy with cust1-classes and cust2-classes and QoS features, use the following commands:

```
Router(config)# policy-map cust-policy
Router(config-pmap)# class cust1
Router(config-pmap-c)# shape average 38400
Router(config-pmap-c)# service-policy cust1-classes
Router(config-pmap-c)# exit
Router(config-pmap)# class cust2
Router(config-pmap-c)# shape peak 51200
Router(config-pmap-c)# service-policy cust2-classes
Router(config-pmap-c)# interface Serial 3/2
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# exit
Router(config)# interface serial0/0
Router(config-if)# service out cust-policy
```

## Related Commands

| Command | Description |
|---|---|
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |

# service-policy (control-plane)

To attach a policy map to a control plane for aggregate or distributed control plane services, use the **service-policy** command in control-plane configuration mode. To remove a service policy from a control plane, use the **no** form of this command.

**service-policy** {**input**| **output**} *policy-map-name*

**no service-policy** {**input**| **output**} *policy-map-name*

## Syntax Description

| | |
|---|---|
| **input** | Applies the specified service policy to packets that are entering the control plane. |
| **output** | Applies the specified service policy to packets that are exiting the control plane, and enables the router to silently discard packets. |
| *policy-map-name* | Name of a service policy map (created using the **policy-map** command) to be attached. The name can be a maximum of 40 alphanumeric characters. |

## Command Default

No service policy is specified.

## Command Modes

Control-plane configuration (config-cp)

## Command History

| Release | Modification |
|---|---|
| 12.2(18)S | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T, and support for the **output** keyword was added. |
| 12.0(29)S | This command was integrated into Cisco IOS Release 12.0(29)S. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(25)S | Support for the **output** keyword was integrated into Cisco IOS Release 12.2(25)S. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| Cisco IOS XE Release 2.2 | This command was implemented on Cisco ASR 1000 series routers. |

## Usage Guidelines

After entering the **control-plane** command, use the **service-policy** command to configure a quality of service (QoS) policy. This policy is attached to the control plane interface for aggregate or distributed control plane services and controls the number or rate of packets that are going to the process level.

When you configure output policing on control-plane traffic, using the **service-policyoutput***policy-map-name* command, a router is automatically enabled to silently discard packets. Output policing is supported as follows:

- Supported only in:
  - Cisco IOS Release 12.2(25)S and later Cisco IOS 12.2S releases.
  - Cisco IOS Release 12.3(4)T and later Cisco IOS 12.3T releases.
  - Cisco IOS Release 12.2(18)SXD1 and later Cisco IOS 12.2SX releases.
  - Cisco IOS XE Release 2.2 and later Cisco IOS XE releases.
- Not supported for attaching a QoS policy for distributed control-plane services.
- Not supported on the Cisco 6500 router, Cisco 7500 series, and Cisco 10720 Internet router.

The **service-policyoutput**command configures output policing, which is performed in silent mode to silently discard packets exiting from the control plane according to the attached QoS policy. Silent mode allows a router that is running Cisco IOS software to operate without sending any system messages. If a packet that is exiting from the control plane is discarded for output policing, you do not receive an error message.

Silent mode allows a router that is running Cisco IOS software to operate without sending any system messages. If a packet that is destined for the router is discarded for any reason, users will not receive an error message. Some events that will not generate error messages are as follows:

- Traffic that is being transmitted to a port to which the router is not listening
- A connection to a legitimate address and port that is rejected because of a malformed request

## Examples

The following example shows how to configure trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 to forward Telnet packets to the control plane without constraint, while allowing all remaining Telnet packets to be policed at the specified rate:

```
! Allow 10.1.1.1 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet

! Allow
10.1.1.2
 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet

! Rate-limit all other Telnet traffic.
Router(config)# access-list 140 permit tcp any any eq telnet
! Define class-map “telnet-class.”
Router(config)# class-map telnet-class

Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-policy
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
```

```
Router(config-pmap)# exit
! Define aggregate control plane service for the active route processor.
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-policy
Router(config-cp)# end
```

The next example shows how to configure trusted networks with source addresses 10.0.0.0 and 10.0.0.2 to receive Internet Control Message Protocol (ICMP) port-unreachable responses without constraint, while allowing all remaining ICMP port-unreachable responses to be dropped:

```
! Allow 10.0.0.0 trusted network traffic.
Router(config)# access-list 141 deny icmp host
10.0.0.0

255.255.255.224
 any port-unreachable

! Allow 10.0.0.2 trusted network traffic.
Router(config)# access-list 141 deny icmp host
10.0.0.2 255.255.255.224
 any port-unreachable

! Rate-limit all other ICMP traffic.
Router(config)# access-list 141 permit icmp any any port-unreachable
Router(config)# class-map icmp-class

Router(config-cmap)# match access-group 141
Router(config-cmap)# exit
Router(config)# policy-map control-plane-out-policy
! Drop all traffic that matches the class "icmp-class."
Router(config-pmap)# class icmp-class
Router(config-pmap-c)# drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# control-plane
! Define aggregate control plane service for the active route processor.
Router(config-cp)# service-policy output control-plane-out-policy
Router(config-cp)# end
```

## Related Commands

| Command | Description |
|---|---|
| **control-plane** | Enters control-plane configuration mode to apply a QoS policy to police traffic destined for the control plane. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **show policy-map control-plane** | Displays the configuration of a class or all classes for the policy map attached to the control plane. |

# service-policy (policy-map class)

To use a service policy as a QoS policy within a policy map (called a hierarchical service policy), use the **service-policy** command in policy-map class configuration mode. To disable a particular service policy as a QoS policy within a policy map, use the **no** form of this command.

**service-policy** *policy-map-name*

**no service-policy** *policy-map-name*

## Syntax Description

| | |
|---|---|
| *policy-map-name* | Specifies the name of the predefined policy map to be used as a QoS policy. The name can be a maximum of 40 alphanumeric characters. |

## Command Default

No service policies are used.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.1(2)E | This command was introduced. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers. |

## Usage Guidelines

This command is used to create hierarchical service policies in policy-map class configuration mode.

This command is different from the **service-policy** {**input**|**output**}*policy-map-name*command used in interface configuration mode. The purpose of the **service-policy**{**input**|**output**}*policy-map-name* is to attach service policies to interfaces.

The child policy is the previously defined service policy that is being associated with the new service policy through the use of the **service-policy**command. The new service policy using the preexisting service policy is the parent policy.

This command has the following restrictions:

- The **priority** command can be used in either the parent or the child policy, but not *both* policies simultaneously.
- The **shape** command can be used in either the parent or the child policy, but not *both* polices simultaneously on a subinterface.
- The **fair-queue** command cannot be defined in the parent policy.
- If the **bandwidth**command is used in the child policy, the **bandwidth** command must also be used in the parent policy. The one exception is for policies using the default class.

## Examples

The following example creates a hierarchical service policy in the service policy called parent:

```
Router(config)# policy-map child
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 10000000
Router(config-pmap-c)# service-policy child
```

FRF.11 and FRF.12 configurations on a Versatile Interface Processor (VIP)-enabled Cisco 7500 series router often require a hierarchical service policy for configuration. A hierarchical service policy for FRF.11 and FRF.12 requires the following elements:

1. A traffic class that uses the Voice over Frame Relay (VoFR) protocol as the only match criterion.
2. A traffic policy that insures low latency queueing (LLQ), which is achieved using the **priority** command, for all VoFR protocol traffic
3. A traffic policy that defines the shaping parameters and includes the elements listed in element 2.

Element 3 can only be fulfilled through the use of a hierarchical service policy, which is configured using the **service-policy** command.

In the following example, element 1 is configured in the traffic class called frf, element 2 is configured in the traffic policy called llq, and element 3 is configured in the traffic policy called llq-shape.

```
Router(config)#

class-map frf
Router(config-cmap)# match protocol vofr
Router(config-cmap)
#
exit
Router(config)#

policy-map llq
Router(config-pmap)#

class frf
Router(config-pmap-c)# priority 2000
Router(config-pmap-c)#

exit
Router(config-pmap)# exit
Router(config)# policy-map llq-shape
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 1000 128000
Router(config-pmap-c)#
```

**service-policy llq**

The final step in using a hierarchical service policy for FRF.11 and FRF.12 is using the service policy in map-class configuration mode. In the following example, the traffic policy called llq-shape is attached to the map class called frag:

```
Router(config)#

map-class frame-relay frag
Router(config-map-class)# frame-relay fragment 40
Router(config-map-class)# service-policy llq-shape
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth (policy-map class)** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map. |
| **fair-queue** | Specifies the number of queues to be reserved for use by a traffic class. |
| **policy-map** | Specifies the name of the service policy to configure. |
| **priority** | Gives priority to a class of traffic belonging to a policy map. |
| **service-policy** | Specifies the name of the service policy to be attached to the interface. |
| **shape** | Specifies average or peak rate traffic shaping. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

# service-policy (service group)

To attach a policy map to a service group, use the **service-policy** command in service-group configuration mode. To remove a policy map from a service group, use the **no** form of this command.

**service-policy** {**input**| **output**} *policy-map-name*

**no service-policy** {**input**| **output**} *policy-map-name*

## Syntax Description

| | |
|---|---|
| **input** | Attaches the policy map to the service group in the input (ingress) direction. |
| **output** | Attaches the policy map to the service group in the output (egress) direction. |
| *policy-map-name* | Policy map name. Enter the name of an existing policy map. |

## Command Default

A policy map is not attached to a service group.

## Command Modes

Service-group configuration (config-service-group)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRE | This command was introduced. |

## Usage Guidelines

The policy map must already exist and must contain the Quality of Service (QoS) feature to be applied to the service group, according to the provisions specified by the Service Level Agreement (SLA). To create and configure the policy map, use the Modular Quality of Service Command-Line Interface (CLI) (MQC). For more information about the MQC, see the *Cisco IOS Quality of Service Solutions Configuration Guide* .

## Examples

In the following example, a policy map called 3-customer-in is attached to service group 1:

```
Router> enable
Router# configure terminal
Router(config)# service-group 1
Router(config-service-group)# service-policy input 3-customer-in
Router(config-service-group)# end
```

# service-policy type qos

To apply a quality of service (QoS) policy map to an identity, use the **service-policytypeqos** command in identity policy configuration mode. To remove the QoS policy map, use the **no** form of this command.

**service-policy type qos** {**input| output**} *policy-map-name*

**no service-policy type qos** {**input| output**} *policy-map-name*

## Syntax Description

| | |
|---|---|
| **input** | Specifies an ingress QoS policy map. |
| **output** | Specifies an egress QoS policy map. |
| *policy-map-name* | The name of the policy map. |

## Command Default

No QoS policy map is applied to an identity.

## Command Modes

Identity policy configuration (config-identity-policy)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SXI | This command was introduced. |

## Usage Guidelines

The **input** and **output**keywords indicate the direction in which the policy map will be applied.

The value for the *policy-map-name*argument represents a QoS policy map configured on the switch using the **policy-map***policy-map-name*global configuration command.

## Examples

The following example applies an ingress QoS policy map to an identity:

```
Router(config)# identity policy policy1
Router(config-identity-policy)# service-policy type qos input my-in-policy
```

## Related Commands

| Command | Description |
|---|---|
| **identity policy** | Creates an identity policy. |
| **policy-map** | Creates or modifies a policy map |

| Command | Description |
| --- | --- |
| **show epm session ip** | Displays the configuration and policies on an interface when a session is active. |

# set atm-clp

To set the ATM cell loss priority (CLP) bit when a policy map is configured, use the **setatm-clp**command in policy-map classconfigurationmode. To remove a specific ATM CLP bit setting, use the **no** form of this command.

**set atm-clp**

**no set atm-clp**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The ATM CLP bit is automatically set to 0 by Cisco router interfaces, when Cisco routers convert IP packets into ATM cells for transmission through Multiprotocol Label Switching (MPLS)-aware ATM networks.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.1(5)T | This command was introduced. |
| 12.2(4)T | This command was implemented on the Cisco MGX 8850 switch and the MGX 8950 switch with a Cisco MGX RPM-PR card. |
| 12.2(4)T2 | This command was implemented on the Cisco 7500 series router. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

To disable this command, remove the service policy from the interface using the **noservice-policy** command.

The **setatm-clp**command works only on platforms that support one of the following adapters: the Enhanced ATM Port Adapter (PA-A3), the ATM Inverse Multiplexer over ATM Port Adapter with eight T1 ports (PA-A3-8T1IMA), or the ATM Inverse Multiplexer over ATM Port Adapter with eight E1 ports (PA-A3-8E1IMA). For more information, refer to the documentation for your specific router.

A policy map containing the **setatm-clp**command can be attached as an output policy only. The **setatm-clp** command does not support packets that originate from the router. A policy map containing ATM set CLP bit

quality of service (QoS) cannot be attached to PPP over X (PPPoX) sessions. The policy map is accepted only if you do not specify the **setatm-clp** command.

## Examples

The following example shows how to set the CLP bit by using the **setatm-clp** command in a policy map:

```
Router(config)#
class-map ip-precedence
Router(config-cmap)#
match ip precedence 0 1
Router(config-cmap)#
exit
Router(config)#
policy-map atm-clp-set
Router(config-pmap)#
class ip-precedence
Router(config-pmap-c)#
set atm-clp
Router(config-pmap-c)#
exit
Router(config-pmap)#
exit
Router(config)#
interface atm 1/0/0.1
Router(config-if)#
service-policy output policy1
```

## Related Commands

| Command | Description |
|---|---|
| class | Associates a map class with a specified data-link connection identifier. |
| class-map | Configures a class map. |
| interface | Creates an interface. |
| match ip precedence | Identifies IP precedence values to use as the match criterion. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| service-policy | Attaches a policy map to an input interface, a virtual circuit (VC), an output interface, or a VC that will be used as the service policy for the interface or VC. |
| **show atm pvc** | Displays all ATM PVCs and traffic information. |
| **show policy-map** | Displays information about the policy map for an interface. |

# set cos

To set the Layer 2 class of service (CoS) value of an outgoing packet, use the **setcos** command in policy-map class configuration mode. To remove a specific CoS value setting, use the **no** form of this command.

**set cos** {*cos-value*| *from-field* [**table** *table-map-name*]}

**no set cos** {*cos-value*| *from-field* [**table** *table-map-name*]}

### Cisco CMTS and 10000 Series Router

**set cos** *cos-value*

## Syntax Description

| | |
|---|---|
| *cos-value* | Specific IEEE 802.1Q CoS value from 0 to 7. |
| *from-field* | Specific packet-marking category to be used to set the CoS value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords are as follows:<br>• **precedence**<br>• **dscp** |
| **table** | (Optional) Indicates that the values set in a specified table map will be used to set the CoS value. |
| *table-map-name* | (Optional) Name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters. |

## Command Default

No CoS value is set for the outgoing packet.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(5)T | This command was introduced. |
| 12.2(13)T | This command was modified for Enhanced Packet Marking to allow a mapping table (table map)to be used to convert and propagate packet-marking values. |

| Release | Modification |
|---|---|
| 12.0(16)BX | This command was implemented on the Cisco 10000 series router for the ESR-PRE2. |
| 12.0(31)S | This command was integrated into Cisco IOS Release 12.0(31)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SCF | This command was integrated into Cisco IOS Release 12.2(33)SCF. |
| 3.2SE | This command was integrated into Cisco IOS XE Release 3.2SE. |

## Usage Guidelines

CoS packet marking is supported only in the Cisco Express Forwarding switching path.

The **setcos** command should be used by a router if a user wants to mark a packet that is being sent to a switch. Switches can leverage Layer 2 header information, including a CoS value marking.

The **setcos** command can be used only in service policies that are attached in the output direction of an interface. Packets entering an interface cannot be set with a CoS value.

The **matchcos** and **setcos** commands can be used together to allow routers and switches to interoperate and provide quality of service (QoS) based on the CoS markings.

Layer 2 to Layer 3 mapping can be configured by matching on the CoS value because switches already can match and set CoS values. If a packet that needs to be marked to differentiate user-defined QoS services is leaving a router and entering a switch, the router should set the CoS value of the packet because the switch can process the Layer 2 header.

### Using This Command with the Enhanced Packet Marking Feature

You can use this command as part of the Enhanced Packet Marking feature to specify the “from-field” packet-marking category to be used for mapping and setting the CoS value. The “from-field” packet-marking categories are as follows:

- Precedence
- Differentiated services code point (DSCP)

If you specify a “from-field” category but do not specify the **table** keyword and the applicable *table-map-nam* e argument, the default action will be to copy the value associated with the “from-field” category as the CoS value. For instance, if you configure the **setcosprecedence** command, the precedence value will be copied and used as the CoS value.

You can do the same for the DSCP marking category. That is, you can configure the **setcosdscp** command, and the DSCP value will be copied and used as the CoS value.

**Note** If you configure the **setcosdscp**command, only the *first three bits* (the class selector bits) of the DSCP field are used.

## Examples

In the following example, the policy map called "cos-set" is created to assign different CoS values for different types of traffic. This example assumes that the class maps called "voice" and "video-data" have already been created.

```
Router(config)#
policy-map cos-set
Router(config-pmap)#
class voice
Router(config-pmap-c)#
set cos 1
Router(config-pmap-c)#
exit
Router(config-pmap)#
class video-data
Router(config-pmap-c)#
set cos 2
Router(config-pmap-c)#
end
```

## Examples

In the following example, the policy map called "policy-cos" is created to use the values defined in a table map called "table-map1". The table map called "table-map1" was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping)command, see the **table-map**(value mapping) command page.

In this example, the setting of the CoS value is based on the precedence value defined in "table-map1":

```
Router(config)#
policy-map policy-cos
Router(config-pmap)#
class class-default
Router(config-pmap-c)#
set cos precedence table table-map1
Router(config-pmap-c)#
end
```

## Examples

The following example shows how to set the class of service for the 802.1p domain:

```
Router(config)# policy-map cos7
Router(config-pmap)# class cos7
Router(config-pmap-c)# set cos 2
Router(config-pmap-c)# end
```

**Note** The **setcos** command is applied when you create a service policy in QoS policy-map configuration mode and attach the service policy to an interface or ATM virtual circuit (VC). For information on attaching a service policy, refer to the "Modular Quality of Service Command-Line Interface Overview" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide* .

## Related Commands

| Command | Description |
|---|---|
| **match cos** | Matches a packet on the basis of Layer 2 CoS marking. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **set dscp** | Marks a packet by setting the Layer 3 DSCP value in the ToS byte. |
| **set precedence** | Sets the precedence value in the packet header. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map class** | Displays the configuration for the specified class of the specified policy map. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

# set cos cos-inner (policy-map configuration)

To set the 802.1Q prioritization bits in the trunk VLAN tag of a QinQ-translated outgoing packet with the priority value from the inner customer-edge VLAN tag, use the **setcoscos-inner** command in policy-map class configuration mode. To return to the default settings, use the **no** form of this command.

**set cos cos-inner**

**no set cos cos-inner**

## Syntax Description

This command has no arguments or keywords.

## Command Default

P bits are copied from the outer provider-edge VLAN tag.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXD | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is supported on the Gigabit Ethernet WAN interfaces on Cisco 7600 series routers that are configured with an Optical Service Module (OSM)-2+4GE-WAN+ OSM module only.

OSMs are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

The 802.1P prioritization bits are used in the VLAN tag for QoS processing.

When the router copies the double-tagged QinQ packets to the destination interface, by default it uses the P bits from the outer (provider) VLAN tag. To preserve the P bits that are in the inner (customer) VLAN tag, use the **setcoscos-inner** command.

For the **setcoscos-inner** command to be effective, you must configure the appropriate interface or subinterface as a trusted interface using the **mlsqostrust** command. Otherwise, the interface or subinterface defaults to being untrusted, where the Layer 2 interface zeroes out the P bits of the incoming packets before the **setcoscos-inner** command can copy them to the outer VLAN tag.

The **setcoscos-inner** command is supported only for the subinterfaces that are configured with an inner (customer) VLAN. The **setcoscos-inner** command is not supported for the subinterfaces that use the **out-range** keyword on the **bridge-domain**(subinterface configuration)command or that are not configured with any form of the **bridge-domain** (subinterface configuration)command.

This behavior remains when you configure the **setcoscos-inner** command on a policy that is applied to a main interface. The**setcoscos-inner**command affects the subinterfaces that are configured with a specific inner

VLAN but it does not affect the subinterfaces that are not configured with any VLAN or that are configured with the **out-range** keyword.

## Examples

This example shows how to configure a policy map for voice traffic that uses the P bits from the inner VLAN tag:

```
Router(config-cmap)# set cos cos-inner
```

This example shows how to configure the default policy map class to reset to its default value:

```
Router(config-cmap)# no set cos cos-inner
```

This example shows the system message that appears when you attempt to apply a policy to a subinterface that is configured with the **bridge-domain(subinterfaceconfiguration)**command:

```
Router(config-if)# bridge-vlan 32 dot1q-tunnel out-range

Router(config-if)# service-policy output cos1

%bridge-vlan 32 does not have any inner-vlan configured. 'set cos cos-inner' is not supported
```

## Related Commands

| Command | Description |
|---|---|
| **bridge-domain (subinterface configuration)** | Binds a PVC to the specified vlan-id. |
| **class map** | Accesses the QoS class map configuration mode to configure QoS class maps. |
| **mode dot1q-in-dot1q access-gateway** | Enables a Gigabit Ethernet WAN interface to act as a gateway for QinQ VLAN translation. |
| **policy-map** | Accesses QoS policy-map configuration mode to configure the QoS policy map. |
| **service-policy** | Attaches a policy map to an interface. |
| **set in dscp (policy-map configuration)** | Marks a packet by setting the IP DSCP in the ToS byte. |
| **set ip precedence (policy-map configuration)** | Sets the precedence value in the IP header. |
| **show cwan qinq** | Displays the inner, outer, and trunk VLANs that are used in QinQ translation. |
| **show cwan qinq bridge-domain** | Displays the provider-edge VLAN IDs that are used on a Gigabit Ethernet WAN interface for QinQ translation or shows the customer-edge VLANs that are used for a specific provider-edge VLAN. |

| Command | Description |
|---|---|
| **show cwan qinq interface** | Displays interface statistics for IEEE 802.1Q-in-802.1Q (QinQ) translation on one or all Gigabit Ethernet WAN interfaces and port-channel interfaces. |
| **show policy-map** | Displays information about the policy map. |
| **show policy-map interface** | Displays the statistics and the configurations of the input and output policies that are attached to an interface. |

# set cos-inner

To mark the inner class of service field in a bridged frame, use the **setcos-inner**command in policy-map class configuration mode. To remove marking of the inner CoS field, use the **no** form of this command.

**set cos-inner** *cos-value*

**no set cos-inner** *cos-value*

## Syntax Description

| | |
|---|---|
| *cos-value* | IEEE 802.1q CoS value from 0-7. |

## Command Default

No default behavior or values.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was introduced. |

## Usage Guidelines

This command was introduced in Cisco IOS Release 12.2(33)SRA to support marking of the inner CoS value when using multipoint bridging (MPB) features on the Enhanced FlexWAN module, and when using MPB features on SPAs with the Cisco 7600 SIP-200 and Cisco 7600 SIP-400 on the Cisco 7600 series router.

This command is not supported on the Cisco 7600 SIP-600.

On the Cisco 7600 SIP-200, this command is not supported with the **setcos** command on the same interface.

For more information about QoS and the forms of marking commands supported by the SIPs on the Cisco 7600 series router, refer to the *Cisco 7600 Series SIP, SSC, and SPA Software Configuration Guide* .

## Examples

The following example shows configuration of a QoS class that filters all traffic matching on VLAN 100 into a class named “vlan-inner-100.” The configuration shows the definition of a policy-map (also named “vlan-inner-100”) that marks the inner CoS with a value of 3 for traffic in the vlan-inner-100 class. Since marking of the inner CoS value is only supported with bridging features, the configuration also shows the service policy being applied as an output policy to a serial SPA interface that bridges traffic into VLAN 100 using the **bridge-domain** command:

```
Router(config)# class-map match-all vlan-inner-100
Router(config-cmap)# match vlan inner 100
Router(config-cmap)# exit
Router(config)# policy-map vlan-inner-100
Router(config-pmap)# class vlan-inner-100
Router(config-pmap-c)# set cos-inner 3
Router(config-pmap-c)# exit
```

```
Router(config-pmap)# exit
Router(config)# interface serial3/0/0
Router(config-if)# no ip address
Router(config_if)# encapsulation ppp
Router(config-if)# bridge-domain 100 dot1q
Router(config-if)# service-policy output vlan-inner-100
Router(config-if)# shutdown
Router(config-if)# no shutdown
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **bridge-domain** | Enables RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged virtual LAN (VLAN) to an ATM permanent virtual circuit (PVC) or Frame Relay data-link connection identifier (DLCI). |
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **class (policy-map)** | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy. |
| **service-policy** | Attaches a policy map to an input interface or virtual circuit (VC) or an output interface or VC, to be used as the service policy for that interface or VC. |

# set cos-inner cos

To copy the outer COS to the inner COS for double-tagged packets, use the **setcos-innercos** command in policy-map class configuration mode. To remove the outer COS copied to the inner COS for double-tagged packets, use the **no** form of this command.

**set cos-inner cos** *cos-value*

**no set cos-inner cos** *cos-value*

## Syntax Description

| | |
|---|---|
| *cos-value* | IEEE 802.1q CoS value from 0-7. |

## Command Default

No default behavior or values.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRB | This command was introduced. |

## Usage Guidelines

This command was introduced in Cisco IOS Release 12.2(33)SRB and is limited to policies that are applied to the EVC service instances.

For classification, the reference to the outer and inner tags is made to the frames as seen on the wire - that is, for ingress frames, tags prior to the "rewrite", while the for egress, it is after the "rewrite" of the tags, if any.

For marking, the reference to the outer COS at the ingress is to the DBUS-COS and reference to the inner is to the COS in the first tag on the frame; while, at the egress, the reference to outer and inner COS is to the ones in the frame.

## Examples

The following example matches on outer COS 3 and 4 and copies the outer COS to the inner COS.

```
Router(config)# class-map cos3_4
Router(config-cmap)# match cos 3 4
Router(config)# policy-map mark-it-in
Router(config-pmap)# class cos3_4
Router(config-pmap-c)# set cos-inner cos
```

## Related Commands

| Command | Description |
|---|---|
| **bridge-domain** | Enables RFC 1483 ATM bridging or RFC 1490 Frame Relay bridging to map a bridged virtual LAN (VLAN) to an ATM permanent virtual circuit (PVC) or Frame Relay data-link connection identifier (DLCI). |
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **class (policy-map)** | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy. |
| **service-policy** | Attaches a policy map to an input interface or virtual circuit (VC) or an output interface or VC, to be used as the service policy for that interface or VC. |

# set discard-class

To mark a packet with a discard-class value, use the **setdiscard-class** command in QoS policy-map configuration mode. To prevent the discard-class value of a packet from being altered, use the **no** form of this command.

**set discard-class** *value*

**no set discard-class** *value*

## Syntax Description

| | |
|---|---|
| *value* | Specifies per-hop behavior (PHB) for dropping traffic. The value sets the priority of a type of traffic. Valid values are numbers from 0 to 7. |

## Command Default

If you do not enter this command, the packet has a discard-class value of 0.

## Command Modes

QoS policy-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.3(7)XI | This command was implemented on the Cisco 10000 series router for the ESR-PRE2. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB. |

## Usage Guidelines

The discard class value indicates the discard portion of the PHB. Use the **setdiscard-class** command only in DiffServ Tunneling Pipe mode. The discard class value is required when the input PHB marking will be used to classify packets on the output interface.

You can also use this command to specify the type of traffic that will be dropped when there is congestion.

**Cisco 10000 Series Router**

This command is supported only on the ESR-PRE2.

## Examples

The following example shows that traffic will be set to the discard-class value of 2:

```
set discard-class 2
```

## Related Commands

| Command | Description |
|---|---|
| **match discard-class** | Matches packets of a certain discard class. |
| **random-detect discard-class-based** | Bases WRED on the discard class value of a packet. |

# set dscp

To mark a packet by setting the differentiated services code point (DSCP) value in the type of service (ToS) byte, use the **set dscp** command in QoS policy-map class configuration mode. To remove a previously set DSCP value, use the **no** form of this command.

**set dscp** {*dscp-value*| *from-field* [**table** *table-map-name*]}

**no set dscp** {*dscp-value*| *from-field* [**table** *table-map-name*]}

## Syntax Description

| | |
|---|---|
| *dscp-value* | A number that sets the DSCP value. The range is from 0 to 63.<br>The following reserved keywords can be specified instead of numeric values:<br>• **EF** (expedited forwarding)<br>• **AF11** (assured forwarding class AF11)<br>• **AF12** (assured forwarding class AF12) |
| *from-field* | Specific packet-marking category to be used to set the DSCP value of the packet. Packet-marking category keywords are as follows:<br>• **cos**<br>• **qos-group**<br>**Note** If you are using a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. |
| **table** | (Optional) Indicates that the values set in a specified table map will be used to set the DSCP value.<br>• This keyword is used in conjunction with the *from-field* argument. |
| *table-map-name* | (Optional) Name of the table map used to specify the DSCP value. The name can be a maximum of 64 alphanumeric characters.<br>• This argument is used in conjunction with the **table** keyword. |

**Command Default** The DSCP value in the ToS byte is not set.

**Command Modes** QoS policy-map class configuration (config-pmap-c)

**Command History**

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. It replaces the **set ip dscp** command. |
| 12.0(28)S | This command was modified. Support for this command in IPv6 was added on the Cisco 12000 series Internet router. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 Series Aggregation Services Routers. |

**Usage Guidelines** Once the DSCP bit is set, other quality of service (QoS) features can then operate on the bit settings.

**DSCP and Precedence Values Are Mutually Exclusive**

The **set dscp** command cannot be used with the **set precedence** command to mark the *same* packet. The two values, DSCP and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

**Precedence Value and Queueing**

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain); data then is queued according to the precedence. Weighted fair queueing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Random Early Detection (WRED) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

**Use of the "from-field" Packet-Marking Category**

If you are using this command as part of the Enhanced Packet Marking feature, it can specify the "from-field" packet-marking category to be used for mapping and setting the DSCP value. The "from-field" packet-marking categories are as follows:

- Class of service (CoS)
- QoS group

If you specify a "from-field" category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the "from-field" category as the DSCP value. For instance, if you configure the **set dscp cos** command, the CoS value will be copied and used as the DSCP value.

**Note** The CoS field is a 3-bit field, and the DSCP field is a 6-bit field. If you configure the **set dscp cos**command, only the three bits of the CoS field will be used.

If you configure the **set dscp qos-group** command, the QoS group value will be copied and used as the DSCP value.

The valid range for the DSCP value is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the **set dscp qos-group** command, note the following points:

- If a QoS group value falls within both value ranges (for example, 44), the packet-marking value will be copied and the packets will be marked.
- If QoS group value exceeds the DSCP range (for example, 77), the packet-marking value will not be copied and the packet will not be marked. No action is taken.

**Setting DSCP Values in IPv6 Environments**

When this command is used in IPv6 environments, the default match occurs on both IPv4 and IPv6 packets. However, the actual packets set by this function are only those that meet the match criteria of the class map containing this function.

**Setting DSCP Values for IPv6 Packets Only**

To set DSCP values for IPv6 values only, you must also use the **match protocol ipv6** command. Without that command, the precedence match defaults to match both IPv4 and IPv6 packets.

**Setting DSCP Values for IPv4 Packets Only**

To set DSCP values for IPv4 values only, you must use the appropriate **match ip** command. Without this command, the class map may match both IPv6 and IPv4 packets, depending on the other match criteria, and the DSCP values may act upon both types of packets.

## Examples

## Examples

In the following example, the policy map called “policy1” is created to use the packet-marking values defined in a table map called “table-map1”. The table map was created earlier with the **table-map** (value mapping)command. For more information about the **table-map** (value mapping) command, see the **table-map** (value mapping) command page.

In this example, the DSCP value will be set according to the CoS value defined in the table map called “table-map1”.

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# set dscp cos table table-map1
Router(config-pmap-c)#end
```

The **set dscp** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not yet attached to an interface. For information on attaching a service policy to an interface, see the “Modular Quality of Service Command-Line Interface” section of the *Quality of Service Solutions Configuration Guide* .

## Related Commands

| Command | Description |
|---|---|
| **match ip dscp** | Identifies one or more DSCP, AF, and CS values as a match criterion. |

| Command | Description |
|---|---|
| **match protocol** | Configures the match criteria for a class map on the basis of the specified protocol. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **set cos** | Sets the Layer 2 CoS value of an outgoing packet. |
| **set precedence** | Sets the precedence value in the packet header. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map class** | Displays the configuration for the specified class of the specified policy map. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |
| **show table-map** | Displays the configuration of a specified table map or all table maps. |
| **table-map (value mapping)** | Creates and configures a mapping table for mapping and converting one packet-marking value to another. |

# set fr-de

To change the discard eligible (DE) bit setting in the address field of a Frame Relay frame to 1 for all traffic leaving an interface, use the **setfr-de**command in policy-map class command. To remove the DE bit setting, use the **no** form of thiscommand.

**set fr-de**

**no set fr-de**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The DE bit is usually set to 0. This command changes the DE bit setting to 1.

## Command Modes

Policy-map class

## Command History

| Release | Modification |
|---|---|
| 12.2(2)T | This command was introduced. |
| 12.2(31)SB2 | This command was integrated in Cisco IOS Release 12.2(31)SB2, and introduced on the PRE3 for the Cisco 10000 series router. |

## Usage Guidelines

To disable this command in a traffic policy, use the **nosetfr-de** command in policy-map class configuration mode of the traffic policy.

If the DE bit is already set to 1, no changes are made to the frame.

## Examples

The following example shows how to set the DE bit using the **setfr-de** command in the traffic policy. The router sets the DE bit of outbound packets belonging to the ip-precedence class.

```
Router(config)#
class-map ip-precedence
Router(config-cmap)#
match ip precedence 0 1
Router(config-cmap)#
exit
Router(config)#
policy-map set-de
Router(config-pmap)#
class ip-precedence
Router(config-pmap-c)#
set fr-de
Router(config-pmap-c)#
exit
Router(config-pmap)#
exit
Router(config)# interface serial 1/0/0
```

```
Router(config-if)# no ip address
Router(config-if)# encapsulation frame-relay
Router(config-if)#
interface serial 1/0/0.1
Router(config-subif)# ip address 10.1.1.1 255.255.255.252
Router(config-subif)# no ip directed-broadcast
Router(config-subif)#
service-policy output set-de
```

## Related Commands

| Command | Description |
|---|---|
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |

# set ip dscp

The **setipdscp** command is replaced by the set dscp command. See the set dscp command for more information.

# set ip dscp (policy-map configuration)

To mark a packet by setting the IP differentiated services code point (DSCP) value in the type of service (ToS) byte, use the **setipdscp** command in policy-map configuration mode. To remove a previously set IP DSCP value, use the **no** form of this command.

**set ip dscp** *ip-dscp-value*

**no set ip dscp** *ip-dscp-value*

## Syntax Description

| | |
|---|---|
| *ip-dscp-value* | IP DSCP value; valid values are from 0 to 63. See the "Usage Guidelines" section for additional information. |

## Command Default

This command has no default settings.

## Command Modes

Policy-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 15.1(2)SNH | This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers. |

## Usage Guidelines

You can enter reserved keywords **EF** (expedited forwarding), **AF11** (assured forwarding class AF11), and **AF12** (assured forwarding class AF12) instead of numeric values for *ip-dscp-value*.

After the IP DSCP bit is set, other quality of service (QoS) features can operate on the bit settings.

You cannot mark a packet by the IP precedence using the**setipprecedence**(policy-map configuration) command and then mark the same packet with an IP DSCP value using the **setipdscp**command.

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set IP precedence at the edge of the network (or administrative domain); data is queued based on the precedence. Weighted Fair Queueing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Random Early Detection (WRED) ensures that high-precedence traffic has lower loss rates than other traffic during traffic congestion.

The **setipprecedence** (policy-map configuration) command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not attached to an interface or to an ATM virtual circuit. See the**service-policy** command for information on attaching a service policy to an interface.

When configuring policy-map class actions, note the following:

- For hardware-switched traffic, Policy Feature Card (PFC) QoS does not support the **bandwidth**, **priority**, **queue-limit**, or **random-detect** policy-map class commands. You can configure these commands because they can be used for software-switched traffic.
- PFC QoS does not support the **setmpls**or **setqos-group** policy-map class commands.
- PFC QoS supports the **setipdscp** and **setipprecedence** policy-map class commands (see the "Configuring Policy Map Class Marking" section in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*).
- You cannot do all three of the following in a policy-map class:
  - Mark traffic with the **setipdscp** or **setipprecedence** (policy-map configuration) commands
  - Configure the trust state
  - Configure policing

In a policy-map class, you can either mark traffic with the **setipdscp** or **setipprecedence**(policy-map configuration) commands or do one or both of the following:

- • Configure the trust state
  - Configure policing

## Examples

This example shows how to set the IP DSCP ToS byte to 8 in the policy map called policy1:

```
Router(config)#
policy-map policy1
Router(config-cmap)#
class class1
Router(config-cmap)#
set ip dscp 8
```

All packets that satisfy the match criteria of class1 are marked with the IP DSCP value of 8. How packets that are marked with the IP DSCP value of 8 are treated is determined by the network configuration.

This example shows that after you configure the settings that are shown for voice packets at the edge of the network, all intermediate routers are then configured to provide low-latency treatment to the voice packets:

```
Router(config)# class-map voice
Router(config-cmap)# match ip dscp ef
Router(config)# policy qos-policy
Router(config-cmap)# class voice
Router(config-cmap)# priority 24
```

## Related Commands

| Command | Description |
|---|---|
| **policy-map** | Accesses QoS policy-map configuration mode to configure the QoS policy map. |
| **service-policy** | Attaches a policy map to an interface. |
| **show policy-map** | Displays information about the policy map. |
| **show policy-map interface** | Displays the statistics and the configurations of the input and output policies that are attached to an interface. |

# set ip dscp tunnel

To set the differentiated services code point (DSCP) value in the tunnel header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) or generic routing encapsulation (GRE) tunneled packet for tunnel marking, use the **set ip dscp tunnel** command in policy-map class configuration mode. To disable this functionality, use the **no** form of this command.

**set ip dscp tunnel** *dscp-value*

**no set ip dscp tunnel** *dscp-value*

## Syntax Description

| | |
|---|---|
| *dscp-value* | Number from 0 to 63 that identifies the tunnel header value. The following reserved keywords can be specified instead of numeric values:<br>• **EF** (expedited forwarding)<br>• **AF11** (assured forwarding class AF11) |

## Command Default

The DSCP value is not set.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.0(28)S | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 12.4(15)T2 | This command was integrated into Cisco IOS Release 12.4(15)T2, and support for marking GRE-tunneled packets was included.<br>**Note** For this release, marking GRE-tunneled packets is supported only on platforms equipped with a Cisco MGX Route Processor Module (RPM-XF). |
| 12.2(33)SB | Support for marking GRE-tunneled packets was included, and support for the Cisco 7300 series router was added. |
| Cisco IOS XE Release 3.5S | This command was integrated into Cisco IOS XE Release 3.5S and was implemented on the Cisco ASR 1000 series router. |

## Usage Guidelines

It is possible to configure L2TPv3 (or GRE) tunnel marking and the **ip tos** commands at the same time. However, Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) (L2TPv3 or GRE) tunnel marking has higher priority over **ip tos** commands, meaning that tunnel marking always rewrites the IP header of the tunnel packet and overwrites the values set by ip tos commands. The order of enforcement is as follows when these commands are used simultaneously:

1. **set ip dscp tunnel** or **set ip precedence tunnel** (L2TPv3 or GRE tunnel marking)
2. **ip tos reflect**
3. **ip tos** *tos-value*

We recommend that you configure only L2TPv3 (or GRE) tunnel marking and reconfigure any peers configured with the **ip tos** commands to use L2TPv3 (or GRE) tunnel marking.

**Note** For Cisco IOS Release 12.4(15)T2, marking GRE-tunneled packets is supported only on platforms equipped with a Cisco RPM-XF.

## Examples

The following example shows the **set ip dscp tunnel** command used in a tunnel marking configuration. In this example, a class map called "class-cl" has been configured to match traffic on the basis of the DSCP value setting. Also, a policy map called "policy1" has been created within which the **setipdscptunnel** command has been configured.

```
Router> enable
Router# configure terminal
Router(config)# class-map class-c1
Router(config-cmap)# match ip dscp 0
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class tunnel
Router(config-pmap-c)# set ip dscp tunnel 5
Router(config-pmap-c)# end
```

**Note** You must still attach a policy map to an interface or ATM PVC using the **service-policy** command. Tunnel marking policies can be applied as an ingress policy on the ingress physical interface of a Service Provider Edge (SPE) router or as an egress policy on the tunnel interface. For more information about attaching a policy map to an interface or ATM PVC, see the "Applying QoS Features Using the MQC" module of the *Cisco IOS Quality of Service Solutions Configuration Guide.*

## Related Commands

| Command | Description |
|---|---|
| **ip tos** | Specifies the ToS level for IP traffic. |
| **set ip precedence tunnel** | Sets the precedence value in the header of an L2TPv3 or GRE tunneled packet. |

# set ip precedence (policy-map configuration)

To set the precedence value in the IP header, use the **setipprecedence** command in policy-map configuration mode. To leave the precedence value at the current setting, use the **no** form of this command.

**set ip precedence** *ip-precedence-value*

**no set ip precedence**

## Syntax Description

| | |
|---|---|
| *ip-precedence-value* | Precedence-bit value in the IP header; valid values are from 0 to 7. See the table below for a list of value definitions. |

## Command Default

This command is disabled by default.

## Command Modes

Policy-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 15.1(2)SNH | This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers. |

## Usage Guidelines

The table below lists the value definitions for precedence values in the IP header. They are listed from least to most important.

***Table 41: Value Definitions for IP Precedence***

| Values | Definitions |
|---|---|
| | routine |
| | priority |
| | immediate |

| Values | Definitions |
|---|---|
| | flash |
| | flash-override |
| | critical |
| | internet |
| | network |

After the IP precedence bits are set, other quality of service (QoS) features, such as Weighted Fair Queueing (WFQ) and Weighted Random Early Detection (WRED), operate on the bit settings.

The network priorities (or some type of expedited handling) mark traffic through the application of WFQ or WRED at points downstream in the network. Typically, you set IP precedence at the edge of the network (or administrative domain); data is queued based on the precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during traffic congestion.

The **setipprecedence**command is applied when you create a service policy in policy-map configuration mode. This service policy is not attached to an interface or to an ATM virtual circuit. See the **service-policy**command for information on attaching a service policy to an interface.

## Examples

This example shows how to set the IP precedence to 5 for packets that satisfy the match criteria of the class map called class1:

```
Router(config)#
policy-map policy1
Router(config-pmap)#
class class1
Router(config-pmap-c)#
set ip precedence 5
```

All packets that satisfy the match criteria of class1 are marked with the IP precedence value of 5. How packets that are marked with the IP-precedence value of 5 are treated is determined by the network configuration.

## Related Commands

| Command | Description |
|---|---|
| **policy-map** | Accesses QoS policy-map configuration mode to configure the QoS policy map. |
| **service-policy** | Attaches a policy map to an interface. |
| **show policy-map** | Displays information about the policy map. |

| Command | Description |
| --- | --- |
| **show policy-map interface** | Displays the statistics and the configurations of the input and output policies that are attached to an interface. |

# set ip precedence (policy-map)

The **setipprecedence**(policy-map) command is replaced by the set precedence command. See the set precedence command for more information.

# set ip precedence (route-map)

To set the precedence value (and an optional IP number or IP name) in the IP header, use the **setipprecedence** command in route-map configuration mode. To leave the precedence value unchanged, use the **no** form of this command.

**set ip precedence** [*number*| *name*]

**no set ip precedence**

## Syntax Description

| | |
|---|---|
| *number* *name* | (Optional) A number or name that sets the precedence bits in the IP header. The values for the *number* argument and the corresponding *name* argument are listed in the table below from least to most important. |

## Command Default

Disabled

## Command Modes

Route-map configuration

## Command History

| Release | Modification |
|---|---|
| 11.0 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

The table below lists the values for the *number* argument and the corresponding *name* argument for precedence values in the IP header. They are listed from least to most important.

***Table 42: Number and Name Values for IP Precedence***

| Number | Name |
|---|---|
| 0 | **routine** |
| 1 | **priority** |
| 2 | **immediate** |

| Number | Name |
|---|---|
| 3 | **flash** |
| 4 | **flash-override** |
| 5 | **critical** |
| 6 | **internet** |
| 7 | **network** |

You can set the precedence using either a number or the corresponding name. Once the IP Precedence bits are set, other QoS services such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) then operate on the bit settings.

The network gives priority (or some type of expedited handling) to marked traffic through the application of WFQ or WRED at points downstream in the network. Typically, you set IP Precedence at the edge of the network (or administrative domain); data then is queued based on the precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during times of congestion.

The mapping from arguments such as **routine** and **priority** to a precedence value is useful only in some instances. That is, the use of the precedence bit is evolving. You can define the meaning of a precedence value by enabling other features that use the value. In the case of the high-end Internet QoS available from Cisco, IP Precedences can be used to establish classes of service that do not necessarily correspond numerically to better or worse handling in the network.

Use the **route-map**(IP)global configuration command with the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another, or for policy routing. Each **route-map**command has an associated list of **match** and **set** commands. The **match** commands specify the match criteria--the conditions under which redistribution or policy routing is allowed for the current **route-map** command. The **set** commands specify the set actions--the particular redistribution or policy routing actions to perform if the criteria enforced by the **match** commands are met. The **noroute-map** command deletes the route map.

The **set**route-map configuration commands specify the redistribution set actions to be performed when all of the match criteria of a route map are met.

## Examples

The following example sets the IP Precedence to 5 (critical) for packets that pass the route map match:

```
interface serial 0
 ip policy route-map texas
route-map texas
match length 68 128
set ip precedence 5
```

## Related Commands

| Command | Description |
|---|---|
| **fair-queue (WFQ)** | Enables WFQ for an interface. |

| Command | Description |
|---|---|
| **ip policy route-map** | Identifies a route map to use for policy routing on an interface. |
| **random-detect dscp** | Changes the minimum and maximum packet thresholds for the DSCP value. |
| **send qdm message** | Configures CAR and DCAR policies. |
| **route-map (IP)** | Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing. |
| **traffic-shape adaptive** | Configures a Frame Relay subinterface to estimate the available bandwidth when BECN signals are received. |
| **traffic-shape fecn-adapt** | Replies to messages with the FECN bit (which are set with TEST RESPONSE messages with the BECN bit set). |
| **traffic-shape group** | Enables traffic shaping based on a specific access list for outbound traffic on an interface. |
| **traffic-shape rate** | Enables traffic shaping for outbound traffic on an interface. |

# set ip precedence tunnel

To set the precedence value in the header of a Layer 2 Tunnel Protocol Version 3 (L2TPv3) or generic routing encapsulation (GRE) tunneled packet for tunnel marking, use the **set ip precedence tunnel** command in policy-map class configuration mode. To disable this functionality, use the **no** form of this command.

**set ip precedence tunnel** *precedence-value*

**no set ip precedence tunnel** *precedence-value*

## Syntax Description

| | |
|---|---|
| *precedence-value* | Number from 0 to 7 that identifies the precedence value of the tunnel header. |

## Command Default

The precedence value is not set.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.0(28)S | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 12.4(15)T2 | This command was integrated into Cisco IOS Release 12.4(15)T2, and support for marking GRE-tunneled packets was included.<br>**Note** For this release, marking GRE-tunneled packets is supported only on platforms equipped with a Cisco MGX Route Processor Module (RPM-XF). |
| 12.2(33)SB | Support for marking GRE-tunneled packets was included, and support for the Cisco 7300 series router was added. |
| Cisco IOS XE Release 3.5S | This command was integrated into Cisco IOS XE Release 3.5S and was implemented on the Cisco ASR 1000 Series Router. |

## Usage Guidelines

It is possible to configure L2TPv3 (or GRE) tunnel marking and the **ip tos** commands at the same time. However, Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC) (L2TPv3 or GRE) tunnel marking has higher priority over **ip tos** commands, meaning that tunnel marking always rewrites the IP header of the tunnel packet and overwrites the values set by ip tos commands. The order of enforcement is as follows when these commands are used simultaneously:

1. **set ip dscp tunnel** or **set ip precedence tunnel** (L2TPv3 or GRE tunnel marking)
2. **ip tos reflect**
3. **ip tos** *tos-value*

We recommend that you configure only L2TPv3 (or GRE) tunnel marking and reconfigure any peers configured with the **ip tos** commands to use L2TPv3 (or GRE) tunnel marking.

**Note** For Cisco IOS Release 12.4(15)T2, marking GRE-tunneled packets is supported only on platforms equipped with a Cisco RPM-XF.

## Examples

The following example shows the **set ip precedence tunnel** command used in a tunnel marking configuration. In this example, a class map called "MATCH_PREC" has been configured to match traffic on the basis of the precedence value. Also, a policy map called "TUNNEL_MARKING" has been created within which the **set ip precedence tunnel** command has been configured.

```
Router> enable
Router# configure terminal
Router(config)# class-map match-any MATCH_PREC
Router(config-cmap)# match ip precedence 0
Router(config-cmap)# exit
Router(config)# policy-map TUNNEL_MARKING
Router(config-pmap)# class MATCH_PREC
Router(config-pmap-c)# set ip precedence tunnel 3
Router(config-pmap-c)# end
```

**Note** You must still attach a policy map to an interface or ATM PVC using the **service-policy** command.Tunnel marking policies can be applied as an ingress policy on the ingress physical interface of a Service Provider Edge (SPE) router or as an egress policy on the tunnel interface. For more information about attaching a policy map to an interface or ATM PVC, see the "Applying QoS Features Using the MQC" module of the *Cisco IOS Quality of Service Solutions Configuration Guide.*

## Related Commands

| Command | Description |
|---|---|
| **ip tos** | Specifies the ToS level for IP traffic in the TN3270 server. |
| **set ip dscp tunnel** | Sets the DSCP value in the header of an L2TPv3 tunneled packet. |

# set ip tos (route-map)

To set the type of service (ToS) bits in the header of an IP packet, use the **setiptos** command in route-map configuration mode. To leave the ToS bits unchanged, use the **no** form of this command.

**set ip tos** [*tos-bit-value*| **max-reliability**| **max-throughput**| **min-delay**| **min-monetary-cost**| **normal**]

**no set ip tos**

## Syntax Description

| | |
|---|---|
| *tos-bit-value* | (Optional) A value (number) from 0 to 15 that sets the ToS bits in the IP header. See the table below for more information. |
| **max-reliability** | (Optional) Sets the maximum reliability ToS bits to 2. |
| **max-throughput** | (Optional) Sets the maximum throughput ToS bits to 4. |
| **min-delay** | (Optional) Sets the minimum delay ToS bits to 8. |
| **min-monetary-cost** | (Optional) Sets the minimum monetary cost ToS bits to 1. |
| **normal** | (Optional) Sets the normal ToS bits to 0. |

## Command Default

Disabled

## Command Modes

Route-map configuration

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.4T | This command was integrated into Cisco IOS Release 12.4T. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command allows you to set four bits in the ToS byte header. The table below shows the format of the four bits in binary form.

***Table 43: ToS Bits and Description***

| T3 | T2 | T1 | T0 | Description |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 normal forwarding |
| 0 | 0 | 0 | 1 | 1 minimum monetary cost |
| 0 | 0 | 1 | 0 | 2 maximum reliability |
| 0 | 1 | 0 | 0 | 4 maximum throughput |
| 1 | 0 | 0 | 0 | 8 minimum delay |

The T3 bit sets the delay. Setting T3 to 0 equals normal delay, and setting it to 1 equals low delay.

The T2 bit sets the throughput. Setting this bit to 0 equals normal throughput, and setting it to 1 equals maximum throughput. Similarly, the T1 and T0 bits set reliability and cost, respectively. Therefore, as an example, if you want to set a packet with the following requirements:

minimum delay T3 = 1

normal throughput T2 = 0

normal reliability T1 = 0

minimum monetary cost T0 = 1

You would set the ToS to 9, which is 1001 in binary format.

Use the **route-map** (IP) global configuration command with the **match** and **set** (route-map) configuration commands to define the conditions for redistributing routes from one routing protocol into another, or for policy routing. Each **route-map** command has an associated list of **match** and**set**commands. The **match** commands specify the match criteria--the conditions under which redistribution or policy routing is allowed for the current route-map command. The**set** commands specify the set actions--the particular redistribution or policy routing actions to perform if the criteria enforced by the match commands are met. The **noroute-map** command deletes the route map.

The **set** (route-map) commands specify the redistribution set actions to be performed when all of the match criteria of a route map are met.

## Examples

The following example sets the IP ToS bits to 8 (minimum delay as shown in set ip tos (route-map), on page 1095) for packets that pass the route-map match:

```
interface serial 0
 ip policy route-map texas
!
```

```
route-map texas
  match length 68 128
  set ip tos 8
!
```

## Related Commands

| Command | Description |
|---|---|
| **ip policy route-map** | Identifies a route map to use for policy routing on an interface. |
| **route-map (IP)** | Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing. |

# set precedence

To set the precedence value in the packet header, use the **set precedence** command in policy-map class configuration mode. To remove the precedence value, use the **no** form of this command.

### Supported Platforms Other Than Cisco 10000 Series Routers

**set precedence** {*precedence-value*| *from-field* [**table** *table-map-name*]}

**no set precedence** {*precedence-value*| *from-field* [**table** *table-map-name*]}

### Cisco 10000 Series Routers

**set precedence** {*precedence-value*}

**no setprecedence** {*precedence-value*}

## Syntax Description

| | |
|---|---|
| *precedence-value* | A number from 0 to 7 that sets the precedence bit in the packet header. |
| *from-field* | Specific packet-marking category to be used to set the precedence value of the packet. If you are using a table map for mapping and converting packet-marking values, this argument value establishes the "map from" packet-marking category. Packet-marking category keywords are as follows:<br>• **cos**<br>• **qos-group** |
| **table** | (Optional) Indicates that the values set in a specified table map will be used to set the precedence value. |
| *table-map-name* | (Optional) Name of the table map used to specify a precedence value based on the class of service (CoS) value. The name can be a maximum of 64 alphanumeric characters. |

## Command Default

This command is disabled.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. This command replaces the **set ip precedence**command. |
| 12.0(28)S | Support for this command in IPv6 was added on the Cisco 12000 series Internet routers. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series router. |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 Series Routers. |

## Usage Guidelines

### Command Compatibility

If a router is loaded with an image from Cisco IOS Release 12.2(13)T that contained an old configuration, the **setip precedence** command is still recognized. However, the **set precedence** command will be used in place of the **set ip precedence** command.

The **set precedence** command cannot be used with the**set dscp** command to mark the *same* packet. The two values, differentiated services code point (DSCP) and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

### Bit Settings

Once the precedence bits are set, other quality of service (QoS) features such as weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) then operate on the bit settings.

### Precedence Value

The network gives priority (or some type of expedited handling) to marked traffic through the application of WFQ or WRED at points downstream in the network. Typically, you set the precedence value at the edge of the network (or administrative domain); data then is queued according to the specified precedence. WFQ can speed up handling for certain precedence traffic at congestion points. WRED can ensure that certain precedence traffic has lower loss rates than other traffic during times of congestion.

### Using This Command with the Enhanced Packet Marking Feature

If you are using this command as part of the Enhanced Packet Marking feature, you can use this command to specify the “from-field” packet-marking category to be used for mapping and setting the precedence value. The “from-field” packet-marking categories are as follows:

- CoS
- QoS group

If you specify a “from-field” category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the “from-field” category as the precedence value. For instance, if you configure the **set precedence cos** command, the CoS value will be copied and used as the precedence value.

You can do the same for the QoS group-marking category. That is, you can configure the **set precedence qos-group** command, and the QoS group value will be copied and used as the precedence value.

The valid value range for the precedence value is a number from 0 to 7. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the **setprecedenceqos-group** command, note the following points:

- If a QoS group value falls within both value ranges (for example, 6), the packet-marking value will be copied and the packets will be marked.
- If QoS group value exceeds the precedence range (for example, 10), the packet-marking value will not be copied, and the packet will not be marked. No action is taken.

### Precedence Values in IPv6 Environments

When this command is used in IPv6 environments, it can set the value in both IPv4 and IPv6 packets. However, the actual packets set by this function are only those that meet the match criteria of the class map containing this function.

### Setting Precedence Values for IPv6 Packets Only

To set the precedence values for IPv6 packets only, the **match protocol ipv6** command must also be used in the class map that classified packets for this action. Without the **match protocol ipv6**command, the class map may classify both IPv6 and IPv4 packets (depending on other match criteria), and the **set precedence** command will act upon both types of packets.

### Setting Precedence Values for IPv4 Packets Only

To set the precedence values for IPv4 packets only, use a command involving the **ip** keyword like the **match ip precedence** or **match ip dscp**command or include the **match protocol ip** command along with the others in the class map. Without the additional **ip** keyword, the class map may match both IPv6 and IPv4 packets (depending on the other match criteria) and the **set precedence**or **set dscp** commandmay act upon both types of packets.

## Examples

In the following example, the policy map named policy-cos is created to use the values defined in a table map named table-map1. The table map named table-map1 was created earlier with the **table-map** (value mapping) command. For more information about the **table-map** (value mapping) command, see the**table-map** (value mapping) command page.

In this example, the precedence value will be set according to the CoS value defined in table-map1.

```
Router(config)# policy-map policy-cos
Router(config-pmap)# class class-default
Router(config-pmap-c)# set precedence cos table table-map1
Router(config-pmap-c)# end
```

The **set precedence** command is applied when you create a service policy in QoS policy-map configuration mode. This service policy is not yet attached to an interface or to an ATM virtual circuit. For information on attaching a service policy to an interface, refer to the “Modular Quality of Service Command-Line Interface Overview” chapter of the *Quality of Service Solutions Configuration Guide.*

## Related Commands

| Command | Description |
|---|---|
| **match dscp** | Identifies a specific IP DSCP value as a match criterion. |

| Command | Description |
|---|---|
| **match precedence** | Identifies IP precedence values as match criteria. |
| **match protocol** | Configures the match criteria for a class map on the basis of the specified protocol. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **set cos** | Sets the Layer 2 CoS value of an outgoing packet. |
| **set dscp** | Marks a packet by setting the Layer 3 DSCP value in the ToS byte. |
| **set qos-group** | Sets a group ID that can be used later to classify packets. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the configuration for all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |
| **show table-map** | Displays the configuration of a specified table map or all table maps. |
| **table-map (value mapping)** | Creates and configures a mapping table for mapping and converting one packet-marking value to another. |

# set qos-group

To set a quality of service (QoS) group identifier (ID) that can be used later to classify packets, use the **setqos-group** command in policy-map class configuration mode. To remove the group ID, use the **no** form of this command.

### Supported Platforms Except the Cisco 10000 Series Router

**set qos-group** {*group-id*| *from-field* [**table** *table-map-name*]}

**no set qos-group** {*group-id*| *from-field* [**table** *table-map-name*]}

### Cisco 10000 Series Router

**set qos-group** *group-id*

**no set qos-group** *group-id*

## Syntax Description

| | |
|---|---|
| *group-id* | Group ID number in the range from 0 to 99. |
| *from-field* | Specific packet-marking category to be used to set the QoS group value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the "map from" packet-marking category. Packet-marking category keywords are as follows:<br>• **cos** --Specifies that the QoS group value is set from the packet's original 802.1P class of service (CoS) field.<br>• **precedence** --Specifies that the QoS group value is set from the packet's original IP precedence field.<br>• **dscp** --Specifies that the QoS group value is set from the packet's original Differentiated Services Code Point (DSCP) field.<br>• **mpls exp topmost** --Specifies that the QoS group value is set from the packet's original topmost MPLS EXP field . |
| **table** *table-map-name* | (Optional) Used in conjunction with the *from-field*argument. Indicates that the values set in a table map specified by *table-map-name*will be used to set the QoS group value. |

## Command Default

No group ID is specified.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 11.1CC | This command was introduced. |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE. |
| 12.0(17)SL | This command was introduced on the Cisco 10000 series router. |
| 12.2(13)T | This command can now be used with the **random-detectdiscard-class-based** command, and this command was modified for the Enhanced Packet Marking feature. A mapping table (table map) can now be used to convert and propagate packet-marking values. |
| 12.2(18)SXE | This command was integrated into Cisco IOS 12.2(18)SXE, and the **cos** keyword was added. |
| 12.2(31)SB | This command was integrated into Cisco IOS Release 12.2(31)SB. |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers. |
| 15.1(2)SNH | This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers. |

## Usage Guidelines

The **setqos-group** command allows you to associate a group ID with a packet. The group ID can be used later to classify packets into QoS groups based as prefix, autonomous system, and community string.

A QoS group and discard class are required when the input per-hop behavior (PHB) marking will be used for classifying packets on the output interface.

**Using This Command with the Enhanced Packet Marking Feature**

If you are using this command as part of the Enhanced Packet Marking feature, you can use this command to specify the "from-field" packet-marking category to be used for mapping and setting the precedence value.

If you specify a "from-field" category but do not specify the **table** keyword and the applicable *table-map-name* argument, the default action will be to copy the value associated with the "from-field" category as the precedence value. For instance, if you enter **setqos-grouppprecedence**, the precedence value will be copied and used as the QoS group value.

A packet is marked with a QoS group value only while it is being processed within the router. The QoS group value is not included in the packet's header when the packet is transmitted over the output interface. However, the QoS group value can be used to set the value of a Layer 2 or Layer 3 field that is included as part of the packet's headers (such as the MPLS EXP, CoS, and DSCP fields).

**Note** The **setqos-groupcos** and **setqos-grouppprecedence** commands are equivalent to the **mlsqostrustcos** and **mlsqostrustprec** commands.

**Tip** The **setqos-group** command cannot be applied until you create a service policy in policy-map configuration mode and then attach the service policy to an interface or ATM virtual circuit (VC). For information on attaching a service policy, refer to the "Modular Quality of Service Command-Line Interface Overview" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

## Examples

The following example shows how to set the QoS group to 1 for all packets that match the class map called class 1. These packets are then rate limited on the basis of the QoS group ID.

```
Router(config)#

policy-map policy1
Router(config-pmap)#

class class1
Router(config-pmap-c)#

set qos-group 1
Router(config-pmap-c)#

end
```

The following example shows how to set the QoS group value based on the packet's original 802.1P CoS value:

```
Router(config)# policy map policy1

Router(config-pmap)# class class-default

Router(config-pmap-c)#

set qos-group cos

Router(config-pmap-c)#

end
```

## Examples

The following example shows how to set the QoS group value based on the values defined in a table map called table-map1. This table map is configured in a policy map called policy1. Policy map policy1 converts and propagates the QoS value according to the values defined in table-map1.

In this example, the QoS group value will be set according to the precedence value defined in table-map1.

```
Router(config)# policy map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)#

set qos-group precedence table table-map1
Router(config-pmap-c)#

end
```

## Related Commands

| Command | Description |
|---|---|
| **match input vlan** | Configures a class map to match incoming packets that have a specific VLAN ID. |
| **match qos-group** | Identifies a specified QoS group value as a match criterion. |
| **mls qos trust** | Sets the trusted state of an interface to determine which incoming QoS field on a packet, if any, should be preserved. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

# set vlan inner

To mark the bridged packets in the permanent virtual circuit (PVC) with a specific virtual LAN identifier (VLAN ID), use the **setvlaninner** command in policy-map class configuration mode. To disable this configuration, use the **no** form of this command.

**set vlan inner** *vlan-number*

**no set vlan inner** *vlan-number*

## Syntax Description

| | |
|---|---|
| *vlan-number* | Number that identifies the VLAN. The range is from 1 to 4094. |

## Command Default

The bridged packets are marked with the default VLAN ID as configured using the **bridge-dot1qencap** command.

## Command Modes

Policy-map class configuration mode (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 15.1(2)T | This command was introduced. |

## Usage Guidelines

Although multiple VLANs are allowed under a single PVC, the locally generated packets including the Address Resolution Protocol (ARP) packets are sent out with the class default VLAN ID only. The **setvlaninner** command must be applied within the class default.

## Examples

The following example shows how to mark the inner VLAN ID as 2 for bridged packets in the 802.1Q tag:

```
Router(config)# policy-map egress-policy
Router(config-pmap)# class egress
Router(config-pmap-c)# set vlan inner 2
```

## Related Commands

| Command | Description |
|---|---|
| **bridge-dot1q encap** | Adds a VLAN ID at an ATM PVC over an ATM xDSL link. |

# shape

To specify average or peak rate traffic shaping, use the **shape** command in class-map configuration mode. To remove traffic shaping, use the **no** form of this command.

**shape** {**average**| **peak**} *cir* [ *bc* ] [ *be* ]

**no shape** {**average**| **peak**} *cir* [ *bc* ] [ *be* ]

## Syntax Description

| | |
|---|---|
| **average** | Specifies average rate shaping. |
| **peak** | Specifies peak rate shaping. |
| *cir* | Committed information rate (CIR), in bits per second (bps). |
| *bc* | (Optional) Committed Burst size, in bits. |
| *be* | (Optional) Excess Burst size, in bits. |

## Command Default

Average or peak rate traffic shaping is not specified.

## Command Modes

Class-map configuration (config-cmap)

## Command History

| Release | Modification |
|---|---|
| 12.1(2)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1(1)T | This command was modified. The allowed values for the cir argument were changed. The value must be between 8,000 and 1,000,000,000 bps. |

## Usage Guidelines

Traffic shaping limits the rate of transmission of data. In addition to using a specifically configured transmission rate, you can use Generic Traffic Shaping (GTS) to specify a derived transmission rate based on the level of congestion.

You can specify two types of traffic shaping; average rate shaping and peak rate shaping. Average rate shaping limits the transmission rate to the CIR. Using the CIR ensures that the average amount of traffic being sent conforms to the rate expected by the network.

Peak rate shaping configures the router to send more traffic than the CIR. To determine the peak rate, the router uses the following formula:

peak rate = CIR(1 + Be / Bc)

where:

- Be is the Excess Burst size.
- Bc is the Committed Burst size.

Peak rate shaping allows the router to burst higher than average rate shaping. However, using peak rate shaping, the traffic sent above the CIR (the delta) could be dropped if the network becomes congested.

If your network has additional bandwidth available (over the provisioned CIR) and the application or class can tolerate occasional packet loss, that extra bandwidth can be exploited through the use of peak rate shaping. However, there may be occasional packet drops when network congestion occurs. If the traffic being sent to the network must strictly conform to the configured network provisioned CIR, then you should use average traffic shaping.

## Examples

The following example shows how to configure average rate shaping to ensure a bandwidth of 256 kbps:

```
shape average 256000
```

The following example shows how to configure peak rate shaping to ensure a bandwidth of 300 kbps but allow throughput up to 512 kbps if enough bandwidth is available on the interface:

```
bandwidth 300
shape peak 512000
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map. |
| **class (policy-map)** | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **shape max-buffers** | Specifies the maximum number of buffers allowed on shaping queues. |

# shape (percent)

To specify average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface, use the **shape** command in policy-map class configuration mode. To remove traffic shaping, use the **no** form of this command.

**shape** {**average**| **peak**} **percent** *percentage* [*sustained-burst-in-msec* **ms**] [**be** *excess-burst-in-msec* **ms**] [**bc** *committed-burst-in-msec* **ms**]

**no shape** {**average**| **peak**} **percent** *percentage* [*sustained-burst-in-msec* **ms**] [**be** *excess-burst-in-msec* **ms**] [**bc** *committed-burst-in-msec* **ms**]

## Syntax Description

| | |
|---|---|
| **average** | Specifies average rate traffic shaping. |
| **peak** | Specifies peak rate traffic shaping. |
| **percent** | Specifies that a percent of bandwidth will be used for either the average rate traffic shaping or peak rate traffic shaping. |
| *percentage* | Specifies the bandwidth percentage. Valid range is a number from 1 to 100. |
| *sustained-burst-in-msec* | (Optional) Sustained burst size used by the first token bucket for policing traffic. Valid range is a number from 4 to 200. |
| **ms** | (Optional) Indicates that the burst value is specified in milliseconds (ms). |
| **be** | (Optional) Excess burst (be) size used by the second token bucket for policing traffic. |
| *excess-burst-in-msec* | (Optional) Specifies the be size in milliseconds. Valid range is a number from 0 to 200. |
| **bc** | (Optional) Committed burst (bc) size used by the first token bucket for policing traffic. |
| *committed-burst-in-msec* | (Optional) Specifies the bc value in milliseconds. Valid range is a number from 1 to 2000. |

## Command Default

The default bc and be is 4 ms.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.1(2)T | This command was introduced. |
| 12.2(13)T | This command was modified for the Percentage-Based Policing and Shaping feature. |
| 12.0(28)S | The command was integrated into Cisco IOS Release 12.0(28)S. |
| 12.2(18)SXE | The command was integrated into Cisco IOS Release 12.2(18)SXE. |
| 12.2(28)SB | The command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers. |

## Usage Guidelines

### Committed Information Rate

This command calculates the committed information rate (CIR) on the basis of a percentage of the available bandwidth on the interface. Once a policy map is attached to the interface, the equivalent CIR value in bits per second (bps) is calculated on the basis of the interface bandwidth and the percent value entered with this command. The **showpolicy-mapinterface** command can then be used to verify the CIR bps value calculated.

The calculated CIR bps rate must be in the range of 8000 and 154,400,000 bps. If the rate is less than 8000 bps, the associated policy map cannot be attached to the interface. If the interface bandwidth changes (for example, more is added), the CIR bps values are recalculated on the basis of the revised amount of bandwidth. If the CIR percentage is changed after the policy map is attached to the interface, the bps value of the CIR is recalculated.

### Conform Burst and Peak Burst Sizes in Milliseconds

This command also allows you to specify the values for the conform burst size and the peak burst size in milliseconds. If you want bandwidth to be calculated as a percentage, the conform burst size and the peak burst size must be specified in milliseconds (ms).

The traffic shape converge rate depends on the traffic pattern and the time slice (Tc) parameter, which is directly affected by the bc that you configured. The Tc and the average rate configured are used to calculate bits per interval sustained. Therefore, to ensure that the shape rate is enforced, use a bc that results in a Tc greater than 10 ms.

### Hierarchical Policy Maps

The **shape** (percent) command, when used in “child” (hierarchical) policy maps, is not supported on the Cisco 7500, the Cisco 7200, or lower series routers. Therefore, the **shape** (percent) command cannot be configured for use in hierarchical policy maps on these routers.

### How Bandwidth Is Calculated

The **shape** (percent) command is often used in conjunction with the **bandwidth** and **priority** commands. The **bandwidth** and **priority** commands can be used to calculate the total amount of bandwidth available on an

entity (for example, a physical interface). When the **bandwidth** and **priority** commands calculate the total amount of bandwidth available on an entity, the following guidelines are invoked:

- If the entity is a physical interface, the total bandwidth is the bandwidth on the physical interface.
- If the entity is a shaped ATM permanent virtual circuit (PVC), the total bandwidth is calculated as follows:
  - For a variable bit rate (VBR) virtual circuit (VC), the sustained cell rate (SCR) is used in the calculation.
  - For an available bit rate (ABR) VC, the minimum cell rate (MCR) is used in the calculation.

For more information on bandwidth allocation, see the "Congestion Management Overview" chapter in the *Cisco IOS Quality of Service Solutions Configuration Guide.*

**Note** Thiscommand cannot be used with the **shapeadaptive** command.

## Examples

The following example configures traffic shaping using an average shaping rate on the basis of a percentage of bandwidth. In this example, 25 percent of the bandwidth has been specified. Additionally, an optional be value and bc value (100 ms and 400 ms, respectively) have been specified.

```
Router> enable
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class-map class1
Router(config-pmap-c)# shape average percent 25 20 ms be 100 ms bc 400 ms
Router(config-pmap-c)# end
```

After the policy map and class maps are configured, the policy map is attached to interface as shown in the following example.

```
Router> enable
Router# configure terminal
Router(config)#

interface serial4/0
Router(config-if)#

service-policy input policy1
Router(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map. |
| **class (policy-map)** | Specifies the name of the class whose policy you want to create or change and the default class (commonly known as the class-default class) before you configure its policy. |

| Command | Description |
|---|---|
| **police (percent)** | Configures traffic policing on the basis of a percentage of bandwidth available on an interface. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **priority** | Gives priority to a class of traffic belonging to a policy map. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| shape adaptive | Estimates the available bandwidth by backward explicit congestion notification (BECN) integration while traffic shaping is enabled for a Frame Relay interface or a point-to-point subinterface. |
| **shape max-buffers** | Specifies the maximum number of buffers allowed on shaping queues. |
| **show policy-map interface** | Displays the statistics and the configurations of the input and output policies that are attached to an interface. |

# shape (policy-map class)

To shape traffic to the indicated bit rate according to the algorithm specified or to enable ATM overhead accounting, use the **shape** command in policy-map class configuration mode. To remove shaping and leave the traffic unshaped, use the **no**form of this command.

**shape** {**average**| **peak**} {*mean-rate* [*burst-size* [ *excess-burst-size* ]]| **percent** *percentage* [*burst-size* **ms** [*excess-burst-size* **ms**]]}

**no shape** [**average**| **peak**]

**shape** [**average**| **peak**] *mean-rate* **[burst-size]** [ *excess-burst-size* ] **account** {**qinq**| **dot1q**} **aal5** {*subscriber-encapsulation*| **user-defined** *offset*}

**no shape** [**average**| **peak**] *mean-rate* **[burst-size]** [ *excess-burst-size* ] **account** {**qinq**| **dot1q**} **aal5** {*subscriber-encapsulation*| **user-defined** *offset*}

**shape** [**average**| **peak**] *mean-rate* [ *burst-size* ] [ *excess-burst-size* ] [**account** {**qinq**| **dot1q**} **aal5** *subscriber-encap*]

**no shape** [**average**| **peak**] *mean-rate* [ *burst-size* ] [ *excess-burst-size* ] [**account** {**qinq**| **dot1q**} **aal5** *subscriber-encap*]

**shape [average]** *mean-rate* [ *unit* ] [ *burst-size* ] [ *excess-burst-size* ] [**account** {**qinq**| **dot1q**} **aal5** *subscriber-encapsulation*]

**no shape [average]** *mean-rate* [ *unit* ] [ *burst-size* ] [ *excess-burst-size* ] [**account** {**qinq**| **dot1q**} **aal5** *subscriber-encapsulation*]

**shape [average]** *mean-rate* [ *burst-size* ] [ *excess-burst-size* ] **account** {{**qinq**| **dot1q**} {**aal5**| **aal3**} *subscriber-encapsulation*| **user-defined** *offset* **[atm]**}

**no shape [average]** *mean-rate* [ *burst-size* ] [ *excess-burst-size* ] **account** {{**qinq**| **dot1q**} {**aal5**| **aal3**} *subscriber-encapsulation*| **user-defined** *offset* **[atm]**}

## Syntax Description

| | |
|---|---|
| **average** | Committed Burst (Bc) is the maximum number of bits sent out in each interval. |
| **peak** | Bc + Excess Burst (Be) is the maximum number of bits sent out in each interval. |
| *mean-rate* | Also called committed information rate (CIR). Indicates the bit rate used to shape the traffic, in bps. When this command is used with backward explicit congestion notification (BECN) approximation, the bit rate is the upper bound of the range of bit rates that will be permitted. The value must be between 1,000 and 1,000,000,000 bits per second. |
| *unit* | (Optional) Specifies the unit of the specified bit rate (for example, kbps). |

| | |
|---|---|
| *burst-size* | (Optional) The number of bits in a measurement interval (Bc). Valid values are 256 to 154400000. |
| *excess-burst-size* | (Optional) The acceptable number of bits permitted to go over the Be. Valid values are 0 to 154400000. |
| **percent** | Specifies the percentage of interface bandwidth for committed information rate. |
| *percentage* | Percentage. Valid values are 1 to 100. |
| *burst-size* | (Optional) Sustained burst, in milliseconds. Valid values are 10 to 2000. |
| **ms** | (Optional) Specifies the time, in milliseconds. |
| *excess-burst-size* | (Optional) Excess burst, in milliseconds. Valid values are 10 to 2000. |
| **ms** | (Optional) Specifies the time, in milliseconds. |
| **account** | (Optional) Enables ATM overhead accounting.<br>**Note** This keyword is required if you configure ATM overhead accounting. |
| **qinq** | Specifies queue-in-queue (qinq) encapsulation as the broadband aggregation system (BRAS) to digital subscriber line access multiplexer (DSLAM) encapsulation type for ATM overhead accounting. |
| **dot1q** | Specifies IEEE 802.1Q VLAN encapsulation as the BRAS-DSLAM encapsulation type for ATM overhead accounting. |
| **aal5** | Specifies the ATM Adaptation Layer 5 service for ATM overhead accounting. AAL5 supports connection-oriented variable bit rate (VBR) services. |
| **aal3** | Specifies the ATM Adaptation Layer 5 that supports both connectionless and connection-oriented links. You must specify either aal3 or aal5.<br>**Note** For the Cisco 7300 and Cisco 7600 series routers, the **aa13** keyword is not supported. |

| | |
|---|---|
| *subscriber-encap* | Specifies the encapsulation type at the subscriber line.<br>• **snap-rbe**<br>• **mux-rbe**<br>• **snap-dot1q-rbe**<br>• **mux-dot1q-rbe**<br>• **snap-pppoa**<br>• **mux-pppoa**<br>• **snap-1483routed**<br>• **mux-1483routed** |
| **user-defined** | Specifies that the router is to use an offset size when calculating ATM overhead. |
| *offset* | Specifies the offset size when calculating ATM overhead. Valid values are from –127 to 127 bytes; 0 is not a valid value.<br>**Note** For the Cisco 7300 and Cisco 7600 series routers, valid values are from -48 to 48 bytes; 0 is not a valid value.<br>**Note** The router configures the offset size if you do not specify the user-defined offset option. |
| **atm** | Applies ATM cell tax in the ATM overhead calculation.<br>**Note** For the Cisco 7300 and Cisco 7600 series routers, the **atm**keyword is not supported.<br>**Note** Configuring both the offset and atm options adjusts the packet size to the offset size and then adds ATM cell tax. |

## Command Default

When the excess burst size (Be) is not configured, the default Be value is equal to the committed burst size (Bc). For more information about burst size defaults, see the "Usage Guidelines" section.

Traffic shaping overhead accounting for ATM is disabled.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)XE | This command was introduced. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |

| Release | Modification |
|---|---|
| 12.0(17)SL | This command was integrated into Cisco IOS Release 12.0(17)SL and implemented on the PRE1 for the Cisco 10000 series router. |
| 12.2(16)BX | This command was integrated into Cisco IOS Release 12.2(16)BX and implemented on the PRE2 for the Cisco 10000 series router. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(31)SB2 | This command was enhanced for ATM overhead accounting and implemented on the Cisco 10000 series router for the PRE3. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(31)SB6 | This command was enhanced to specify an offset size when calculating ATM overhead and implemented on the Cisco 10000 series router for the PRE3. |
| 12.2(33)SRC | This command was modified. Support for the Cisco 7600 series router was added. |
| 12.2(33)SB | This command was modified. Support for the Cisco 7300 series router was added. |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers. |
| 15.2(1)T | This command was modified. The allowed values for the offset argument were changed. The value must be between -127 and 127 bytes; 0 is not a valid value. The allowed value for the mean-rate argument was changed. The value must be between 1,000 and 1,000,000,000 bits per second. |

## Usage Guidelines

The measurement interval is the committed burst size (Bc) divided by committed information rate (CIR). Bc cannot be set to 0. If the measurement interval is too large (greater than 128 milliseconds), the system subdivides it into smaller intervals.

If you do not specify the committed burst size (Bc) and the excess burst size (Be), the algorithm decides the default values for the shape entity. The algorithm uses a 4 milliseconds measurement interval, so Bc is CIR * (4 / 1000).

Burst sizes larger than the default committed burst size (Bc) need to be explicitly specified. The larger the Bc, the longer the measurement interval. A long measurement interval may affect voice traffic latency, if applicable.

When the excess burst size (Be) is not configured, the default value is equal to the committed burst size (Bc).

**Traffic Shaping on the Cisco 10000 Series Performance Routing Engine**

The Cisco 10000 series router does not support the peak keyword.

On the PRE2, you specify a shape rate and a unit for the rate. Valid values for the rate are from 1 to 2488320000 and units are bps, kbps, mbps, gbps. The default unit is kbps. For example:

```
shape 128000 bps
```

On the PRE3, you only need to specify a shape rate. Because the unit is always bps on the PRE3, the unit argument is not available. Valid values for the shape rate are from 1000 to 2488320000.

```
shape 1000
```

The PRE3 accepts the PRE2 shape command as a hidden command. However, the PRE3 rejects the PRE2 shape command if the specified rate is outside the valid PRE3 shape rate range (1000 to 2488320000).

**Traffic Shaping Overhead Accounting for ATM (Cisco 7300 Series Router, Cisco 7600 Series Router, and Cisco 10000 Series Router)**

When configuring ATM overhead accounting on the Cisco 7300 series router, the Cisco 7600 series router, or the Cisco 10000 series router, you must specify the BRAS-DSLAM, DSLAM-CPE, and subscriber line encapsulation types. The router supports the following subscriber line encapsulation types:

- **snap-rbe**
- **mux-rbe**
- **snap-dot1q-rbe**
- **mux-dot1q-rbe**
- **snap-pppoa**
- **mux-pppoa**
- **snap-1483routed**
- **mux-1483routed**

For hierarchical policies, configure ATM overhead accounting in the following ways:

- Enabled on parent--If you enable ATM overhead accounting on a parent policy, you are not required to enable accounting on the child policy.
- Enabled on child and parent--If you enable ATM overhead accounting on a child policy, then you must enable ATM overhead accounting on the parent policy.

The encapsulation types must match for the child and parent policies.

The user-defined offset values must match for the child and parent policies.

## Examples

The following example configures a shape entity with a CIR of 1 Mbps and attaches the policy map called dts-interface-all-action to interface pos1/0/0:

```
policy-map dts-interface-all-action
 class class-interface-all
  shape average 1000000
interface pos1/0/0
 service-policy output dts-interface-all-action
```

## Examples

When a parent policy has ATM overhead accounting enabled for shaping, you are not required to enable accounting at the child level using the police command. In the following configuration example, ATM overhead

accounting is enabled for bandwidth on the gaming and class-default class of the child policy map named subscriber_classes and on the class-default class of the parent policy map named subscriber_line. The voip and video classes do not have ATM overhead accounting explicitly enabled. These priority classes have ATM overhead accounting implicitly enabled because the parent policy has ATM overhead accounting enabled. Notice that the features in the parent and child policies use the same encapsulation type.

```
policy-map subscriber_classes
 class voip
  priority level 1
  police 8000
 class video
  priority level 2
  police 20000
 class gaming
  bandwidth remaining percent 80 account dot1q aal5 snap-dot1q-rbe
 class class-default
  bandwidth remaining percent 20 account dot1q aal5 snap-dot1q-rbe
policy-map subscriber_line
 class class-default
  shape average 8000 account dot1q aal5 snap-dot1q-rbe
  service policy subscriber_classes
```

In the following example, the router will use 20 overhead bytes and ATM cell tax in calculating ATM overhead.

```
policy-map child
 class class1
  bandwidth 500 account user-defined 20 atm
 class class2
  shape average 30000 account user-defined 20 atm
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map, and enables ATM overhead accounting. |
| **shape adaptive** | Configures a Frame Relay interface or a point-to-point subinterface to estimate the available bandwidth by BECN integration while traffic shaping is enabled. |
| **shape fecn-adapt** | Configures a Frame Relay PVC to reflect received FECN bits as BECN bits in Q.922 TEST RESPONSE messages. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. If configured, the command output includes information about ATM overhead accounting. |
| **show running-config** | Displays the current configuration of the router. If configured, the command output includes information about ATM overhead accounting. |

# shape adaptive

To configure a Frame Relay interface or a point-to-point subinterface to estimate the available bandwidth by backward explicit congestion notification (BECN) integration while traffic shaping is enabled, use the **shapeadaptive**command in policy-map class configuration mode. To leave the available bandwidth unestimated, use the **no** form of this command.

**shape adaptive** *mean-rate-lower-bound*

**no shape adaptive**

## Syntax Description

| | |
|---|---|
| *mean-rate-lower-bound* | Specifies the lower bound of the range of permitted bit rates. |

## Command Default

Bandwidth is not estimated.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(5)XE | This command was introduced. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.2(13)T | This command was implemented on the Cisco 1700 series, Cisco 2500 series, Cisco 2600 series, Cisco 3620 router, Cisco 3631 router, Cisco 3640 router, Cisco 3660 router, Cisco 3725 router, Cisco 3745 router, Cisco 7200 series, Cisco 7400 series routers. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

If traffic shaping is not enabled, this command has no effect.

When continuous BECN messages are received, the shape entity immediately decreases its maximum shape rate by one-fourth for each BECN message received until it reaches the lower bound committed information rate (CIR). If, after several intervals, the interface has not received another BECN and traffic is waiting in the shape queue, the shape entity increases the shape rate back to the maximum rate by 1/16 for each interval. A

shape entity configured with the **shapeadaptive***mean-rate-lower-bound* command will always be shaped between the mean rate upper bound and the mean rate lower bound.

**Note** The **shapeadaptive** command cannot be used with the **shape(percent)** command.

## Examples

The following example configures a shape entity with CIR of 128 kbps and sets the lower bound CIR to 64 kbps when BECNs are received:

```
policy-map dts-p2p-all-action

class class-p2p-all

shape adaptive 64000
```

## Related Commands

| Command | Description |
|---|---|
| **shape (percent)** | Specifies average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface |

# shape fecn-adapt

To configure a Frame Relay interface to reflect received forward explicit congestion notification (FECN) bits as backward explicit congestion notification (BECN) bits in Q.922 TEST RESPONSE messages, use the **shapefecn-adapt**command in policy-map class configuration mode. To configure the Frame Relay interface to not reflect FECN as BECN, use the **no** form of this command.

**shape fecn-adapt**

**no shape fecn-adapt**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No default behavior or values.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(5)XE | This command was introduced. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.2(13)T | This command was implemented on the Cisco 1700 series, Cisco 2500 series, Cisco 2600 series, Cisco 3620 router, Cisco 3631 router, Cisco 3640 router, Cisco 3660 router, Cisco 3725 router, Cisco 3745 router, Cisco 7200 series, Cisco 7400 series routers. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

When the downstream Frame Relay switch is congested, a Frame Relay interface or point-to-point interface receives a Frame Relay message with the FECN bit on. This message may be an indication that no traffic is waiting to carry a BECN to the far end (voice/multimedia traffic is one-way). When the **shapefecn-adapt** command is configured, a small buffer is allocated and a Frame Relay TEST RESPONSE is built on behalf of the Frame Relay switch. The Frame Relay TEST RESPONSE is equipped with the triggering data-link connection identifier (DLCI) of the triggering mechanism. It also sets the BECN bit and sends it out to the wire.

## Examples

The following example configures a shape entity with a committed information rate (CIR) of 1 Mbps and adapts the Frame Relay message with FECN to BECN:

```
policy-map dts-p2p-all-action
class class-p2p-all
shape average 1000000
shape fecn-adapt
```

## Related Commands

| Command | Description |
|---|---|
| **shape adaptive** | Configures a Frame Relay interface or a point-to-point subinterface to estimate the available bandwidth by BECN integration while traffic shaping is enabled. |
| **shape (percent)** | Configures an interface to shape traffic to an indicated bit rate. |

# shape max-buffers

To specify the number of buffers allowed on shaping queues, use the **shapemax-buffers**command in class-map configuration mode. To set the number of buffers to its default value, use the **no** form of this command.

**shape max-buffers** *number-of-buffers*

**no shape max-buffers**

## Syntax Description

| | |
|---|---|
| *number-of-buffers* | Specifies the number of buffers. The minimum number of buffers is 1; the maximum number of buffers is 4096. |

## Command Default

1000 buffers are preset.

## Command Modes

Class-map configuration (config-cmap)

## Command History

| Release | Modification |
|---|---|
| 12.1(2)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T, but without support for hierarchical queueing framework (HQF). See the "Usage Guidelines" for additional information. |

## Usage Guidelines

You can specify the maximum number of buffers allowed on shaping queues for each class configured to use Generic Traffic Shaping (GTS).

You configure this command under a class in a policy map. However, the **shapemax-buffers**command is not supported for HQF in Cisco IOS Release 12.4(20)T. Use the **queue-limit** command, which provides similar functionality.

## Examples

The following example configures shaping and sets the maximum buffer limit to 100:

```
shape average 350000
shape max-buffers 100
```

## Related Commands

| Command | Description |
|---|---|
| **bandwidth** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map. |
| **class (policy-map)** | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **queue-limit** | Specifies or modifies the maximum number of packets a queue can hold for a class policy configured in a policy map. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **shape** | Specifies average or peak rate traffic shaping. |

# show access-lists rate-limit

To display information about rate-limit access lists, use the **showaccess-listsrate-limit**command in EXEC mode.

**show access-lists rate-limit** [ *acl-index* ]

## Syntax Description

| | |
|---|---|
| *acl-index* | (Optional) Rate-limit access list number from 1 to 299. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 11.1CC | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Examples

The following is sample output from the **showaccess-listsrate-limit** command:

```
Router# show access-lists rate-limit
Rate-limit access list 1
    0
Rate-limit access list 2
    1
Rate-limit access list 3
    2
Rate-limit access list 4
    3
Rate-limit access list 5
    4
Rate-limit access list 6
    5
Rate-limit access list 9
    mask FF
Rate-limit access list 10
    mask 0F
Rate-limit access list 11
    mask F0
Rate-limit access list 100
    1001.0110.1111
Rate-limit access list 101
    00E0.34B8.D840
Rate-limit access list 199
    1111.1111.1111
```

The following is sample output from the **showaccess-listsrate-limit** command when specific rate-limit access lists are specified:

```
Router# show access-lists rate-limit 1
Rate-limit access list 1
    0
Router# show access-lists rate-limit 9
Rate-limit access list 9
    mask FF
Router# show access-lists rate-limit 101
Rate-limit access list 101
    00E0.34B8.D840
```

The table below describes the significant fields shown in the displays.

***Table 44: show access-lists rate-limit Field Descriptions***

| Field | Description |
|---|---|
| Rate-limit access list | Rate-limit access list number. A number from 1 to 99 represents a precedence-based access list. A number from 100 to 199 indicates a MAC address-based access list. |
| 0 | IP Precedence for packets in this rate-limit access list. |
| mask FF | IP Precedence mask for packets in this rate-limit access list. |
| 1001.0110.1111 | MAC address for packets in this rate-limit access list. |

## Related Commands

| Command | Description |
|---|---|
| **access-list rate-limit** | Configures an access list for use with CAR policies. |
| **show access-lists** | Displays the contents of current IP and rate-limit access lists. |

# show atm bundle

To display the bundle attributes assigned to each bundle virtual circuit (VC) member and the current working status of the VC members, use the **showatmbundle** command in privileged EXEC mode.

**show atm bundle** [ *bundle-name* ]

## Syntax Description

| | |
|---|---|
| *bundle-name* | (Optional) Name of the bundle whose member information to be displayed. |

## Command Default

If no bundle name is specified, all bundles assigned to VC are displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Examples

The following is sample output from the **showatmbundle**command (* indicates that this VC is the VC for all precedence levels not explicitly configured):

```
Router# show atm bundle

new-york on atm1/0.1 Status: UP
                     Config. Active  Bumping    PG/ Peak  Avg/Min  Burst
Name       VPI/VCI   Preced. Preced. Predec./   PV  kbps  kbps     Cells  Status
                                     Accept
ny-control   0/207      7        7      4  /Yes   pv  10000  5000     32      UP
ny-premium   0/206     6-5      6-5     7  /No    pg  20000  10000    32      UP
ny-priority  0/204     4-2      4-2     1  /Yes   pg  10000  3000             UP
ny-basic*    0/201     1-0      1-0     -  /Yes   pg  10000                   UP
los-angeles on atm1/0.1 - Status: UP

                     Config. Active  Bumping    pg/ Peak  Avg/Min  Burst
Name       VPI/VCI   Preced. Preced. Predec./   pv  kbps  kbps     Cells  Status
                                     Accept
la-high     0/407     7-5      7-5     4 /Yes      pv  20000  5000     32     UP
la-med      0/404     4-2      4-2     1 /Yes      pg  10000  3000             UP
la-low*     0/401     1-0      1-0     - /Yes      pg  10000                   UP
san-francisco on atm1/0.1 Status: UP
                     Config. Active  Bumping    PG/ Peak  Avg/Min  Burst
```

```
Name        VPI/VCI    Preced. Preced. Predec./   PV  kbps  kbps     Cells  Status
                                       Accept
sf-control    0/307      7       7      4 /Yes    pv  10000  5000     32      UP
sf-premium    0/306     6-5     6-5     7 /No     pg  20000  10000    32      UP
sf-priority   0/304     4-2     4-2     1 /Yes    pg  10000  3000             UP
sf-basic*     0/301     1-0     1-0     - /Yes    pg  10000                   UP
```

## Related Commands

| Command | Description |
|---|---|
| **bundle** | Creates or modifies an existing bundle. |
| **show atm bundle statistics** | Displays statistics on the specified bundle. |
| **show atm map** | Displays the list of all configured ATM static maps to remote hosts on an ATM network. |

# show atm bundle stat

To display statistics or detailed statistics on the specified bundle, use the **showatmbundlestat**command in privileged EXEC mode.

**show atm bundle** *bundle-name* **stat [detail]**

## Syntax Description

| | |
|---|---|
| *bundle-name* | Name of the bundle whose member information to be displayed. |
| **detail** | (Optional) Displays detailed statistics. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Examples

The following is sample output from the **showatmbundlestat**command:

```
Router# show atm bundle san-jose stat

Bundle Name: Bundle State: UP
AAL5-NLPID
OAM frequency : 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
BUNDLE is not managed.
InARP frequency: 15 minute(s)
InPkts: 3, OutPkts: 3, Inbytes: 1836, Outbytes: 1836
InPRoc: 3, OutPRoc: 0, Broadcasts: 3
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
Router# show atm bundle san-jose stat detail
Bundle Name: Bundle State: UP
AAL5-NLPID
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
BUNDLE is not managed.
InARP frequency: 15 minute(s)
InPkts: 3, OutPkts: 3, InBytes; 1836, OutBytes: 1836
InPRoc: 3, OutPRoc: 0, Broadcasts: 3
InFast: 0, OutFast: 0, InAS: 0, OutAS: 0
ATM1/0.52: VCD: 6, VPI: 0 VCI: 218, Connection Name: sj-basic
UBR, PeakRate: 155000
```

```
AAL5-LLC/SNAP, etype:0x0, Flags: 0xC20, VCmode: 0xE00
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopbavk status: OAM Disabled
OMA VC state: Not Managed
ILMI VC state: Not Managed
InARP frequency: 15 minute(s)
InPkts: 3, OutPkts: 3, InBytes; 1836, OutBytes: 1836
InPRoc: 3, OutPRoc: 0,Broadcasts: 3
InFast: 0, OutFast: 0, InAS: 0, OututAS: 0
OAM cells received: 0
F5 InEndloop: 0, F5 InSegloop: 0, F5 InAIS: 0, F5 InRDI: 0
F4 InEndloop: 0, F4 OutSegloop:0, F4 InAIS: 0, F4 InRDI: 0
OAM cells sent: 0
F5 OutEndloop: 0. F5 OutSegloop: 0, f5 Out RDI:0
F4 OutEndloop: 0, F4 OutSegloop: 0, F4 OUtRDI: 0
OAM cell drops: 0
Status; UP
ATM1/0.52: VCD: 4, VPI: 0 VCI: 216, Connection Name: sj-premium
UBR, PeakRate: 155000
AAL5-LLC/SNAP, etype: 0x0, Flags: 0xC20, VCmode: 0xE000
OAM frequency: 0 second(s), OAM retry frequency: 1 second(s)
OAM up retry count: 3, OAM down retry count: 5
OAM Loopback status: OAM Disabled
OAM VC state:  Not Managed
ILMI VC state: Not Managed
InARP frequency: 15 minute(s)
InPkts: 0, OutPkts: 0, InBytes; 0, OutBytes: 0
InPRoc: 0, OutPRoc: 0, Broadcasts: 0
InFast: 0, OutFast: 0, InAS: 0
OAM cells received: 0
F5 InEndloop: 0, F4 InSegloop: 0, F4InAIS; 0, F4 InRDI: 0
F4 OutEndloop: 0, F4 OutSegloop: F4 OutRDI: 0
OAM cell drops: 0
Status: UP
```

## Related Commands

| Command | Description |
|---|---|
| **bundle** | Creates or modifies an existing bundle. |
| **show atm bundle** | Displays the bundle attributes assigned to each bundle VC member and the current working status of the VC members. |
| **show atm map** | Displays the list of all configured ATM static maps to remote hosts on an ATM network. |

# show atm bundle svc

To display the bundle attributes assigned to each bundle virtual circuit (VC) member and the current working status of the VC members, use the **showatmbundlesvc**command in privileged EXEC mode.

**show atm bundle svc** [ *bundle-name* ]

## Syntax Description

| | |
|---|---|
| *bundle-name* | (Optional) Name of the switched virtual circuit (SVC) bundle to be displayed, as identified by the **bundlesvc** command. |

## Command Default

If no bundle name is specified, all SVC bundles configured on the system are displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(4)T | This command was introduced. |

## Examples

The following example provides output for the **showatmbundlesvc**command. The bundle named “finance” is configured on ATM interface 1/0.1 with eight members. All of the members are up except bundle member zero. Bundle member zero is the default member, which if initiated once will always be on and used as the default for all traffic.

```
Router# show atm bundle svc finance
finance on ATM1/0.1:UP
                        Config    Current  Peak   Avg/Min   Burst
VC Name       VPI/VCI   Preced.   Preced.  Kbps   kbps      Cells    Sts
seven         0/37        7         7      10000   5000      32      UP
six           0/36        6         6       6000                    UP
five          0/40        5         5       5000                    UP
four          0/41        4         4       4000                    UP
three         0/42        3         3       3000                    UP
two           0/43        2         2       2000                    UP
one           0/44        1         1       1000                    UP
zero*                     0
```

The table below describes the significant fields in the display.

***Table 45: show atm bundle svc Field Descriptions***

| Field | Description |
|---|---|
| finance on ATM1/0.1: UP | Name of SVC bundle, interface type and number,and status of bundle. |

| Field | Description |
|---|---|
| VC Name | Name of SVC bundle. |
| VPI/VCI | Virtual path identifier and virtual channel identifier. |
| Config. Preced. | Configured precedence. |
| Current Preced. | Current precedence. |
| Peak Kbps | Peak kbps for the SVC. |
| Avg/Min kbps | Average or minimum kbps for the SVC. |
| Sts | Status of the bundle member. |
| * | Indicates the default bundle member. |

## Related Commands

| Command | Description |
|---|---|
| **bundle svc** | Creates or modifies an SVC bundle. |

# show atm bundle svc stat

To display the statistics of a switched virtual circuit (SVC) bundle, use the **showatmbundlesvcstat**command in privileged EXEC mode.

**show atm bundle svc** *bundle-name* **stat [detail]**

## Syntax Description

| | |
|---|---|
| *bundle-name* | Name of the SVC bundle as identified by the **bundlesvc** command. |
| **detail** | (Optional) Displays the detailed ATM bundle statistics. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(4)T | This command was introduced. |

## Examples

The following example provides output for the **showatmbundlesvcstat**command using a bundle named “city”:

```
Router# show atm bundle svc city stat
Bundle Name:Bundle State:INITIALIZING
AAL5-NLPID
OAM frequency:0 second(s), OAM retry frequency:10 second(s)
OAM up retry count:4, OAM down retry count:3
BUNDLE is managed by.
InARP frequency:15 minutes(s)
InPkts:0, OutPkts:0, InBytes:0, OutBytes:0
InPRoc:0, OutPRoc:0, Broadcasts:0
InFast:0, OutFast:0, InAS:0, OutAS:0
InPktDrops:0, OutPktDrops:0
CrcErrors:0, SarTimeOuts:0, OverSizedSDUs:0,
                LengthViolation:0, CPIErrors:0
```

show atm bundle svc stat, on page 1134 describes the significant fields in the display.

***Table 46: show atm bundle svc statistics Field Descriptions***

| Field | Description |
|---|---|
| Bundle Name | Name of the bundle. |
| State | State of the bundle. |
| BUNDLE is managed by | Bundle management. |

| Field | Description |
|---|---|
| InARP frequency | Number of minutes between Inverse ARP messages or “DISABLED” if Inverse ARP is not in use on this VC. |
| InPkts | Total number of packets received on this virtual circuit (VC), including all fast-switched and process-switched packets. |
| OutPkts | Total number of packets sent on this VC, including all fast-switched and process-switched packets. |
| InBytes | Total number of bytes received on this VC, including all fast-switched and process-switched packets. |
| OutBytes | Total number of bytes sent on this VC, including all fast-switched and process-switched packets. |
| InPRoc | Number of incoming packets being process-switched. |
| OutPRoc | Number of outgoing packets being process-switched. |
| Broadcasts | Number of process-switched broadcast packets. |
| InFast | Number of incoming packets being fast-switched. |
| OutFast | Number of outgoing packets being fast-switched. |
| InAS | Number of autonomous-switched or silicon-switched input packets received. |
| OutAS | Number of autonomous-switched or silicon-switched input packets sent. |
| InPktDrops | Number of incoming packets dropped. |
| OutPktDrops | Number of outgoing packets dropped. |
| CrcErrors | Number of cyclic redundancy check (CRC) errors. |
| SarTimeOuts | Number of packets that timed out before segmentation and reassembly occurred. |
| LengthViolation | Number of packets too long or too short. |

## Related Commands

| Command | Description |
|---|---|
| **bundle svc** | Creates or modifies an SVC bundle. |

# show auto discovery qos through show ip rsvp hello client lsp detail


- show auto discovery qos, page 1139
- show auto qos, page 1143
- show class-map, page 1148
- show class-map type nat, page 1151
- show class-map type port-filter, page 1153
- show control-plane cef-exception counters, page 1155
- show control-plane cef-exception features, page 1157
- show control-plane counters, page 1159
- show control-plane features, page 1161
- show control-plane host counters, page 1163
- show control-plane host features, page 1165
- show control-plane host open-ports, page 1167
- show control-plane transit counters, page 1169
- show control-plane transit features, page 1171
- show cops servers, page 1173
- show crypto eng qos, page 1174
- show crypto entropy status, page 1175
- show frame-relay ip rtp header-compression, page 1177
- show frame-relay ip tcp header-compression, page 1182
- show interfaces fair-queue, page 1185
- show interfaces random-detect, page 1188
- show interfaces rate-limit, page 1191
- show iphc-profile, page 1194

- show ip nat translations rsvp, page 1196
- show ip nbar attribute, page 1198
- show ip nbar link-age, page 1200
- show ip nbar pdlm, page 1202
- show ip nbar port-map, page 1203
- show ip nbar protocol activated, page 1205
- show ip nbar protocol-attribute, page 1206
- show ip nbar protocol-discovery, page 1208
- show ip nbar protocol-id, page 1212
- show ip nbar protocol-pack, page 1224
- show ip nbar resources flow, page 1226
- show ip nbar statistics , page 1227
- show ip nbar trace, page 1228
- show ip nbar unclassified-port-stats, page 1230
- show ip nbar version, page 1233
- show ip rsvp, page 1236
- show ip rsvp aggregation ip, page 1244
- show ip rsvp aggregation ip endpoints, page 1248
- show ip rsvp atm-peak-rate-limit, page 1252
- show ip rsvp authentication, page 1254
- show ip rsvp counters, page 1261
- show ip rsvp counters state teardown, page 1265
- show ip rsvp fast bw-protect, page 1267
- show ip rsvp fast detail, page 1270
- show ip rsvp fast-reroute, page 1275
- show ip rsvp fast-reroute bw-protect, page 1279
- show ip rsvp fast-reroute detail, page 1283
- show ip rsvp hello, page 1289
- show ip rsvp hello client lsp detail, page 1291

# show auto discovery qos

To display the data collected during the Auto-Discovery (data collection) phase of the AutoQoS for the Enterprise feature, use the **showautodiscoveryqos**command in privileged EXEC mode.

**show auto discovery qos** [**interface** [*type number*]]

## Syntax Description

| | |
|---|---|
| **interface** | (Optional) Indicates that the configurations for a specific interface type will be displayed. |
| *type number* | (Optional) Specifies the interface type and number. |

## Command Default

Displays the configurations created for all interface types.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(7)T | This command was introduced. |
| 12.3(11)T | Command output was modified to include suggested policy map information. |

## Usage Guidelines

The suggested policy output (shown in the example below) lets you preview class maps and policy maps before you issue the **autoqos** command on an interface. You can then continue with the Auto-Discovery phase until more data is gathered or you can cut and paste the existing data and edit it as desired.

## Examples

The following is sample output from the **showautodiscoveryqos** command. This example displays the data collected during the Auto-Discovery (data collection) phase using DSCP classification in trusted mode and includes suggested policy map information.

```
Router# show auto discovery qos
Serial2/1.1
 AutoQoS Discovery enabled for trusted DSCP
 Discovery up time: 2 hours, 42 minutes
 AutoQoS Class information:
 Class Voice:
  Recommended Minimum Bandwidth: 118 Kbps/1% (PeakRate)
  Detected DSCPs and data:
  DSCP value         AverageRate        PeakRate           Total
                     (kbps/%)           (kbps/%)           (bytes)
  -----------        -----------        --------           ------------
  46/ef              106/1              118/1              129510064
 Class Interactive Video:
```

```
 Recommended Minimum Bandwidth: 25 Kbps/<1% (AverageRate)
 Detected DSCPs and data:
 DSCP value         AverageRate        PeakRate           Total
                    (kbps/%)           (kbps/%)           (bytes)
 -----------        -----------        --------           ------------
 34/af41            25/<1              28/<1              31084292
Class Signaling:
 Recommended Minimum Bandwidth: 50 Kbps/<1% (AverageRate)
 Detected DSCPs and data:
 DSCP value         AverageRate        PeakRate           Total
                    (kbps/%)           (kbps/%)           (bytes)
 -----------        -----------        --------           ------------
 24/cs3             50/<1              56/<1              61838040
Class Streaming Video:
 Recommended Minimum Bandwidth: 79 Kbps/<1% (AverageRate)
 Detected DSCPs and data:
 DSCP value         AverageRate        PeakRate           Total
                    (kbps/%)           (kbps/%)           (bytes)
 -----------        -----------        --------           ------------
 32/cs4             79/<1              88/<1              96451788
Class Transactional:
 Recommended Minimum Bandwidth: 105 Kbps/1% (AverageRate)
 Detected DSCPs and data:
 DSCP value         AverageRate        PeakRate           Total
                    (kbps/%)           (kbps/%)           (bytes)
 -----------        -----------        --------           ------------
 18/af21            105/1              117/1              127798678
Class Bulk:
 Recommended Minimum Bandwidth: 132 Kbps/1% (AverageRate)
 Detected DSCPs and data:
 DSCP value         AverageRate        PeakRate           Total
                    (kbps/%)           (kbps/%)           (bytes)
 -----------        -----------        --------           ------------
 10/af11            132/1              147/1              160953984
Class Scavenger:
 Recommended Minimum Bandwidth: 24 Kbps (AverageRate)/0% (fixed)
 Detected DSCPs and data:
 DSCP value         AverageRate        PeakRate           Total
                    (kbps/%)           (kbps/%)           (bytes)
 -----------        -----------        --------           ------------
 8/cs1              24/<1              27/<1              30141238
Class Management:
 Recommended Minimum Bandwidth: 34 Kbps/<1% (AverageRate)
 Detected DSCPs and data:
 DSCP value         AverageRate        PeakRate           Total
                    (kbps/%)           (kbps/%)           (bytes)
 -----------        -----------        --------           ------------
 16/cs2             34/<1              38/<1              41419740
Class Routing:
 Recommended Minimum Bandwidth: 7 Kbps/<1% (AverageRate)
 Detected DSCPs and data:
 DSCP value         AverageRate        PeakRate           Total
                    (kbps/%)           (kbps/%)           (bytes)
 -----------        -----------        --------           ------------
 48/cs6             7/<1               7/<1               8634024
Class Best Effort:
 Current Bandwidth Estimation: 820 Kbps/8% (AverageRate)
 Detected DSCPs and data:
 DSCP value         AverageRate        PeakRate           Total
                    (kbps/%)           (kbps/%)           (bytes)
 -----------        -----------        --------           ------------
 0/default          820/8              915/9              997576380
Suggested AutoQoS Policy based on a discovery uptime of 2 hours, 42 minutes:
 !
 class-map match-any AutoQoS-Voice-Trust
  match ip dscp ef
 !
 class-map match-any AutoQoS-Inter-Video-Trust
  match ip dscp af41
 !
 class-map match-any AutoQoS-Signaling-Trust
  match ip dscp cs3
 !
```

```
class-map match-any AutoQoS-Stream-Video-Trust
 match ip dscp cs4
!
class-map match-any AutoQoS-Transactional-Trust
 match ip dscp af21
 match ip dscp af22
 match ip dscp af23
!
class-map match-any AutoQoS-Bulk-Trust
 match ip dscp af11
 match ip dscp af12
 match ip dscp af13
!
class-map match-any AutoQoS-Scavenger-Trust
 match ip dscp cs1
!
class-map match-any AutoQoS-Management-Trust
 match ip dscp cs2
!
class-map match-any AutoQoS-Routing-Trust
 match ip dscp cs6
!
policy-map AutoQoS-Policy-S2/1.1Trust
 class AutoQoS-Voice-Trust
  priority percent 1
 class AutoQoS-Inter-Video-Trust
  bandwidth remaining percent 1
 class AutoQoS-Signaling-Trust
  bandwidth remaining percent 1
 class AutoQoS-Stream-Video-Trust
  bandwidth remaining percent 1
 class AutoQoS-Transactional-Trust
  bandwidth remaining percent 1
  random-detect dscp-based
 class AutoQoS-Bulk-Trust
  bandwidth remaining percent 1
  random-detect dscp-based
 class AutoQoS-Scavenger-Trust
  bandwidth remaining percent 1
 class AutoQoS-Management-Trust
  bandwidth remaining percent 1
 class AutoQoS-Routing-Trust
  bandwidth remaining percent 1
 class class-default
  fair-queue
```

The table below describes the significant fields shown in the display.

***Table 47: show auto discovery qos Field Descriptions***

| Field | Description |
|---|---|
| Serial2/1.1 | The interface or subinterface on which data is being collected. |
| AutoQoS Discovery enabled for trusted DSCP | Indicates that the data collection phase of AutoQoS has been enabled. |
| Discovery up time | Indicates the period of time in which data was collected. |
| AutoQoS Class information | Displays information for each AutoQoS class. |

| Field | Description |
|---|---|
| Class Voice | Information for the named class, along with data pertaining to the detected applications. This data includes DSCP value, average rate (in kilobits per second (kbps)), peak rate (kbps), and total packets (bytes). |
| Suggested AutoQoS Policy based on a discovery uptime of hours and minutes | Policy-map and class-map statistics based on a specified discovery time. |

## Related Commands

| Command | Description |
|---|---|
| **auto qos** | Installs the QoS class maps and policy maps created by the AutoQoS for the Enterprise feature. |
| **auto discovery qos** | Begins discovering and collecting data for configuring the AutoQoS for the Enterprise feature. |
| **show auto qos** | Displays the interface configurations, policy maps, and class maps created by AutoQoS on a specific interface or all interfaces. |

# show auto qos

To display the interface configurations, policy maps, and class maps created by AutoQoS on a specific interface or all interfaces, use the **showautoqos**command in privileged EXEC mode.

**show auto qos** [**interface** [*type slot/ port*]]

## Syntax Description

| | |
|---|---|
| **interface** | (Optional) Displays the configurations created by the AutoQoS--VoIP feature on all the interfaces or PVCs on which the AutoQoS--VoIP feature is enabled.<br>• If you configure the **interface** keyword but do not specify an interface type, the **showautoqosinterface**command displays the configurations created by the AutoQoS--VoIP feature on all the interfaces or PVCs on which the AutoQoS--VoIP feature is enabled. |
| *type* | (Optional) Interface type; valid values are **atm**, **ethernet**, **fastethernet**, **ge-wan**, **gigabitethernet**, **pos**, and**tengigabitethernet**. |
| *slot* / *port* | (Optional) Slot and port number. |

## Command Default

If no arguments or keywords are specified, configurations created for all interface types are displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced as part of the AutoQoS--VoIP feature. |
| 12.3(7)T | This command was modified for the AutoQoS for the Enterprise feature. The output was modified to display the classes, class maps, and policy maps created on the basis of the data collected during the Auto-Discovery phase of the AutoQoS for the Enterprise feature. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 15.2(1)T | This command was modified. The output does not display the Frame Relay traffic shaping configuration. |

## Usage Guidelines

The **showautoqosinterface** command can be used with Frame Relay data-link connection identifiers (DLCIs) and ATM PVCs.

When the AutoQoS--VoIP or the AutoQos for the Enterprise features are enabled, configurations are generated for each interface or PVC. These configurations are then used to create the interface configurations, policy maps, class maps, and access control lists (ACLs) for use on the network. The **showautoqos**command can be used to verify the contents of the interface configurations, policy maps, class maps, and ACLs.

**Catalyst 6500 Series Switches**

AutoQoS is supported on the following modules:

- WS-X6548-RJ45
- WS-X6548-RJ21
- WS-X6148-GE-TX
- WS-X6548-GE-TX-CR
- WS-X6148-RJ45V
- WS-X6148-RJ21V
- WS-X6348-RJ45
- WS-X6348-RJ21
- WS-X6248-TEL

## Examples

## Examples

The **showautoqosinterface***typeslot/port* command displays the configurations created by the AutoQoS--VoIP feature on the specified interface.

In the following example, the serial subinterface 6/1.1 has been specified:

```
Router# show auto qos interface serial 6/1.1
S6/1.1: DLCI 100 -
!
interface Serial6/1.1 point-to-point
 frame-relay interface-dlci 100
  class AutoQoS-VoIP-FR-Serial6/1-100
 frame-relay ip rtp header-compression
!
map-class frame-relay AutoQoS-VoIP-FR-Serial6/1-100
 frame-relay cir 512000
 frame-relay bc 5120
 frame-relay be 0
 frame-relay mincir 512000
 service-policy output AutoQoS-Policy-UnTrust
 frame-relay fragment 640
```

When the **interface** keyword is configured but an interface type is not specified, the **showautoqosinterface**command displays the configurations created by the AutoQoS--VoIP feature on all the interfaces or PVCs on which the AutoQoS--VoIP feature is enabled.

```
Router# show auto qos interface
Serial6/1.1: DLCI 100 -
!
interface Serial6/1.1 point-to-point
```

```
 frame-relay interface-dlci 100
  class AutoQoS-VoIP-FR-Serial6/1-100
 frame-relay ip rtp header-compression
!
map-class frame-relay AutoQoS-VoIP-FR-Serial6/1-100
 frame-relay cir 512000
 frame-relay bc 5120
 frame-relay be 0
 frame-relay mincir 512000
 service-policy output AutoQoS-Policy-UnTrust
 frame-relay fragment 640
ATM2/0.1: PVC 1/100 -
!
interface ATM2/0.1 point-to-point
 pvc 1/100
  tx-ring-limit 3
  encapsulation aal5mux ppp Virtual-Template200
!
interface Virtual-Template200
 bandwidth 512
 ip address 10.10.107.1 255.255.255.0
 service-policy output AutoQoS-Policy-UnTrust
 ppp multilink
 ppp multilink fragment-delay 10
 ppp multilink interleave
```

The following example displays all of the configurations created by the AutoQoS--VoIP feature:

```
Router# show auto qos
Serial6/1.1: DLCI 100 -
!
interface Serial6/1.1 point-to-point
 frame-relay interface-dlci 100
  class AutoQoS-VoIP-FR-Serial6/1-100
frame-relay ip rtp header-compression
!
map-class frame-relay AutoQoS-VoIP-FR-Serial6/1-100
 frame-relay cir 512000
 frame-relay bc 5120
 frame-relay be 0
 frame-relay mincir 512000
 service-policy output AutoQoS-Policy-UnTrust
 frame-relay fragment 640
```

The table below describes the significant fields shown in the display.

***Table 48: show auto qos Field Descriptions (AutoQoS--VoIP Feature Configured)***

| Field | Description |
|---|---|
| class AutoQoS-VoIP-FR-Serial6/1-100 | Name of the class created by the AutoQoS-VoIP feature. In this instance, the name of the class is AutoQoS-VoIP-FR-Serial6/1-100. |
| service-policy output AutoQoS-Policy-UnTrust | Indicates that the policy map called "AutoQoS-Policy-UnTrust" has been attached to an interface in the outbound direction of the interface. |

show auto qos interface Command: Configured for the AutoQoS for the Enterprise Feature

The following is sample output from the **showautoqos** command. This example displays the classes, class maps, and policy maps created on the basis of the data collected during the Auto-Discovery phase of the AutoQoS for the Enterprise feature.

```
Router# show auto qos
 !
  policy-map AutoQoS-Policy-Se2/1.1
   class AutoQoS-Voice-Se2/1.1
    priority percent 70
    set dscp ef
   class AutoQoS-Inter-Video-Se2/1.1
    bandwidth remaining percent 10
    set dscp af41
   class AutoQoS-Stream-Video-Se2/1.1
    bandwidth remaining percent 1
    set dscp cs4
   class AutoQoS-Transactional-Se2/1.1
    bandwidth remaining percent 1
    set dscp af21
   class AutoQoS-Scavenger-Se2/1.1
    bandwidth remaining percent 1
    set dscp cs1
   class class-default
    fair-queue
 !
policy-map AutoQoS-Policy-Se2/1.1-Parent
   class class-default
    shape average 1024000
    service-policy AutoQoS-Policy-Se2/1.1
 !
 class-map match-any AutoQoS-Stream-Video-Se2/1.1
  match protocol cuseeme
 !
 class-map match-any AutoQoS-Transactional-Se2/1.1
  match protocol sqlnet
 !
class-map match-any AutoQoS-Voice-Se2/1.1
  match protocol rtp audio
 !
 class-map match-any AutoQoS-Inter-Video-Se2/1.1
  match protocol rtp video
 !
 rmon event 33333 log trap AutoQoS description "AutoQoS SNMP traps for Voice Drops" owner
AutoQoS
Serial2/1.1: DLCI 58 -
 !
 interface Serial2/1.1 point-to-point
  frame-relay interface-dlci 58
   class AutoQoS-FR-Serial2/1-58
 !
 map-class frame-relay AutoQoS-FR-Serial2/1-58
  frame-relay cir 1024000
frame-relay bc 10240
  frame-relay be 0
  frame-relay mincir 1024000
  service-policy output AutoQoS-Policy-Se2/1.1-Parent
```

The table below describes the significant fields shown in the display.

***Table 49: show auto qos Field Descriptions (AutoQoS for the Enterprise Feature Configured)***

| Field | Description |
|---|---|
| policy-map AutoQoS-Policy-Se2/1.1 | Name of the policy map created by the AutoQoS feature. In this instance, the name of the policy map is AutoQoS-Policy-Se2/1.1. |

| Field | Description |
|---|---|
| class AutoQoS-Voice-Se2/1.1<br>priority percent 70 set dscp ef | Name of the class created by the AutoQoS feature. In this instance, the name of the class is AutoQoS-Voice-Se2/1.1. Following the class name, the specific QoS features configured for the class are displayed. |
| class-map match-any AutoQoS-Stream-Video-Se2/1.1<br>match protocol cuseeme | Name of the class map and the packet matching criteria specified. |

## Related Commands

| Command | Description |
|---|---|
| **auto discovery qos** | Begins discovering and collecting data for configuring the AutoQoS for the Enterprise feature. |
| **auto qos** | Installs the QoS class maps and policy maps created by the AutoQoS for the Enterprise feature. |
| **auto qos voip** | Configures the AutoQoS--VoIP feature on an interface. |
| **show auto discovery qos** | Displays the data collected during the Auto-Discovery phase of the AutoQoS for the Enterprise feature. |

# show class-map

To display class maps and their matching criteria, use the **showclass-map** command in user EXEC or privileged EXEC mode.

### Cisco 3660, 3845, 6500, 7400, and 7500 Series Routers

**show class-map** [**type** {**stack**| **access-control**}] [ *class-map-name* ]

### Cisco 7600 and ASR 1000 Series Routers

**show class-map** [ *class-map-name* ]

## Syntax Description

| | |
|---|---|
| **type stack** | (Optional) Displays class maps configured to determine the correct protocol stack in which to examine via flexible packet matching (FPM). |
| **type access-control** | (Optional) Displays class maps configured to determine the exact pattern to look for in the protocol stack of interest. |
| *class-map-name* | (Optional) Name of the class map. The class map name can be a maximum of 40 alphanumeric characters. |

## Command Default

All class maps are displayed.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.2(13)T | This command was modified to display the Frame Relay data-link connection identifier (DLCI) number or Layer 3 packet length as a criterion for matching traffic inside a class map. |
| 12.2(14)SX | This command was implemented on the Cisco 7600 series routers. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

| Release | Modification |
|---|---|
| 12.4(4)T | The **type**, **stack**and **access-control**keywords were added to support FPM. |
| Cisco IOS XE Release 2.2 | This command was implemented on Cisco ASR Aggregation Services 1000 series routers. |
| 15.0(1)M | This command was modified. The output was modified to display encrypted filter information. |

## Usage Guidelines

You can use the **showclass-map**command to display all class maps and their matching criteria. If you enter the optional *class-map-name* argument, the specified class map and its matching criteria will be displayed.

## Examples

In the following example, three class maps are defined. Packets that match access list 103 belong to class c3, IP packets belong to class c2, and packets ingressing through Ethernet interface 1/0 belong to class c1. The output from the **showclass-map** command shows the three defined class maps.

```
Router# show class-map
 Class Map c3
 Match access-group 103
 Class Map c2
 Match protocol ip
 Class Map c1
 Match input-interface Ethernet1/0
```

In the following example, a class map called c1 has been defined, and the Frame Relay DLCI number of 500 has been specified as a match criterion:

```
Router# show class-map
class map match-all c1
   match fr-dlci 500
```

The following example shows how to display class-map information for all class maps:

```
Router# show class-map
 Class Map match-any class-default (id 0)
   Match any
 Class Map match-any class-simple (id 2)
   Match any
 Class Map match-all ipp5 (id 1)
   Match ip precedence 5
 Class Map match-all agg-2 (id 3)
```

The following example shows how to display class-map information for a specific class map:

```
Router# show class-map ipp5
 Class Map match-all ipp5 (id 1)
   Match ip precedence 5
```

The following is sample output from the **showclass-maptypeaccess-control** command for an encrpted FPM filter:

```
Router# show class-map type access-control accesscontrol1
 Class Map type access-control match-all accesscontrol1 (id 4)
   Match encrypted FPM filter
            filter-hash   : FC50BED10521002B8A170F29AF059C53
            filter-version: 0.0_DummyVersion_20090101_1830
            filter-id     : cisco-sa-20090101-dummy_ddts_001
```

```
Match start TCP payload-start offset 0 size 10 regex "abc.*def"
Match field TCP source-port eq 1234
```

The table below describes the significant fields shown in the display.

***Table 50: show class-map Field DescriptionsA number in parentheses may appear next to the class-map name and match criteria information. The number is for Cisco internal use only and can be disregarded.***

| Field | Description |
|---|---|
| Class Map | Class of traffic being displayed. Output is displayed for each configured class map in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| Match | Match criteria specified for the class map. Criteria include the Frame Relay DLCI number, Layer 3 packet length, IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) groups. |

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **match fr-dlci** | Specifies the Frame Relay DLCI number as a match criterion in a class map. |
| **match packet length (class-map)** | Specifies and uses the length of the Layer 3 packet in the IP header as a match criterion in a class map. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# show class-map type nat

To display network address translation (NAT) class maps and their matching criteria, use the **showclass-maptypenat**command in privileged EXEC mode.

**show class-map type nat** [ *class-map-name* ]

## Syntax Description

| | |
|---|---|
| *class-map-name* | (Optional) Name of the NAT class map. The name can be a maximum of 40 alphanumeric characters. |

## Command Default

Information for all NAT class maps is displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

The **showclass-maptypenat**command displays all NAT class maps and their matching criteria. To display a particular NAT class map and its matching criteria, specify the class-map name.

## Examples

The following is sample output from the **showclass-maptypenat**command that disaplays all the class maps:

```
Router# show class-map type nat
Class Map match-all ipnat-class-acl-we (id 5)
   Match access-group  0
```

The table below describes the significant fields shown in the display.

***Table 51: show class-map type nat Field Descriptions***

| Field | Description |
|---|---|
| Class Map | Displays the name of the class map along with the conditions applied for the class map to match the incoming packets. |
| Match | Match criteria specified for the class map. |

## Related Commands

| Command | Description |
|---|---|
| **show class-map type inspect** | Displays Layer 3 and Layer 4 or Layer 7 (application-specific) inspect type class maps and their matching criteria. |
| **show class-map type port-filter** | Displays port-filter class maps and their matching criteria. |

# show class-map type port-filter

To display class maps for port filters and their matching criteria, use the **showclass-maptypeport-filter** command in privileged EXEC mode.

**show class-map type port-filter** [ *class-map-name* ]

## Syntax Description

| | |
|---|---|
| *class-map-name* | (Optional) Name of the port-filter class map. The name can be a maximum of 40 alphanumeric characters. |

## Command Default

If no argument is specified, information for all port-filter class maps is displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Usage Guidelines

Use the **showclass-maptypeport-filter** command to display TCP/UDP port policing of control plane packets. The **showclass-maptypeport-filter**command displays all port-filter class maps and their matching criteria. To display class maps for a particular port-filter class map, specify the class map name.

## Examples

The following is sample output from the **showclass-maptypeport-filter** command that displays all the class maps:

```
Router# show class-map type port-filter
Class Map type port-filter match-all pf-policy (id 9)
   Match  port tcp 45 56
 Class Map type port-filter match-any cl1 (id 4)
   Match none
 Class Map type port-filter match-all pf-class (id 8)
   Match not  port udp 123
   Match  closed-ports
```

The following is sample output from the **showclass-maptypeport-filter** command that displays the class map pf-class:

```
Router# show class-map type port-filter pf-class
Class Map type port-filter match-all pf-class (id 8)
   Match not  port udp 123
   Match  closed-ports
```

The table below describes the significant fields shown in the display.

*Table 52: show class-map type port-filter Field Descriptions*

| Field | Description |
|---|---|
| Class Map | Port-filter class maps being displayed. Output is displayed for each configured class map. The choice for implementing class matches (for example, match-all or match-any) appears next to the traffic class. |
| Match | Match criteria specified for the class map. Valid matching criteria are **closed-ports**, **not**, and **port**. |

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to a specified class. |

# show control-plane cef-exception counters

To display the control-plane packet counters for the control-plane cef-exception subinterface, use the **showcontrol-planecef-exceptioncounters** command in privileged EXEC mode.

**show control-plane cef-exception counters**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |

## Usage Guidelines

The**showcontrol-planecef-exceptioncounters** command displays the following packet counts for features configured on the control-plane cef-exception subinterface:

- Total number of packets that were processed by the cef-exception subinterface
- Total of packets that were dropped
- Total number of errors

## Examples

The following is sample output from the **showcontrol-planecef-exceptioncounters** command:

```
Router# show control-plane cef-exception counters
 Control plane cef-exception path counters:
 Feature      Packets Processed/Dropped/Errors
 Control Plane Policing       63456/9273/0
```

The table below describes the significant fields shown in the display.

***Table 53: show control-plane cef-exception counters Field Descriptions***

| Field | Description |
|---|---|
| Feature | Name of the configured feature on this subinterface. |
| Packets Processed | Total number of packets that were processed by the feature. |
| Dropped | Total number of packets that were dropped by the feature. |
| Errors | Total number of errors detected by the feature. |

## Related Commands

| Command | Description |
|---|---|
| **clear control-plane** | Clears packet counters for control-plane interfaces and subinterfaces. |
| **control-plane** | Enters control-plane configuration mode, which allows you to associate or modify attributes or parameters that are associated with the control-plane of the device. |
| **debug control-plane** | Displays debugging output from the control-plane routines. |
| **show control-plane cef-exception features** | Displays the configured features for the control-plane CEF-exception subinterface. |
| **show control-plane counters** | Displays the control-plane packet counters for the aggregate control-plane interface. |
| **show control-plane features** | Displays the configured features for the aggregate control-plane interface. |
| **show control-plane host counters** | Displays the control-plane packet counters for the control-plane host subinterface. |
| **show control-plane host features** | Displays the configured features for the control-plane host subinterface. |
| **show control-plane host open-ports** | Displays a list of open TCP/UDP ports that are registered with the port-filter database. |
| **show control-plane transit counters** | Displays the control-plane packet counters for the control-plane transit subinterface. |

# show control-plane cef-exception features

To display the control-plane features for control-plane cef-exception subinterface, use the **showcontrol-planecef-exceptionfeatures** command in privileged EXEC mode.

**show control-plane cef-exception features**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |

## Usage Guidelines

The**showcontrol-planecef-exceptionfeatures** command displays the following aggregate feature configurations for the control-plane cef-exception subinterface:

- Number of features configured for the control-plane cef-exception subinterface.
- Name of the feature
- Date and time the feature was activated

## Examples

The following is sample output from the **showcontrol-planecef-exceptionfeatures** command:

```
Router# show control-plane cef-exception features
 Total 1 features configure
  Control plane cef-exception path features:
  Control Plane Policing activated Nov 09 2005 12:40
```

The table below describes the significant fields shown in the display.

***Table 54: show control-plane cef-exception features Field Descriptions***

| Field | Description |
|---|---|
| Total features configured | Number of features configured. |
| Feature Name | Name of the configured features. |
| Activated | Date and time the feature was activated. |

## Related Commands

| Command | Description |
|---|---|
| **clear control-plane** | Clears packet counters for control-plane interfaces and subinterfaces. |
| **control-plane** | Enters control-plane configuration mode, which allows you to associate or modify attributes or parameters that are associated with the control-plane of the device. |
| **debug control-plane** | Displays debugging output from the control-plane routines. |
| **show control-plane cef-exception counters** | Displays the control-plane packet counters for the control-plane CEF-exception subinterface. |
| **show control-plane counters** | Displays the control-plane packet counters for the aggregate control-plane interface. |
| **show control-plane features** | Displays the configured features for the aggregate control-plane interface. |
| **show control-plane host counters** | Displays the control-plane packet counters for the control-plane host subinterface. |
| **show control-plane host features** | Displays the configured features for the control-plane host subinterface. |
| **show control-plane host open-ports** | Displays a list of open TCP/UDP ports that are registered with the port-filter database. |
| **show control-plane transit counters** | Displays the control-plane packet counters for the control-plane transit subinterface. |

# show control-plane counters

To display the control-plane counters for all control-plane interfaces, use the **showcontrol-planecounters** command in privileged EXEC mode.

**show control-plane counters**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |

## Usage Guidelines

The**showcontrol-planecounters** command displays the following aggregate packet counts for all control-plane interfaces and subinterface:

- Total number of packets that were processed by control-plane aggregate host, transit, and cef-exception subinterfaces
- Total number of packets that were dropped
- Total number of errors

## Examples

The following is sample output from the **showcontrol-planecounters** command:

```
Router# show control-plane counters
 Feature Path     Packets Processed/Dropped/Errors
  aggregate      43271/6759/0
  host      24536/4238/0
  transit      11972/2476/0
     cef-exception path       6345/0/0
```

The table below describes the significant fields shown in the display.

***Table 55: show control-plane counters Field Descriptions***

| Field | Description |
|---|---|
| Feature | Name of the interface or subinterface displayed. |
| Packets Processed | Total number of packets that were processed by the subinterface. |
| Dropped | Total number of packets that were dropped. |

| Field | Description |
|---|---|
| Errors | Total number of errors detected. |

## Related Commands

| Command | Description |
|---|---|
| **clear control-plane** | Clears packet counters for control-plane interfaces and subinterfaces. |
| **control-plane** | Enters control-plane configuration mode, which allows you to associate or modify attributes or parameters that are associated with the control-plane of the device. |
| **debug control-plane** | Displays debugging output from the control-plane routines. |
| **show control-plane cef-exception counters** | Displays the control-plane packet counters for the control-plane CEF-exception subinterface. |
| **show control-plane cef-exception features** | Displays the configured features for the control-plane CEF-exception subinterface. |
| **show control-plane features** | Displays the configured features for the aggregate control-plane interface. |
| **show control-plane host counters** | Displays the control-plane packet counters for the control-plane host subinterface. |
| **show control-plane host features** | Displays the configured features for the control-plane host subinterface. |
| **show control-plane host open-ports** | Displays a list of open TCP/UDP ports that are registered with the port-filter database. |
| **show control-plane transit counters** | Displays the control-plane packet counters for the control-plane transit subinterface. |
| **show control-plane transit features** | Displays the configured features for the control-plane transit subinterface. |

# show control-plane features

To display the configured control-plane features, use the **showcontrol-planefeatures** command in privileged EXEC mode.

**show control-plane features**

## Syntax Description

This command has no arguments or keywords

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |

## Usage Guidelines

The**showcontrol-planefeatures** command displays control-plane features enabled on the control-plane aggregate sub-interfaces. Information includes the following:

- Number of features configured for the control plane
- Name of the feature
- Date and time the feature was activated

## Examples

The following is sample output from the **showcontrol-planefeatures** command:

```
Router# show control-plane features
 Total 1 features configured
  Control plane host path features:
  TCP/UDP Portfilter activated Nov 09 2005 12:40
```

The table below describes the significant fields shown in the display.

***Table 56: show control-plane features Field Descriptions***

| Field | Description |
|---|---|
| Total features configured | Number of features configured. |
| Feature Name | Name of the configured features. |
| activated | Date and time the feature was activated. |

## Related Commands

| Command | Description |
|---|---|
| **clear control-plane** | Clears packet counters for control-plane interfaces and subinterfaces. |
| **control-plane** | Enters control-plane configuration mode, which allows you to associate or modify attributes or parameters that are associated with the control-plane of the device. |
| **debug control-plane** | Displays debugging output from the control-plane routines. |
| **show control-plane cef-exception counters** | Displays the control-plane packet counters for the control-plane CEF-exception subinterface. |
| **show control-plane cef-exception features** | Displays the configured features for the control-plane CEF-exception subinterface. |
| **show control-plane counters** | Displays the control-plane packet counters for the aggregate control-plane interface. |
| **show control-plane host counters** | Displays the control-plane packet counters for the control-plane host subinterface. |
| **show control-plane host features** | Displays the configured features for the control-plane host subinterface. |
| **show control-plane host open-ports** | Displays a list of open TCP/UDP ports that are registered with the port-filter database. |
| **show control-plane transit counters** | Displays the control-plane packet counters for the control-plane transit subinterface. |
| **show control-plane transit features** | Displays the configured features for the control-plane transit subinterface. |

# show control-plane host counters

To display the control-plane packet counters for the control-plane host subinterface, use the **showcontrol-planehostcounters** command in privileged EXEC mode.

**show control-plane host counters**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |

## Usage Guidelines

The**showcontrol-planehostcounters** command displays the following packet counts for the control-plane host subinterface:

- Total number of packets that were processed by features configured on the host subinterface
- Total number of packets that were dropped
- Total number of errors

## Examples

The following is sample output from the **showcontrol-planehostcounters** command:

```
Router# show control-plane host counters
 Control plane host path counters:
 Feature      Packets Processed/Dropped/Errors
 TCP/UDP portfilter       46/46/0
```

The table below describes the significant fields shown in the display.

***Table 57: show control-plane host counters Field Descriptions***

| Field | Description |
|---|---|
| Feature | Name of the feature configured on the host subinterface. |
| Packets Processed | Total number of packets that were processed by the feature. |
| Dropped | Total number of packets that were dropped. |
| Errors | Total number of errors detected. |

## Related Commands

| Command | Description |
|---|---|
| **clear control-plane** | Clears packet counters for control-plane interfaces and subinterfaces. |
| **control-plane** | Enters control-plane configuration mode, which allows you to associate or modify attributes or parameters that are associated with the control-plane of the device. |
| **debug control-plane** | Displays debugging output from the control-plane routines. |
| **show control-plane cef-exception counters** | Displays the control-plane packet counters for the control-plane CEF-exception subinterface. |
| **show control-plane cef-exception features** | Displays the configured features for the control-plane CEF-exception subinterface. |
| **show control-plane counters** | Displays the control-plane packet counters for the aggregate control-plane interface. |
| **show control-plane features** | Displays the configured features for the aggregate control-plane interface. |
| **show control-plane host features** | Displays the configured features for the control-plane host subinterface. |
| **show control-plane host open-ports** | Displays a list of open TCP/UDP ports that are registered with the port-filter database. |
| **show control-plane transit counters** | Displays the control-plane packet counters for the control-plane transit subinterface. |
| **show control-plane transit features** | Displays the configured features for the control plane transit subinterface. |

# show control-plane host features

To display the configured control-plane features for the control-plane host sub-interface, use the **showcontrol-planehostfeatures** command in privileged EXEC mode.

**show control-plane host features**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |

## Usage Guidelines

The**showcontrol-planehostfeatures** command displays the features configured for the control-plane host subinterface. Information includes the following:

- Number of features configured for the control plane
- Name of the feature
- Date and time the feature was activated

## Examples

The following is sample output from the **showcontrol-planehostfeatures** command:

```
Router# show control-plane host features
   Control plane host path features:
  TCP/UDP Portfilter activated Nov 09 2005 12:40
```

The table below describes the significant fields shown in the display.

***Table 58: show control-plane host features Field Descriptions***

| Field | Description |
|---|---|
| Feature Name | Name of the configured features. |
| activated | Date and time the feature was activated. |

## Related Commands

| Command | Description |
|---|---|
| **clear control-plane** | Clears packet counters for control-plane interfaces and subinterfaces. |
| **control-plane** | Enters control-plane configuration mode, which allows you to associate or modify attributes or parameters that are associated with the control plane of the device. |
| **debug control-plane** | Displays debugging output from the control-plane routines. |
| **show control-plane cef-exception counters** | Displays the control plane packet counters for the control-plane CEF-exception subinterface. |
| **show control-plane cef-exception features** | Displays the configured features for the control-plane CEF-exception subinterface. |
| **show control-plane counters** | Displays the control-plane packet counters for the aggregate control-plane interface. |
| **show control-plane features** | Displays the configured features for the aggregate control-plane interface. |
| **show control-plane host counters** | Displays the control-plane packet counters for the control-plane host subinterface. |
| **show control-plane host open-ports** | Displays a list of open TCP/UDP ports that are registered with the port-filter database. |
| **show control-plane transit counters** | Displays the control-plane packet counters for the control-plane transit subinterface. |
| **show control-plane transit features** | Displays the configured features for the control-plane transit subinterface. |

# show control-plane host open-ports

To display a list of open TCP/UDP ports that are registered with the port-filter database, use the **showcontrol-planehostopen-ports** command in privileged EXEC mode.

**show control-plane host open-ports**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |

## Usage Guidelines

The**showcontrol-planehostopen-ports** command displays a list of open TCP/UDP ports that are registered with the port-filter database.

## Examples

The following is sample output from the**showcontrol-planehostopen-ports** command.

```
Router# show control-plane host open-ports

Active internet connections (servers and established)
Port        Local Address      Foreign Address                 Service    State
 tcp                *:23                *:0                    Telnet   LISTEN
 tcp                *:53                *:0                DNS Server   LISTEN
 tcp                *:80                *:0                 HTTP CORE   LISTEN
 tcp              *:1720                *:0                     H.225   LISTEN
 tcp              *:5060                *:0                       SIP   LISTEN
 tcp                *:23     192.0.2.18:58714               Telnet   ESTABLISHED
 udp                *:53                *:0                DNS Server   LISTEN
 udp                *:67                *:0            DHCPD Receive   LISTEN
 udp             *:52824                *:0                   IP SNMP   LISTEN
 udp               *:161                *:0                   IP SNMP   LISTEN
 udp               *:162                *:0                   IP SNMP   LISTEN
 udp              *:5060                *:0                       SIP   LISTEN
 udp              *:2517                *:0                 CCH323_CT   LISTEN
```

The table below describes the significant fields shown in the display.

***Table 59: show control-plane host open-ports Field Descriptions***

| Field | Description |
|---|---|
| Port | Port type, either TCP or UDP. |
| Local Address | Local IP address and port number. An asterisk (*) indicates that the service is listening on all configured network interfaces. |

| Field | Description |
|---|---|
| Foreign Address | Remote IP address and port number. An asterisk (*) indicates that the service is listening on all configured network interfaces. |
| Service | Name of the configured Cisco IOS service listening on the port. |
| State | Listen or Established. |

## Related Commands

| Command | Description |
|---|---|
| **clear control-plane** | Clears packet counters for control-plane interfaces and subinterfaces. |
| **control-plane** | Enters control-plane configuration mode, which allows you to associate or modify attributes or parameters that are associated with the control plane of the device. |
| **debug control-plane** | Displays debugging output from the control-plane routines. |
| **show control-plane cef-exception counters** | Displays the control-plane packet counters for the control-plane CEF-exception subinterface. |
| **show control-plane cef-exception features** | Displays the configured features for the control-plane CEF-exception subinterface. |
| **show control-plane counters** | Displays the control-plane packet counters for the aggregate control-plane interface. |
| **show control-plane features** | Displays the configured features for the aggregate control-plane interface. |
| **show control-plane host counters** | Displays the control plane packet counters for the control-plane host subinterface. |
| **show control-plane host features** | Displays the configured features for the control-plane host subinterface. |
| **show control-plane transit counters** | Displays the control plane packet counters for the control-plane transit subinterface. |
| **show control-plane transit features** | Displays the configured features for the control-plane transit subinterface. |

# show control-plane transit counters

To display the control-plane packet counters for the control-plane transit sub-interface, use the **showcontrol-planetransitcounters** command in privileged EXEC mode.

**show control-plane transit counters**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |

## Usage Guidelines

The**showcontrol-planetransitcounters** command displays the following packet counts for the control-plane transit subinterface:

- Total number of packets that were processed by the transit subinterface
- Total number of packets that were dropped
- Total number of errors

## Examples

The following is sample output from the **showcontrol-planetransitcounters** command.

```
Router# show control-plane transit counters
 Control plane transit path counters:
 Feature      Packets Processed/Dropped/Errors
     Control Plane Policing       63456/2391/0
```

The table below describes the significant fields shown in the display.

***Table 60: show control-plane transit counters Field Descriptions***

| Field | Description |
|---|---|
| Feature | Name of the feature configured on the transit sub-interface. |
| Packets Processed | Total number of packets that were processed by the configured feature. |
| Dropped | Total number of packets that were dropped. |
| Errors | Total number of errors detected. |

## Related Commands

| Command | Description |
|---|---|
| **clear control-plane** | Clears packet counters for control-plane interfaces and subinterfaces. |
| **control-plane** | Enters control-plane configuration mode, which allows you to associate or modify attributes or parameters that are associated with the control plane of the device. |
| **debug control-plane** | Displays debugging output from the control-plane routines. |
| **show control-plane cef-exception counters** | Displays the control plane packet counters for the control-plane CEF-exception subinterface. |
| **show control-plane cef-exception features** | Displays the configured features for the control-plane CEF-exception subinterface. |
| **show control-plane counters** | Displays the control-plane packet counters for the aggregate control-plane interface. |
| **show control-plane features** | Displays the configured features for the aggregate control-plane interface. |
| **show control-plane host counters** | Displays the control plane packet counters for the control-plane host subinterface. |
| **show control-plane host features** | Displays the configured features for the control-plane host subinterface. |
| **show control-plane host open-ports** | Displays a list of open TCP/UDP ports that are registered with the port-filter database. |
| **show control-plane transit features** | Displays the configured features for the control-plane transit subinterface. |

# show control-plane transit features

To display the configured control-plane features for the control-plane transit subinterface, use the **showcontrol-planetransitfeatures**command in privileged EXEC mode.

**show control-plane transit features**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |

## Usage Guidelines

The**showcontrol-planetransitfeatures** command displays the control-plane features configured for the control-plane transit subinterface. Information includes the following:

- Number of features configured for the control plane
- Name of the feature
- Date and time the feature was activated

## Examples

The following is sample output from the **showcontrol-planetransitfeatures** command:

```
Router# show control-plane transit features
  Control plane transit path features:
  Control Plane Policing activated Nov 09 2005 12:40
```

The table below describes the significant fields shown in the display.

***Table 61: show control-plane transit features Field Descriptions***

| Field | Description |
|---|---|
| Total Features Configured | Number of features configured. |
| Feature Name | Name of the configured features. |
| Activated | Date and time the feature was activated. |

## Related Commands

| Command | Description |
|---|---|
| **clear control-plane** | Clears packet counters for control-plane interfaces and subinterfaces. |
| **control-plane** | Enters control-plane configuration mode, which allows you to associate or modify attributes or parameters that are associated with the control plane of the device. |
| **debug control-plane** | Displays debugging output from the control-plane routines. |
| **show control-plane cef-exception counters** | Displays the control-plane packet counters for the control-plane CEF-exception subinterface. |
| **show control-plane cef-exception features** | Displays the configured features for the control-plane CEF-exception subinterface. |
| **show control-plane counters** | Displays the control-plane packet counters for the aggregate control-plane interface. |
| **show control-plane features** | Displays the configured features for the aggregate control-plane interface. |
| **show control-plane host counters** | Displays the control plane packet counters for the control-plane host subinterface. |
| **show control-plane host features** | Displays the configured features for the control-plane host subinterface. |
| **show control-plane host open-ports** | Displays a list of open ports that are registered with the port-filter database. |
| **show control-plane transit counters** | Displays the control-plane packet counters for the control-plane transit subinterface. |

# show cops servers

To display the IP address and connection status of the policy servers for which the router is configured, use the **showcopsservers** command in EXEC mode.

**show cops servers**

## Syntax Description

This command has no keywords or arguments.

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

You can also use the show cops server command to display information about the Common Open Policy Service (COPS) client on the router.

## Examples

In the following example, information is displayed about the current policy server and client. When Client Type appears followed by an integer, 1 stands for Resource Reservation Protocol (RSVP) and 2 stands for Differentiated Services Provisioning. (0 indicates keepalive.)

```
Router# show cops servers
COPS SERVER: Address: 10.0.0.1. Port: 3288. State: 0. Keepalive: 120 sec
Number of clients: 1. Number of sessions: 1.
 COPS CLIENT: Client type: 1.  State: 0.
```

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp policy cops** | Displays policy server address(es), ACL IDs, and current state of the router-server connection. |

# show crypto eng qos

To monitor and maintain low latency queueing (LLQ) for IPSec encryption engines, use the show crypto eng qos command in privileged EXEC mode.

**show crypto eng qos**

## Syntax Description

This command has no keywords or arguments.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced in Cisco IOS Release 12.2(13)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS release 12.(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **show crypto eng qos** command to determine if QoS is enabled on LLQ for IPSec encryption engines.

## Examples

The following example shows how to determine if LLQ for IPSec encryption engines is enabled:

```
Router# show crypto eng qos
crypto engine name: Multi-ISA Using VAM2
        crypto engine type: hardware
                      slot: 5
                  queuing: enabled
         visible bandwidth: 30000 kbps
                   llq size: 0
    default queue size/max: 0/64
      interface table size: 32
  FastEthernet0/0 (3), iftype 1, ctable size 16, input filter:ip
precedence 5
    class voice (1/3), match ip precedence 5
          bandwidth 500 kbps, max token 100000
          IN  match pkt/byte 0/0, police drop 0
          OUT match pkt/byte 0/0, police drop 0
  class default, match pkt/byte 0/0, qdrop 0
  crypto engine bandwidth:total 30000 kbps, allocated 500 kbps
```

The field descriptions in the above display are self-explanatory.

# show crypto entropy status

To display the status of crypto entropy on the Cisco ASR 1000 Series Aggregation Services Routers, use the **show crypto entropy status** command in the EXEC mode.

**show crypto entropy status**

## Syntax Description

This command has no arguments or keywords.

## Command Default

None

## Command Modes

EXEC(#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.7.3S | This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers. |
| Cisco IOS XE Release 3.8S | The command outputs were modified on the Cisco ASR 1000 Series Aggregation Services Routers. |

## Examples

The following is a sample output of the **show crypto entropy status** command when crypto entropy is enabled:

```
Router# show crypto entropy status

# Entropy source       Type Status  Entropy Bits
1 randfill              SW  Working  128(*)
2 getrandombytes        SW  Working  160(*)
3 Nitrox / Octeon       HW  Working  256
(*) - The entropy collected from SW sources were not counted as a part of
      achieving the entropy target!
```

Table 62: Table 1 show crypto entropy status Field Descriptions describes the significant fields shown in the display.

***Table 62: Table 1 show crypto entropy status Field Descriptions***

| Field | Description |
|---|---|
| Entropy source | Source of crypto entropy. |

| Field | Description |
|---|---|
| Type | Type of crypto entropy. It can be one of the following values:<br>• SW-Entropy originated from the software.<br>HW-Entropy originated from the hardware. |
| Status | Status of crypto entropy. It can be one of the following values:<br>• Working-Entropy is working.<br>Offline-Entropy is offline. |
| Entropy Bits | Size of crypto entropy, in bits. |

The following is a sample output of the **show crypto entropy status** command when crypto entropy is disabled:

```
Router# show crypto entropy status

# Entropy source       Type Status  Entropy Bits
1 randfill              SW  Working  128
2 getrandombytes        SW  Working  160
3 Nitrox / Octeon       HW  Offline   --
```

**Note** The fields in the display are explained in Table 62: Table 1 show crypto entropy status Field Descriptions

## Related Commands

| Command | Description |
|---|---|
| platform ipsec fips-mode | |

# show frame-relay ip rtp header-compression

To display Frame Relay Real-Time Transport Protocol (RTP) header compression statistics, use the **showframe-relayiprtpheader-compression**command in user EXEC or privileged EXEC mode.

**show frame-relay ip rtp header-compression** [**interface** *type number*] [ *dlci* ]

## Syntax Description

| | |
|---|---|
| **interface** *type number* | (Optional) Specifies an interface for which information will be displayed. A space between the interface type and number is optional. |
| *dlci* | (Optional) Specifies a data-link connection identifier (DLCI) for which information will be displayed. The range is from 16 to 1022. |

## Command Default

RTP header compression statistics are displayed for all DLCIs on interfaces that have RTP header compression configured.

## Command Modes

User EXEC Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. The output for this command was modified to display RTP header compression statistics for Frame Relay permanent virtual circuit (PVC) bundles. |
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC, and the *dlci* argument was added. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.4(9)T | The *dlci* argument was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(11)T | The output for this command was modified to display Enhanced Compressed Real-Time Transport Protocol (ECRTP) header compression statistics for Frame Relay permanent virtual circuit (PVC) bundles. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Examples

The following is sample output from the **showframe-relayiprtpheader-compression**command:

```
Router# show frame-relay ip rtp header-compression
 DLCI 21         Link/Destination info: ip 10.1.4.1
  Interface Serial3/0 DLCI 21 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
 DLCI 20         Link/Destination info: ip 10.1.1.1
  Interface Serial3/1 DLCI 20 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
 DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface Serial3/1 DLCI 21 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
 DLCI 22         Link/Destination info: ip 10.1.3.1
  Interface Serial3/1 DLCI 22 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

The following is sample output from the **showframe-relayiprtpheader-compression**command when ECRTP is enabled:

```
Router# show frame-relay ip rtp header-compression
 DLCI 16         Link/Destination info: ip 10.0.0.1
  Interface Serial4/1 DLCI 16 (compression on, IETF, ECRTP)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 16 rx slots, 16 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 16 free contexts
```

In the following example, the **showframe-relayiprtpheader-compression** command displays information about DLCI 21:

```
Router# show frame-relay ip rtp header-compression 21
 DLCI 21         Link/Destination info: ip 10.1.4.1
  Interface Serial3/0 DLCI 21 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
 DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface Serial3/1 DLCI 21 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
```

```
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

In the following example, the **showframe-relayiprtpheader-compression** command displays information for all DLCIs on serial interface 3/1:

```
Router# show frame-relay ip rtp header-compression interface serial3/1
 DLCI 20         Link/Destination info: ip 10.1.1.1
  Interface Serial3/1 DLCI 20 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
 DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface Serial3/1 DLCI 21 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
 DLCI 22         Link/Destination info: ip 10.1.3.1
  Interface Serial3/1 DLCI 22 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

In the following example, the **showframe-relayiprtpheader-compression** command displays information only for DLCI 21 on serial interface 3/1:

```
Router# show frame-relay ip rtp header-compression interface serial3/1 21
 DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface Serial3/1 DLCI 21 (compression on, Cisco)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

The following sample output from the **showframe-relayiprtpheader-compression** command shows statistics for a PVC bundle called MP-3-static:

```
Router# show frame-relay ip rtp header-compression interface Serial1/4
 vc-bundle MP-3-static      Link/Destination info:ip 10.1.1.1
  Interface Serial1/4:
    Rcvd:   14 total, 13 compressed, 0 errors
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:   15 total, 14 compressed,
             474 bytes saved, 119 bytes sent
             4.98 efficiency improvement factor
    Connect:256 rx slots, 256 tx slots,
             1 long searches, 1 misses 0 collisions, 0 negative cache hits
             93% hit ratio, five minute miss rate 0 misses/sec, 0 max
```

The table below describes the significant fields shown in the displays.

***Table 63: show frame-relay ip rtp header-compression Field Descriptions***

| Field | Description |
|---|---|
| Interface | Type and number of the interface and type of header compression. |

| Field | Description |
|---|---|
| Rcvd: | Table of details concerning received packets. |
| total | Number of packets received on the interface. |
| compressed | Number of packets with compressed headers. |
| errors | Number of errors. |
| dropped | Number of dropped packets. |
| buffer copies | Number of buffers that were copied. |
| buffer failures | Number of failures in allocating buffers. |
| Sent: | Table of details concerning sent packets. |
| total | Total number of packets sent. |
| compressed | Number of packets sent with compressed headers. |
| bytes saved | Total savings in bytes because of compression. |
| bytes sent | Total bytes sent after compression. |
| efficiency improvement factor | Compression efficiency. |
| Connect: | Table of details about the connections. |
| rx slots | Total number of receive slots. |
| tx slots | Total number of transmit slots. |
| long searches | Searches that needed more than one lookup. |
| misses | Number of new states that were created. |
| hit ratio | Number of times that existing states were revised. |
| five minute miss rate | Average miss rate. |
| max | Maximum miss rate. |

## Related Commands

| Command | Description |
|---|---|
| **frame-relay ip rtp compression-connections** | Specifies the maximum number of RTP header compression connections on a Frame Relay interface. |

| Command | Description |
|---|---|
| **frame-relay ip rtp header-compression** | Enables RTP header compression for all Frame Relay maps on a physical interface. |
| **frame-relay map ip compress** | Enables both RTP and TCP header compression on a link. |
| **frame-relay map ip nocompress** | Disables both RTP and TCP header compression on a link. |
| **frame-relay map ip rtp header-compression** | Enables RTP header compression per DLCI. |
| **show ip rpf events** | Displays RTP header compression statistics. |

# show frame-relay ip tcp header-compression

To display Frame Relay Transmission Control Protocol (TCP)/IP header compression statistics, use the **showframe-relayiptcpheader-compression** command in user EXEC or privileged EXEC mode.

**show frame-relay ip tcp header-compression** [**interface** *type number*] [ *dlci* ]

## Syntax Description

| | |
|---|---|
| **interface** *type number* | (Optional) Specifies an interface for which information will be displayed. A space is optional between the type and number. |
| *dlci* | (Optional) Specifies a data-link connection identifier (DLCI) for which information will be displayed. Range is from 16 to 1022. |

## Command Modes

User EXEC Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |
| 12.2(13)T | This command was integrated into Cisco IOS Release 12.2(13)T. The command was modified to support display of RTP header compression statistics for Frame Relay permanent virtual circuit (PVC) bundles. |
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC, and the *dlci* argument was added. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.4(9)T | The *dlci* argument was added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Examples

The following is sample output from the**showframe-relayiptcpheader-compression** command:

```
Router# show frame-relay ip tcp header-compression
DLCI 200          Link/Destination info: ip 10.108.177.200
Interface Serial0:
```

```
Rcvd:     40 total, 36 compressed, 0 errors
          0 dropped, 0 buffer copies, 0 buffer failures
Sent:     0 total, 0 compressed
          0 bytes saved, 0 bytes sent
Connect:  16 rx slots, 16 tx slots, 0 long searches, 0 misses, 0% hit ratio
          Five minute miss rate 0 misses/sec, 0 max misses/sec
```

The following sample output from the **showframe-relayiptcpheader-compression**command shows statistics for a PVC bundle called “MP-3-static”:

```
Router# show frame-relay ip tcp header-compression interface Serial1/4
 vc-bundle MP-3-static      Link/Destination info:ip 10.1.1.1
  Interface Serial1/4:
    Rcvd:   14 total, 13 compressed, 0 errors
            0 dropped, 0 buffer copies, 0 buffer failures
    Sent:   15 total, 14 compressed,
            474 bytes saved, 119 bytes sent
            4.98 efficiency improvement factor
    Connect:256 rx slots, 256 tx slots,
            1 long searches, 1 misses 0 collisions, 0 negative cache hits
            93% hit ratio, five minute miss rate 0 misses/sec, 0 max
```

In the following example, the **showframe-relayiptcpheader-compression** command displays information about DLCI 21:

```
Router# show frame-relay ip tcp header-compression 21
DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface POS2/0 DLCI 21 (compression on, VJ)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
DLCI 21         Link/Destination info: ip 10.1.4.1
  Interface Serial3/0 DLCI 21 (compression on, VJ)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

The following is sample output from the**showframe-relayiptcpheader-compression** command for a specific DLCI on a specific interface:

```
Router# show frame-relay ip tcp header-compression pos2/0 21
DLCI 21         Link/Destination info: ip 10.1.2.1
  Interface POS2/0 DLCI 21 (compression on, VJ)
    Rcvd:    0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
    Connect: 256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

The table below describes the fields shown in the display.

***Table 64: show frame-relay ip tcp header-compression Field Descriptions***

| Field | Description |
|---|---|
| Rcvd: | Table of details concerning received packets. |
| total | Sum of compressed and uncompressed packets received. |

| Field | Description |
|---|---|
| compressed | Number of compressed packets received. |
| errors | Number of errors caused by errors in the header fields (version, total length, or IP checksum). |
| dropped | Number of packets discarded. Seen only after line errors. |
| buffer failures | Number of times that a new buffer was needed but was not obtained. |
| Sent: | Table of details concerning sent packets. |
| total | Sum of compressed and uncompressed packets sent. |
| compressed | Number of compressed packets sent. |
| bytes saved | Number of bytes reduced because of the compression. |
| bytes sent | Actual number of bytes transmitted. |
| Connect: | Table of details about the connections. |
| rx slots, tx slots | Number of states allowed over one TCP connection. A state is recognized by a source address, a destination address, and an IP header length. |
| long searches | Number of times that the connection ID in the incoming packet was not the same as the previous one that was processed. |
| misses | Number of times that a matching entry was not found within the connection table and a new entry had to be entered. |
| hit ratio | Percentage of times that a matching entry was found in the compression tables and the header was compressed. |
| Five minute miss rate | Miss rate computed over the most recent 5 minutes and the maximum per-second miss rate during that period. |

# show interfaces fair-queue

**Note** Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **showinterfacesfair-queue**command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide* .

**Note** Effective with Cisco IOS XE Release 3.2S, the **showinterfacesfair-queue**command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide*.

To display information and statistics about weighted fair queueing (WFQ) for a Versatile Interface Processor (VIP)-based interface, use the **showinterfacesfair-queue**command in EXEC mode.

**show interfaces** [*type number*] **fair-queue**

## Syntax Description

| | |
|---|---|
| *type* | (Optional) The type of the interface. |
| *number* | (Optional) The number of the interface. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 11.1CC | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.6 | This command was modified. This command was hidden. |
| 15.0(1)S | This command was modified. This command was hidden. |

| Release | Modification |
|---|---|
| 15.1(3)T | This command was modified. This command was hidden. |
| Cisco IOS XE Release 3.2S | This command was replaced by an MQC command (or sequence of MQC commands). |

## Examples

The following is sample output from the **showinterfacesfair-queue** command for VIP-distributed WFQ (DWFQ):

```
Router# show interfaces fair-queue
Hssi0/0/0 queue size 0
        packets output 1417079, drops 2
 WFQ: aggregate queue limit 54, individual queue limit 27
    max available buffers 54

     Class 0: weight 10 limit 27 qsize 0 packets output 1150 drops 0
     Class 1: weight 20 limit 27 qsize 0 packets output 0 drops 0
     Class 2: weight 30 limit 27 qsize 0 packets output 775482 drops 1
     Class 3: weight 40 limit 27 qsize 0 packets output 0 drops 0
```

The table below ddescribes the significant fields shown in the display.

***Table 65: show interfaces fair-queue Field Descriptions***

| Field | Description |
|---|---|
| queue size | Current output queue size for this interface. |
| packets output | Number of packets sent out this interface or number of packets in this class sent out the interface. |
| drops | Number of packets dropped or number of packets in this class dropped. |
| aggregate queue limit | Aggregate limit, in number of packets. |
| individual queue limit | Individual limit, in number of packets. |
| max available buffers | Available buffer space allocated to aggregate queue limit, in number of packets. |
| Class | QoS group or type of service (ToS) class. |
| weight | Percent of bandwidth allocated to this class during periods of congestion. |
| limit | Queue limit for this class in number of packets. |
| qsize | Current size of the queue for this class. |

## Related Commands

| Command | Description |
|---|---|
| **show interfaces** | Displays statistics for all interfaces configured on the router or access server. |

# show interfaces random-detect

**Note** Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **showinterfacesrandom-detect**command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide* .

**Note** Effective with Cisco IOS XE Release 3.2S, the **showinterfacesrandom-detect**command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* .

To display information about Weighted Random Early Detection (WRED) for a Versatile Interface Processor (VIP)-based interface, use the **showinterfacesrandom-detect**command in EXEC mode.

**show interfaces** [*type number*] **random-detect**

## Syntax Description

| | |
|---|---|
| *type* | (Optional) The type of the interface. |
| *number* | (Optional) The number of the interface. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 11.1CC | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.6 | This command was modified. This command was hidden. |
| 15.0(1)S | This command was modified. This command was hidden. |

| Release | Modification |
|---|---|
| 15.1(3)T | This command was modified. This command was hidden. |
| Cisco IOS XE Release 3.2S | This command was replaced by an MQC command (or sequence of MQC commands). |

## Examples

The following is sample output from the **showinterfacesrandom-detect** command for VIP-distributed WRED (DWRED):

```
Router# show interfaces random-detect
 FastEthernet1/0/0 queue size 0
        packets output 29692, drops 0
 WRED: queue average 0
       weight 1/512
      Precedence 0: 109 min threshold, 218 max threshold, 1/10 mark weight
        1 packets output, drops: 0 random, 0 threshold
      Precedence 1: 122 min threshold, 218 max threshold, 1/10 mark weight
         (no traffic)
      Precedence 2: 135 min threshold, 218 max threshold, 1/10 mark weight
        14845 packets output, drops: 0 random, 0 threshold
      Precedence 3: 148 min threshold, 218 max threshold, 1/10 mark weight
         (no traffic)
      Precedence 4: 161 min threshold, 218 max threshold, 1/10 mark weight
         (no traffic)
      Precedence 5: 174 min threshold, 218 max threshold, 1/10 mark weight
         (no traffic)
      Precedence 6: 187 min threshold, 218 max threshold, 1/10 mark weight
        14846 packets output, drops: 0 random, 0 threshold
      Precedence 7: 200 min threshold, 218 max threshold, 1/10 mark weight
         (no traffic)
```

The table below describes the significant fields shown in the display.

***Table 66: show interfaces random-detect Field Descriptions***

| Field | Description |
|---|---|
| queue size | Current output queue size for this interface. |
| packets output | Number of packets sent out this interface. |
| drops | Number of packets dropped. |
| queue average | Average queue length. |
| weight | Weighting factor used to determine the average queue size. |
| Precedence | WRED parameters for this precedence. |
| min threshold | Minimum threshold for this precedence. |
| max threshold | Maximum length of the queue. When the average queue is this long, any additional packets will be dropped. |

| Field | Description |
|---|---|
| mark weight | Probability of a packet being dropped if the average queue is at the maximum threshold. |
| packets output | Number of packets with this precedence that have been sent. |
| random | Number of packets dropped randomly through the WRED process. |
| threshold | Number of packets dropped automatically because the average queue was at the maximum threshold length. |
| (no traffic) | No packets with this precedence. |

## Related Commands

| Command | Description |
|---|---|
| **random-detect (interface)** | Enables WRED or DWRED. |
| **random-detect flow** | Enables flow-based WRED. |
| **show interfaces** | Displays statistics for all interfaces configured on the router or access server. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# show interfaces rate-limit

To display information about committed access rate (CAR) for an interface, use the **showinterfacesrate-limit**command in EXEC mode.

**show interfaces** [*type number*] **rate-limit**

## Syntax Description

| | |
|---|---|
| *type* | (Optional) The type of the interface. |
| *number* | (Optional) The number of the interface. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 11.1CC | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Examples

The following is sample output from the **showinterfacesrate-limit** command:

```
Router# show interfaces fddi2/1/0 rate-limit
Fddi2/1/0
 Input
  matches: access-group rate-limit 100
   params: 800000000 bps, 64000 limit, 80000 extended limit
   conformed 0 packets, 0 bytes; action: set-prec-continue 1
   exceeded 0 packets, 0 bytes; action: set-prec-continue 0
   last packet: 4737508ms ago, current burst: 0 bytes
   last cleared 01:05:47 ago, conformed 0 bps, exceeded 0 bps
  matches: access-group 101
   params: 80000000 bps, 56000 limit, 72000 extended limit
   conformed 0 packets, 0 bytes; action: set-prec-transmit 5
   exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
   last packet: 4738036ms ago, current burst: 0 bytes
   last cleared 01:02:05 ago, conformed 0 bps, exceeded 0 bps
  matches: all traffic
   params: 50000000 bps, 48000 limit, 64000 extended limit
   conformed 0 packets, 0 bytes; action: set-prec-transmit 5
   exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
   last packet: 4738036ms ago, current burst: 0 bytes
   last cleared 01:00:22 ago, conformed 0 bps, exceeded 0 bps
 Output
  matches: all traffic
   params: 80000000 bps, 64000 limit, 80000 extended limit
```

```
  conformed 0 packets, 0 bytes; action: transmit
  exceeded 0 packets, 0 bytes; action: drop
  last packet: 4809528ms ago, current burst: 0 bytes
  last cleared 00:59:42 ago, conformed 0 bps, exceeded 0 bps
```

The table below describes the significant fields shown in the display.

***Table 67: show interfaces rate-limit Field Descriptions***

| Field | Description |
|---|---|
| Input | These rate limits apply to packets received by the interface. |
| matches | Packets that match this rate limit. |
| params | Parameters for this rate limit, as configured by the **rate-limit**command. |
| bps | Average rate, in bits per second. |
| limit | Normal burst size, in bytes. |
| extended limit | Excess burst size, in bytes. |
| conformed | Number of packets that have conformed to the rate limit. |
| action | Conform action. |
| exceeded | Number of packets that have exceeded the rate limit. |
| action | Exceed action. |
| last packet | Time since the last packet, in milliseconds. |
| current burst | Instantaneous burst size at the current time. |
| last cleared | Time since the burst counter was set back to zero by the **clearcounters** command. |
| conformed | Rate of conforming traffic. |
| exceeded | Rate of exceeding traffic. |
| Output | These rate limits apply to packets sent by the interface. |

## Related Commands

| Command | Description |
|---|---|
| **access-list rate-limit** | Configures an access list for use with CAR policies. |
| **clear counters** | Clears the interface counters. |
| **shape** | Specifies average or peak rate traffic shaping. |
| **show access-lists** | Displays the contents of current IP and rate-limit access lists. |
| **show interfaces** | Displays statistics for all interfaces configured on the router or access server. |

# show iphc-profile

To display configuration information for one or more IP Header Compression (IPHC) profiles, use the **showiphc-profile**command in user EXEC or privileged EXEC mode.

**show iphc-profile** [ *profile-name* ]

## Syntax Description

| | |
|---|---|
| *profile-name* | (Optional) Name of an IPHC profile to display. |

## Command Default

If you do not specify an IPHC profile name, all IPHC profiles are displayed.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |
| 12.4(24)T | This command was modified. The output was enhanced to display recoverable loss when EcRTP is configured. |

## Usage Guidelines

### Information Included in Display

The display includes information such as the profile type, the type of header compression enabled, the number of contexts, the refresh period (for Real-Time Transport [RTP] header compression), whether feedback messages are disabled, and the interfaces to which the IPHC profile is attached.

### For More Information About IPHC Profiles

An IPHC profile is used to enable and configure header compression on your network. For more information about using IPHC profiles to configure header compression, see the “Header Compression” module and the “Configuring Header Compression Using IPHC Profiles” module of the *Cisco IOS Quality of Service Solutions Configuration Guide* .

## Examples

The following is sample output from the **showiphc-profile** command. In the output, information about two IPHC profiles, profile19 and profile20, is displayed.

```
Router# show iphc-profile
IPHC Profile "profile19"
Type: IETF
  Compressing: NON-TCP (RTP)
  Contexts   : NON-TCP fixed at 0
  Refresh    : NON-TCP every 5 seconds or 256 packets
  EcRTP      : recoverable loss enabled 1
  Controlled interfaces: (0)
```

```
  Reference Count:  (1)
IPHC Profile "profile20"
Type: IETF
  Compressing: NON-TCP (RTP)
  Contexts   : NON-TCP fixed at 0
  Refresh    : NON-TCP every 5 seconds or 256 packets
  EcRTP      : recoverable loss enabled 4 (dynamic)
  Controlled interfaces: (0)
  Reference Count:  (0)
```

The table below describes the significant fields shown in the display.

***Table 68: show iphc-profile Field Descriptions***

| Field | Description |
|---|---|
| IPHC Profile | IPHC profile name. |
| Type | IPHC profile type: either VJ (for van-jacobson) or IETF. |
| Compressing | Type of header compression used, such as TCP, non-TCP, or RTP. |
| Contexts | Number of contexts and setting used to calculate the context number. |
| Refresh | Indicates maximum number of packets or maximum time between context refresh. |
| EcRTP | Indicates if recoverable loss is enabled and if EcRTP recoverable loss is configured to dynamic. |
| Controlled interfaces | Interfaces to which the IPHC profile is attached. |
| Reference Count | Indicates the number of active IPHC-profile submodes. |

## Related Commands

| Command | Description |
|---|---|
| **iphc-profile** | Creates an IPHC profile. |

# show ip nat translations rsvp

To display active Network Address Translations (NAT) for Resource Reservation Protocol (RSVP) messages, use the **show ip nat translations rsvp** command in privileged EXEC mode.

**show ip nat translations rsvp** [ **vrf** *vrf-name* ]

## Syntax Description

| | |
|---|---|
| **vrf** *vrf-name* | (Optional) Displays VPN routing and forwarding (VRF) traffic-related information. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.2(2)T | This command was introduced. |

## Usage Guidelines

Use the **show ip nat translations rsvp** command to display the IP address/port translations performed by the RSVP-NAT-Application Layer Gateway (ALG) on RSVP packets.

## Examples

The following is sample output from the **show ip nat translations rsvp** command:

```
Router# show ip nat translations rsvp

RSVP-NAT-ALG:
 Inside Local: Address: <ip-address>, Port: <port-number>
 Outside Local: Address: <ip-address>, Port: <port-number>
 Inside Global: Address: <ip-address>, Port: <port-number>
 Outside Global: Address: <ip-address>, Port: <port-number>
 L4-Protocol: <protocol-number>
 Local Path Phop: <ip-address>
 Local Resv Phop: <ip-address>
 Local Resv Confirm: <ip-address>
```

The table below describes the significant fields shown in the display.

***Table 69: show ip nat translations rsvp Field Descriptions***

| Field | Description |
|---|---|
| Inside Local | The IP address and port number assigned to a host on the inside network; probably not a legitimate address assigned by the Network Interface Card (NIC) or service provider. |

| Field | Description |
|---|---|
| Outside Local | IP address and port number of an outside host as it appears to the inside network; probably not a legitimate address assigned by the NIC or service provider. |
| Inside Global | The legitimate IP address and port number that represents one or more inside local IP addresses to the outside world. |
| Outside Global | The IP address and port number assigned to a host on the outside network by its owner. |
| Address | The IP address representing the appropriate category of translation. |
| Port | The port number representing the appropriate category of translation. |
| L4-Protocol | The Layer 4 protocol of the port identifying the address. |
| Local Path Phop | Address of the previous local hop that is used to send the Resv message from global to local. |
| Local Resv Phop | Address of previous local hop that is saved when Resv message comes from local to global. This address is used in traversing the Resv error message. |
| Local Resv Confirm | Address of the local hop saved when processing the Resv message, which is used to traverse the Resv confirm message. |

# show ip nbar attribute

To display the configured attributes used by the Network-Based Application Recognition (NBAR), use the **show ip nbar attribute** command in privileged EXEC mode.

**show ip nbar attribute** [**application-group**| **category**| **encrypted**| **sub-category**| **tunnel**]

## Syntax Description

| | |
|---|---|
| **application-group** | (Optional) Specifies the application-group attribute. |
| **category** | (Optional) Specifies the category attribute. |
| **encrypted** | (Optional) Specifies the encrypted applications. |
| **sub-category** | (Optional) Specifies the subcategory attribute. |
| **tunnel** | (Optional) Specifies the tunneled applications. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.4S | This command was introduced. |

## Usage Guidelines

The **show ip nbar attribute** command displays all the attributes used by the NBAR. Use the keywords to display only the specified attribute.

## Examples

The following is the sample output from the **show ip nbar attribute** command:

```
Router# show ip nbar attribute
      Name :  category
      Help :  category attribute
      Type :  group
    Groups :  email, newsgroup, location-based-services, instant-messaging, netg
      Need :  Mandatory
   Default :  other
      Name :  sub-category
      Help :  sub-category attribute
      Type :  group
    Groups :  routing-protocol, terminal, epayement, remote-access-terminal, nen
      Need :  Mandatory
   Default :  other
      Name :  application-group
      Help :  application-group attribute
      Type :  group
    Groups :  skype-group, wap-group, pop3-group, kerberos-group, tftp-group, bp
      Need :  Mandatory
```

```
Default :  other
   Name :  tunnel
   Help :  Tunnelled applications
   Type :  group
 Groups :  tunnel-no, tunnel-yes, tunnel-unassigned
   Need :  Mandatory
Default :  tunnel-unassigned
   Name :  encrypted
   Help :  Encrypted applications
   Type :  group
 Groups :  encrypted-yes, encrypted-no, encrypted-unassigned
   Need :  Mandatory
Default :  encrypted-unassigned
```

The following table describes the significant fields shown in the display.

***Table 70: show ip nbar attribute Field Descriptions***

| Field | Description |
|---|---|
| Name | Indicates the name of the attribute. |
| Help | Provides the attribute information. |
| Type | Indicates the attribute type. |
| Groups | Specifies the groups within the attribute. |
| Need | Specifies the need of the attribute. |
| Default | Provides the default status of the attribute. |

## Related Commands

| Command | Description |
|---|---|
| **match protocol attribute application-group** | Configures the match criterion for a class map based on the application group. |
| **match protocol attribute category** | Configures the match criterion for a class map based on the category. |
| **match protocol attribute encrypted** | Configures the match criterion for a class map based on the encryption. |
| **match protocol attribute sub-category** | Configures the match criterion for a class map based on the subcategory. |
| **match protocol attribute tunnel** | Configures the match criterion for a class map based on tunneling. |

# show ip nbar link-age

To display the protocol linkage by network-based application recognition (NBAR), use the **showipnbarlink-age**command in privileged EXEC mode.

**show ip nbar link-age** [ *protocol-name* ]

## Syntax Description

| | |
|---|---|
| *protocol-name* | (Optional) Displays the linkage for only the specified protocol name. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(20)T | This command was introduced. |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers. |

## Usage Guidelines

The **showipnbarlink-age** command displays the linkage of all the NBAR protocols. The *protocol-name* argument can be used to limit the display for a specific protocol.

## Examples

The following is sample output from the **showipnbarlink-age** command:

```
Router# show ip nbar link-age

System Link Age: 30 seconds
No.  Protocol                 Link Age (seconds)
1    skype                       120
2  bittorrent                   120
3  winmx                        120
```

The following is sample output from the **showipnbarlink-age** command for a specific protocol:

```
Router# show ip nbar link-age
 eigrp
System Link Age: 30 seconds
Protocol                  Link Age (seconds)
eigrp                        120
```

The table below describes the significant fields shown in the display.

*Table 71: show ip nbar link-age Field Descriptions*

| Field | Description |
|---|---|
| No. | Serial number of the list of protocols displayed. |
| Protocol | Name of the NBAR protocol. |
| Link Age (seconds) | Time, in seconds, at which the links for a protocol are aged (expire). |

## Related Commands

| Command | Description |
|---|---|
| **ip nbar resources protocol** | Sets the expiration time for NBAR flow-link tables on a protocol basis. |

# show ip nbar pdlm

To display the Packet Description Language Module (PDLM) in use by network-based application recognition (NBAR), use the **showipnbarpdlm** command in privileged EXEC mode.

**show ip nbar pdlm**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(5)XE2 | This command was introduced. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.1(13)E | This command was implemented on Catalyst 6000 family switches without FlexWAN modules. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(17a)SX1 | This command was integrated into Cisco IOS Release 12.2(17a)SX1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

This command is used to display a list of all the PDLMs that have been loaded into NBAR using the **ipnbarpdlm**command.

## Examples

In this example of the **showipnbarpdlm** command, the citrix.pdlm PDLM has been loaded from Flash memory:

```
Router# show ip nbar pdlm

The following PDLMs have been loaded:
flash://citrix.pdlm
```

## Related Commands

| Command | Description |
|---|---|
| **ip nbar pdlm** | Extends or enhances the list of protocols recognized by NBAR through a Cisco-provided PDLM. |

# show ip nbar port-map

To display the current protocol-to-port mappings in use by network-based application recognition (NBAR), use the **showipnbarport-map** command in privileged EXEC mode.

**show ip nbar port-map** [*protocol-name* [ *protocol-type* ]]

## Syntax Description

| | |
|---|---|
| *protocol-name* | (Optional) Name of the protocol. For more information on the available protocols, use the question mark (?) online help function. |
| protocol-type | (Optional) Type of the protocol. Two types of protocols can be specified:<br>• **tcp** --Displays information related to Transmission Control Protocol (TCP) ports.<br>• **udp** --Displays information related to User Datagram Protocol (UDP) ports. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)XE2 | This command was introduced. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(13)E | This command was implemented on Catalyst 6000 family switches. The FlexWAN modules were removed. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(17a)SX1 | This command was integrated into Cisco IOS Release 12.2(17a)SX1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(22)T | This command was integrated into Cisco IOS Release 12.4(22)T. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T. |

## Usage Guidelines

The **showipnbarport-map** command displays port assignments for NBAR protocols.

You can use the **showipnbarport-map** command to display the current protocol-to-port mappings in use by NBAR. When you use the **ipnbarport-map** command, the **showipnbarport-map**command displays the ports you have assigned to the protocol. If you do not use the **ipnbarport-map**command to configure any protocol, the **showipnbarport-map** command displays the default ports. Use the *protocol-name* argument to limit the display to a specific protocol. You can either use the UDP or the TCP *protocol-type* argument type.

## Examples

The following is sample output from the **showipnbarport-map** command:

```
Router# show ip nbar port-map
port-map    cuseeme    udp    7648    7649    24032
port-map    cuseeme    tcp    7648    7649
port-map    dhcp       udp    67      68
port-map    dhcp       tcp    67      68
```

The table below describes the significant fields shown in the display.

***Table 72: show ip route track-table Field Descriptions***

| Field | Description |
|---|---|
| port-map | Specifies the ports assigned. |
| cuseeme | Specifies that the CU-SeeMe Protocol is used. |
| udp | Specifies the User Datagram Protocol type. |
| tcp | Specifies the Transmission Control Protocol type. |
| dhcp | Specifies the Dynamic Host Configuration Protocol type. |

## Related Commands

| Command | Description |
|---|---|
| **ip nbar port-map** | Configures NBAR to search for a protocol or protocol name using a port number other than the well-known port number. |

# show ip nbar protocol activated

To display all the activated Network-Based Application Recognition (NBAR) protocols on a device, use the **show ip nbar protocol activated** command in privileged EXEC mode.

**show ip nbar protocol activated**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.2(4)M | This command was introduced. |

## Usage Guidelines

NBAR must be enabled for debugging.

## Examples

The following is sample output from the **show ip nbar protocol activated** command.

```
Device# show ip nbar protocol activated

Following Protocol are enabled
 Feature:PD
       Hwidb:Ethernet0/0 MI:1 SI:0 FR:0 PVC:0
All iana protocols
```

The table below describes significant fields shown in this output.

***Table 73: show ip nbar protocol activated Field Descriptions***

| Field | Description |
|---|---|
| Hwidb | Displays the configured hardware IDB. |
| MT1 | Displays the configured main interface. |
| SI | Displays the configured sub interface. |
| FR | Displays the configured frame relay. |
| PVC | Displays the configured ATM PVC. |

# show ip nbar protocol-attribute

To display the protocol attributes used by the Network-Based Application Recognition (NBAR), use the **show ip nbar protocol-attribute** command in privileged EXEC mode.

**show ip nbar protocol-attribute** [*protocol-name*]

## Syntax Description

| | |
|---|---|
| *protocol-name* | (Optional) Name of the protocol for which to display the attributes. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.4S | This command was introduced. |

## Usage Guidelines

The **show ip nbar protocol-attribute** command is used to display the attributes of all the protocols. To display the attributes of a specific protocol, specify the protocol name.

## Examples

The following is sample output from the **show ip nbar protocol-attribute** command. The fields in the display are self-explanatory.

```
Router# show ip nbar protocol-attribute ospf
    Protocol Name :  ospf
                 category :  net-admin
             sub-category :  routing-protocol
        application-group :  other
                   tunnel :  tunnel-no
                encrypted :  encrypted-no

Router# show ip nbar protocol-attribute
            Protocol Name :  ftp
                 category :  file-sharing
             sub-category :  client-server
        application-group :  ftp-group
                   tunnel :  tunnel-no
                encrypted :  encrypted-no

            Protocol Name :  http
                 category :  browsing
             sub-category :  other
        application-group :  other
                   tunnel :  tunnel-no
                encrypted :  encrypted-no

            Protocol Name :  egp
                 category :  net-admin
             sub-category :  routing-protocol
        application-group :  other
```

```
           tunnel :  tunnel-no
        encrypted :  encrypted-no

    Protocol Name :  gre
         category :  net-admin
     sub-category :  tunneling-protocols
application-group :  other
           tunnel :  tunnel-yes
        encrypted :  encrypted-no

    Protocol Name :  icmp
         category :  net-admin
     sub-category :  network-management
application-group :  other
           tunnel :  tunnel-no
        encrypted :  encrypted-no

    Protocol Name :  eigrp
         category :  net-admin
     sub-category :  routing-protocol
application-group :  other
           tunnel :  tunnel-no
        encrypted :  encrypted-no
```

## Related Commands

| Command | Description |
|---|---|
| **match protocol attribute application-group** | Configures the match criterion for a class map based on the application group. |
| **match protocol attribute category** | Configures the match criterion for a class map based on the category. |
| **match protocol attribute encrypted** | Configures the match criterion for a class map based on encryption. |
| **match protocol attribute sub-category** | Configures the match criterion for a class map based on the subcategory. |
| **match protocol attribute tunnel** | Configures the match criterion for a class map based on tunneling. |

# show ip nbar protocol-discovery

To display the statistics gathered by the Network-Based Application Recognition (NBAR) Protocol Discovery feature, use the **showipnbarprotocol-discoverycommandinprivilegedEXEC**mode.

**show ip nbar protocol-discovery** [**interface** *type number*] [**stats** {**byte-count**| **bit-rate**| **packet-count**| **max-bit-rate**}] [**protocol** *protocol-name*] [**top-n** *number*]

## Syntax Description

| | |
|---|---|
| **interface** | (Optional) Specifies that Protocol Discovery statistics for the interface are to be displayed. |
| *type* | Type of interface or subinterface whose policy configuration is to be displayed. |
| *number* | Port, connector, VLAN, or interface card number. |
| **stats** | (Optional) Specifies that the byte count, byte rate, or packet count is to be displayed. |
| **byte-count** | (Optional) Specifies that the byte count is to be displayed. |
| **max-bit-rate** | (Optional) Specifies that the maximum bit rate is to be displayed. |
| **packet-coun t** | (Optional) Specifies that the packet count is to be displayed. |
| **protocol** | (Optional) Specifies that statistics for a specific protocol are to be displayed. |
| *protocol-name* | (Optional) User-specified protocol name for which the statistics are to be displayed. |
| **top-n** | (Optional) Specifies that a top-n is to be displayed. A top-n is the number of most active NBAR-supported protocols, where n is the number of protocols to be displayed. For instance, if top-n 3 is entered, the three most active NBAR-supported protocols will be displayed. |
| *number* | (Optional) Specifies the number of most active NBAR-supported protocols to be displayed. |

## Command Default

Statistics for all interfaces on which the NBAR Protocol Discovery feature is enabled are displayed.

**Command Modes**

Privileged EXEC (#)

**Command History**

| Release | Modification |
|---|---|
| 12.0(5)XE2 | This command was introduced. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.1(13)E | This command was implemented on Catalyst 6000 family switches without FlexWAN modules. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(17a)SX1 | This command was integrated into Cisco IOS Release 12.2(17a)SX1. |
| 12.3(7)T | The command output was modified to include Max Bit Rate. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(18)ZYA | This command was integrated into Cisco IOS Release 12.2(18)ZYA. This command was modified to include information about VLANs (as applicable) and to provide support for both Layer 2 and Layer 3 Etherchannels (Catalyst switches only). |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T. |

**Usage Guidelines**

Use the **showipnbarprotocol-discovery**command to display statistics gathered by the NBAR Protocol Discovery feature. This command, by default, displays statistics for all interfaces on which protocol discovery is currently enabled. The default output of this command includes, in the following order, input bit rate (in bits per second), input byte count, input packet count, and protocol name.

Protocol discovery can be used to monitor both input and output traffic and may be applied with or without a service policy enabled. NBAR protocol discovery gathers statistics for packets switched to output interfaces. These statistics are not necessarily for packets that exited the router on the output interfaces, because packets may have been dropped after switching for various reasons, including policing at the output interface, access lists, or queue drops.

**Layer 2/3 Etherchannel Support**

With Cisco IOS Release 12.2(18)ZYA, intended for use on the Cisco 6500 series switch that is equipped with a Supervisor 32/programmable intelligent services accelerator (PISA), the **showipnbarprotocol-discovery** command is supported on both Layer 2 and Layer 3 Etherchannels.

## Examples

The following example displays output from the **showipnbarprotocol-discovery** command for the five most active protocols on an Ethernet interface:

```
Router# show ip nbar protocol-discovery top-n 5

 Ethernet2/0
                          Input                    Output
                          -----                    ------
  Protocol                Packet Count             Packet Count
                          Byte Count               Byte Count
                          30sec Bit Rate (bps)     30sec Bit Rate (bps)
                          30sec Max Bit Rate (bps) 30sec Max Bit Rate (bps)
-------------------------- ------------------------ ------------------------
   rtp                    3272685                  3272685
                                        242050604                242050604

                          768000                   768000
                          2002000                  2002000
   gnutella               513574                   513574
                          118779716                118779716
                          383000                   383000
                          987000                   987000
   ftp                    482183                   482183
                          37606237                 37606237
                          121000                   121000
                          312000                   312000
   http                   144709                   144709
                          32351383                 32351383
                          105000                   105000
                          269000                   269000
   netbios                96606                    96606
                          10627650                 10627650
                          36000                    36000
                          88000                    88000
   unknown                1724428                  1724428
                          534038683                534038683
                          2754000                  2754000
                          4405000                  4405000
   Total                  6298724                  6298724
                          989303872                989303872
                          4213000                  4213000
                          8177000                  8177000
```

The table below describes the significant fields shown in the display.

***Table 74: show ip nbar protocol-discovery Field Descriptions***

| Field | Description |
|---|---|
| Interface | Type and number of an interface. |
| Input | Incoming traffic on an interface. |
| Output | Outgoing traffic on an interface. |
| Protocol | The protocols being used. Unknown is the sum of all the protocols that NBAR could not classify for some reason. |
| Packet Count | Number of packets coming in and going out the interface. |

| Field | Description |
|---|---|
| Byte Count | Number of bytes coming in and going out the interface. |
| 30sec Bit Rate | Average value of the bit rate in bits per second (bps) since protocol discovery was enabled, per protocol, over the last 30 seconds. |
| 30sec Max Bit Rate | Highest value of the bit rate in bits per second (bps) since protocol discovery was enabled, per protocol, over the last 30 seconds. |
| Total | Total input and output traffic. |

## Related Commands

| Command | Description |
|---|---|
| **ip nbar protocol-discovery** | Configures NBAR to discover traffic for all protocols known to NBAR on a particular interface. |

# show ip nbar protocol-id

To display information about Network-Based Application Recognition (NBAR) protocol IDs, use the **showipnbarprotocol-id** command in privileged EXEC mode.

**show ip nbar protocol-id** [ *protocol-name* ]

## Syntax Description

| | |
|---|---|
| *protocol-name* | (Optional) Name of the protocol. |

## Command Default

If the optional argument is not specified, NBAR protocol IDs for all protocols are displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced. |
| 12.2(33)SRE | This command was integrated into Cisco IOS Release 12.2(33)SRE. |
| 15.1(1)S | This command was integrated into Cisco IOS Release 15.1(1)S. |
| Cisco IOS Release XE 3.2S | This command was modified. Support for additional IANA protocols was added. |

## Examples

The following is sample output from the **showipnbarprotocol-id** command:

```
Router# show ip nbar protocol-id
Protocol Name              id            type
-----------------------------------------------
ftp                        2           Standard
http                       3           Standard
egp                        8           L3 IANA
gre                        47          L3 IANA
icmp                       1           L3 IANA
eigrp                      88          L3 IANA
ipinip                     4           L3 IANA
ipsec                      9           Standard
ospf                       89          L3 IANA
bgp                        179         L4 IANA
cuseeme                    12          Standard
dhcp                       13          Standard
finger                     79          L4 IANA
gopher                     70          L4 IANA
secure-http                16          Standard
imap                       17          Standard
secure-imap                18          Standard
irc                        194         L4 IANA
secure-irc                 994         L4 IANA
```

```
kerberos                  21          Standard
l2tp                      1701         L4 IANA
ldap                      389         L4 IANA
secure-ldap               636         L4 IANA
sqlserver                 1433         L4 IANA
netbios                   26          Standard
nfs                       2049         L4 IANA
nntp                      28          Standard
secure-nntp               563         L4 IANA
notes                     1352         L4 IANA
ntp                       123         L4 IANA
pcanywhere                32          Standard
pop3                      110         L4 IANA
secure-pop3               995         L4 IANA
pptp                      1723         L4 IANA
rip                       520         L4 IANA
rsvp                      37          Standard
snmp                      38          Standard
socks                     39          Standard
ssh                       22          L4 IANA
syslog                    41          Standard
telnet                    23          L4 IANA
secure-telnet             992         L4 IANA
secure-ftp                990         L4 IANA
xwindows                  45          Standard
printer                   515         L4 IANA
novadigm                  47          Standard
tftp                      48          Standard
exchange                  49          Standard
vdolive                   50          Standard
sqlnet                    51          Standard
rcmd                      52          Standard
netshow                   53          Standard
sunrpc                    54          Standard
streamwork                55          Standard
citrix                    56          Standard
fasttrack                 57          Standard
gnutella                  58          Standard
kazaa2                    59          Standard
rtsp                      60          Standard
rtp                       61          Standard
mgcp                      62          Standard
skinny                    63          Standard
h323                      64          Standard
sip                       65          Standard
rtcp                      66          Standard
winmx                     68          Standard
bittorrent                69          Standard
directconnect             70          Standard
smtp                      71          Standard
dns                       72          Standard
hl7                       73          Standard
fix                       74          Standard
msn-messenger             75          Standard
dicom                     76          Standard
yahoo-messenger           77          Standard
mapi                      78          Standard
aol-messenger             79          Standard
cifs                      80          Standard
cisco-phone               81          Standard
youtube                   82          Standard
skype                     83          Standard
sap                       84          Standard
blizwow                   85          Standard
whois++                   63          L4 IANA
klogin                    543         L4 IANA
kshell                    544         L4 IANA
ora-srv                   1525         L4 IANA
sqlexec                   9088         L4 IANA
clearcase                 371         L4 IANA
appleqtc                  458         L4 IANA
rcp                       469         L4 IANA
isakmp                    500         L4 IANA
```

```
ibm-db2                  523         L4 IANA
lockd                    4045         L4 IANA
npp                      92          L4 IANA
microsoftds              98          Standard
doom                     666         L4 IANA
vnc                      100         Standard
echo                     7           L4 IANA
systat                   11          L4 IANA
daytime                  13          L4 IANA
chargen                  19          L4 IANA
time                     37          L4 IANA
isi-gl                   55          L4 IANA
rtelnet                  107         L4 IANA
server-ipx               213         L4 IANA
xdmcp                    177         L4 IANA
nicname                  43          L4 IANA
corba-iiop               111         Standard
tacacs                   112         Standard
telepresence-media       113         Standard
telepresence-control     114         Standard
edonkey                  243         Custom
custom-10                244         Custom
custom-09                245         Custom
custom-08                246         Custom
custom-07                247         Custom
custom-06                248         Custom
custom-05                249         Custom
custom-04                250         Custom
custom-03                251         Custom
custom-02                252         Custom
custom-01                253         Custom
mftp                     349         L4 IANA
matip-type-a             350         L4 IANA
matip-type-b             351         L4 IANA
dtag-ste-sb              352         L4 IANA
ndsauth                  353         L4 IANA
datex-asn                355         L4 IANA
cloanto-net-1            356         L4 IANA
bhevent                  357         L4 IANA
shrinkwrap               358         L4 IANA
nsrmp                    359         L4 IANA
scoi2odialog             360         L4 IANA
semantix                 361         L4 IANA
srssend                  362         L4 IANA
rsvp_tunnel              363         L4 IANA
aurora-cmgr              364         L4 IANA
dtk                      365         L4 IANA
odmr                     366         L4 IANA
mortgageware             367         L4 IANA
qbikgdp                  368         L4 IANA
rpc2portmap              369         L4 IANA
codaauth2                370         L4 IANA
ulistproc                372         L4 IANA
legent-1                 373         L4 IANA
legent-2                 374         L4 IANA
hassle                   375         L4 IANA
tnETOS                   377         L4 IANA
is99c                    379         L4 IANA
is99s                    380         L4 IANA
hp-collector             381         L4 IANA
hp-managed-node          382         L4 IANA
hp-alarm-mgr             383         L4 IANA
arns                     384         L4 IANA
ibm-app                  385         L4 IANA
asa                      386         L4 IANA
aurp                     387         L4 IANA
unidata-ldm              388         L4 IANA
fatserv                  347         L4 IANA
uis                      390         L4 IANA
synotics-relay           391         L4 IANA
synotics-broker          392         L4 IANA
meta5                    393         L4 IANA
embl-ndt                 394         L4 IANA
```

```
netware-ip                396         L4 IANA
mptn                      397         L4 IANA
kryptolan                 398         L4 IANA
iso-tsap-c2               399         L4 IANA
ups                       401         L4 IANA
genie                     402         L4 IANA
decap                     403         L4 IANA
nced                      404         L4 IANA
ncld                      405         L4 IANA
imsp                      406         L4 IANA
timbuktu                  407         L4 IANA
prm-sm                    408         L4 IANA
prm-nm                    409         L4 IANA
decladebug                410         L4 IANA
rmt                       411         L4 IANA
synoptics-trap            412         L4 IANA
smsp                      413         L4 IANA
infoseek                  414         L4 IANA
bnet                      415         L4 IANA
onmux                     417         L4 IANA
hyper-g                   418         L4 IANA
ariel1                    419         L4 IANA
ariel2                    421         L4 IANA
ariel3                    422         L4 IANA
opc-job-start             423         L4 IANA
opc-job-track             424         L4 IANA
smartsdp                  426         L4 IANA
svrloc                    427         L4 IANA
ocs_cmu                   428         L4 IANA
ocs_amu                   429         L4 IANA
utmpsd                    430         L4 IANA
utmpcd                    431         L4 IANA
iasd                      432         L4 IANA
nnsp                      433         L4 IANA
mobileip-agent            434         L4 IANA
mobilip-mn                435         L4 IANA
dna-cml                   436         L4 IANA
comscm                    437         L4 IANA
dsfgw                     438         L4 IANA
dasp                      439         L4 IANA
sgcp                      440         L4 IANA
decvms-sysmgt             441         L4 IANA
cvc_hostd                 442         L4 IANA
snpp                      444         L4 IANA
ddm-rdb                   446         L4 IANA
ddm-dfm                   447         L4 IANA
ddm-ssl                   448         L4 IANA
as-servermap              449         L4 IANA
tserver                   450         L4 IANA
sfs-smp-net               451         L4 IANA
sfs-config                452         L4 IANA
creativeserver            453         L4 IANA
contentserver             3365         L4 IANA
creativepartnr            455         L4 IANA
scohelp                   457         L4 IANA
skronk                    460         L4 IANA
datasurfsrv               461         L4 IANA
datasurfsrvsec            462         L4 IANA
alpes                     463         L4 IANA
kpasswd                   464         L4 IANA
digital-vrc               466         L4 IANA
mylex-mapd                467         L4 IANA
photuris                  468         L4 IANA
scx-proxy                 470         L4 IANA
mondex                    471         L4 IANA
ljk-login                 472         L4 IANA
hybrid-pop                473         L4 IANA
tn-tl-fd1                 476         L4 IANA
ss7ns                     477         L4 IANA
spsc                      478         L4 IANA
iafserver                 479         L4 IANA
iafdbase                  480         L4 IANA
bgs-nsi                   482         L4 IANA
```

```
ulpnet                  483         L4 IANA
integra-sme             484         L4 IANA
powerburst              485         L4 IANA
avian                   486         L4 IANA
saft                    487         L4 IANA
gss-http                488         L4 IANA
nest-protocol           489         L4 IANA
micom-pfs               490         L4 IANA
go-login                491         L4 IANA
ticf-1                  492         L4 IANA
ticf-2                  493         L4 IANA
pov-ray                 494         L4 IANA
intecourier             495         L4 IANA
pim-rp-disc             496         L4 IANA
dantz                   497         L4 IANA
siam                    498         L4 IANA
iso-ill                 499         L4 IANA
stmf                    501         L4 IANA
asa-appl-proto          502         L4 IANA
intrinsa                503         L4 IANA
mailbox-lm              505         L4 IANA
ohimsrv                 506         L4 IANA
crs                     507         L4 IANA
xvttp                   508         L4 IANA
snare                   509         L4 IANA
fcp                     510         L4 IANA
passgo                  511         L4 IANA
exec                    512         L4 IANA
shell                   430         Standard
videotex                516         L4 IANA
talk                    517         L4 IANA
ntalk                   518         L4 IANA
utime                   519         L4 IANA
ripng                   521         L4 IANA
ulp                     522         L4 IANA
pdap                    344         L4 IANA
ncp                     524         L4 IANA
timed                   525         L4 IANA
tempo                   526         L4 IANA
stx                     527         L4 IANA
custix                  528         L4 IANA
irc-serv                529         L4 IANA
courier                 530         L4 IANA
conference              531         L4 IANA
netnews                 532         L4 IANA
netwall                 533         L4 IANA
iiop                    535         L4 IANA
opalis-rdv              536         L4 IANA
nmsp                    537         L4 IANA
gdomap                  538         L4 IANA
apertus-ldp             539         L4 IANA
uucp                    540         L4 IANA
uucp-rlogin             541         L4 IANA
commerce                542         L4 IANA
appleqtcsrvr            545         L4 IANA
dhcpv6-client           546         L4 IANA
dhcpv6-server           547         L4 IANA
idfp                    549         L4 IANA
new-rwho                550         L4 IANA
cybercash               551         L4 IANA
pirp                    553         L4 IANA
remotefs                556         L4 IANA
openvms-sysipc          557         L4 IANA
sdnskmp                 558         L4 IANA
teedtap                 559         L4 IANA
rmonitor                560         L4 IANA
monitor                 561         L4 IANA
chshell                 562         L4 IANA
9pfs                    564         L4 IANA
whoami                  565         L4 IANA
streettalk              566         L4 IANA
banyan-rpc              567         L4 IANA
ms-shuttle              568         L4 IANA
```

```
ms-rome                  569         L4 IANA
meter                    570         L4 IANA
sonar                    572         L4 IANA
banyan-vip               573         L4 IANA
ftp-agent                574         L4 IANA
vemmi                    575         L4 IANA
ipcd                     576         L4 IANA
vnas                     577         L4 IANA
ipdd                     578         L4 IANA
decbsrv                  579         L4 IANA
sntp-heartbeat           580         L4 IANA
bdp                      581         L4 IANA
scc-security             582         L4 IANA
philips-vc               583         L4 IANA
keyserver                584         L4 IANA
password-chg             586         L4 IANA
submission               587         L4 IANA
tns-cml                  590         L4 IANA
http-alt                 8008         L4 IANA
eudora-set               592         L4 IANA
http-rpc-epmap           593         L4 IANA
tpip                     594         L4 IANA
cab-protocol             595         L4 IANA
smsd                     596         L4 IANA
ptcnameservice           597         L4 IANA
sco-websrvrmg3           598         L4 IANA
acp                      599         L4 IANA
ipcserver                600         L4 IANA
urm                      606         L4 IANA
nqs                      607         L4 IANA
sift-uft                 608         L4 IANA
npmp-trap                609         L4 IANA
npmp-local               610         L4 IANA
npmp-gui                 611         L4 IANA
hmmp-ind                 612         L4 IANA
hmmp-op                  613         L4 IANA
sshell                   614         L4 IANA
sco-inetmgr              615         L4 IANA
sco-sysmgr               616         L4 IANA
sco-dtmgr                617         L4 IANA
dei-icda                 618         L4 IANA
sco-websrvrmgr           620         L4 IANA
escp-ip                  621         L4 IANA
collaborator             622         L4 IANA
cryptoadmin              624         L4 IANA
dec_dlm                  625         L4 IANA
passgo-tivoli            627         L4 IANA
qmqp                     628         L4 IANA
3com-amp3                629         L4 IANA
rda                      630         L4 IANA
ipp                      631         L4 IANA
bmpp                     632         L4 IANA
servstat                 633         L4 IANA
ginad                    634         L4 IANA
rlzdbase                 635         L4 IANA
lanserver                637         L4 IANA
mcns-sec                 638         L4 IANA
msdp                     639         L4 IANA
entrust-sps              640         L4 IANA
repcmd                   641         L4 IANA
esro-emsdp               642         L4 IANA
sanity                   643         L4 IANA
dwr                      644         L4 IANA
ldp                      646         L4 IANA
dhcp-failover            647         L4 IANA
rrp                      648         L4 IANA
aminet                   2639         L4 IANA
obex                     650         L4 IANA
ieee-mms                 651         L4 IANA
hello-port               652         L4 IANA
repscmd                  653         L4 IANA
aodv                     654         L4 IANA
tinc                     655         L4 IANA
```

```
spmp                    656         L4 IANA
rmc                     657         L4 IANA
tenfold                 658         L4 IANA
mac-srvr-admin          660         L4 IANA
hap                     661         L4 IANA
pftp                    662         L4 IANA
purenoise               663         L4 IANA
sun-dr                  665         L4 IANA
disclose                667         L4 IANA
mecomm                  668         L4 IANA
meregister              669         L4 IANA
vacdsm-sws              670         L4 IANA
vacdsm-app              671         L4 IANA
vpps-qua                672         L4 IANA
cimplex                 673         L4 IANA
acap                    674         L4 IANA
dctp                    675         L4 IANA
vpps-via                676         L4 IANA
vpp                     677         L4 IANA
ggf-ncp                 678         L4 IANA
mrm                     679         L4 IANA
entrust-aaas            680         L4 IANA
entrust-aams            681         L4 IANA
mdc-portmapper          685         L4 IANA
hcp-wismar              686         L4 IANA
asipregistry            687         L4 IANA
realm-rusd              688         L4 IANA
nmap                    689         L4 IANA
vatp                    690         L4 IANA
msexch-routing          691         L4 IANA
hyperwave-isp           692         L4 IANA
connendp                693         L4 IANA
ha-cluster              694         L4 IANA
ieee-mms-ssl            695         L4 IANA
rushd                   696         L4 IANA
uuidgen                 697         L4 IANA
olsr                    698         L4 IANA
accessnetwork           699         L4 IANA
elcsd                   704         L4 IANA
agentx                  705         L4 IANA
silc                    706         L4 IANA
borland-dsj             707         L4 IANA
entrust-kmsh            709         L4 IANA
entrust-ash             710         L4 IANA
cisco-tdp               711         L4 IANA
netviewdm1              729         L4 IANA
netviewdm2              730         L4 IANA
netviewdm3              731         L4 IANA
netgw                   741         L4 IANA
netrcs                  742         L4 IANA
flexlm                  744         L4 IANA
fujitsu-dev             747         L4 IANA
ris-cm                  748         L4 IANA
pump                    751         L4 IANA
qrh                     752         L4 IANA
rrh                     753         L4 IANA
tell                    754         L4 IANA
nlogin                  758         L4 IANA
con                     759         L4 IANA
ns                      760         L4 IANA
rxe                     761         L4 IANA
quotad                  762         L4 IANA
cycleserv               763         L4 IANA
omserv                  764         L4 IANA
webster                 765         L4 IANA
phonebook               767         L4 IANA
vid                     769         L4 IANA
cadlock                 770         L4 IANA
rtip                    771         L4 IANA
cycleserv2              772         L4 IANA
submit                  643         Standard
entomb                  775         L4 IANA
multiling-http          777         L4 IANA
```

```
wpgs                    780          L4 IANA
device                  801          L4 IANA
itm-mcell-s             828          L4 IANA
pkix-3-ca-ra            829          L4 IANA
dhcp-failover2          847          L4 IANA
rsync                   873          L4 IANA
iclcnet-locate          886          L4 IANA
iclcnet_svinfo          887          L4 IANA
accessbuilder           888          L4 IANA
omginitialrefs          900          L4 IANA
smpnameres              901          L4 IANA
xact-backup             911          L4 IANA
ftps-data               989          L4 IANA
nas                     991          L4 IANA
vsinet                  996          L4 IANA
maitrd                  997          L4 IANA
applix                  999          L4 IANA
surf                    1010          L4 IANA
rmiactivation           1098          L4 IANA
rmiregistry             1099          L4 IANA
ms-sql-m                1434          L4 IANA
ms-olap                 2393          L4 IANA
msft-gc                 3268          L4 IANA
msft-gc-ssl             3269          L4 IANA
tlisrv                  1527          L4 IANA
coauthor                1529          L4 IANA
rdb-dbs-disp            1571          L4 IANA
oraclenames             1575          L4 IANA
oraclenet8cman          1630          L4 IANA
net8-cman               1830          L4 IANA
micromuse-lm            1534          L4 IANA
orbix-locator           3075          L4 IANA
orbix-config            3076          L4 IANA
orbix-loc-ssl           3077          L4 IANA
shockwave               1626          L4 IANA
sitaraserver            2629          L4 IANA
sitaramgmt              2630          L4 IANA
sitaradir               2631          L4 IANA
mysql                   3306          L4 IANA
net-assistant           3283          L4 IANA
msnp                    1863          L4 IANA
groove                  2492          L4 IANA
directplay              2234          L4 IANA
directplay8             6073          L4 IANA
kali                    2213          L4 IANA
worldfusion             2595          L4 IANA
directv-web             3334          L4 IANA
directv-soft            3335          L4 IANA
directv-tick            3336          L4 IANA
directv-catlg           3337          L4 IANA
wap-push                2948          L4 IANA
wap-pushsecure          2949          L4 IANA
wap-push-http           4035          L4 IANA
wap-push-https          4036          L4 IANA
wap-wsp                 9200          L4 IANA
wap-wsp-wtp             9201          L4 IANA
wap-wsp-s               9202          L4 IANA
wap-wsp-wtp-s           9203          L4 IANA
wap-vcard               9204          L4 IANA
wap-vcal                9205          L4 IANA
wap-vcard-s             9206          L4 IANA
wap-vcal-s              9207          L4 IANA
ibprotocol              6714          L4 IANA
gtp-user                2152          L4 IANA
xdtp                    3088          L4 IANA
parsec-game             6582          L4 IANA
hopopt                  0            L3 IANA
ggp                     3            L3 IANA
st                      5            L3 IANA
cbt                     7            L3 IANA
zserv                   346          L4 IANA
igrp                    9            L3 IANA
bbnrccmon               10           L3 IANA
```

```
pawserv                  345         L4 IANA
texar                    333         L4 IANA
rtsps                    322         L4 IANA
pip                      1321         L4 IANA
ptp-general              320         L4 IANA
nat-stun                 3478         L4 IANA
compressnet              2           L4 IANA
rje                      5           L4 IANA
discard                  9           L4 IANA
qotd                     17          L4 IANA
msp                      18          L4 IANA
ftp-data                 20          L4 IANA
nsw-fe                   27          L4 IANA
msg-icp                  29          L4 IANA
csi-sgwp                 348         L4 IANA
msg-auth                 31          L4 IANA
dsp                      33          L4 IANA
rap                      38          L4 IANA
rlp                      39          L4 IANA
graphics                 41          L4 IANA
name                     42          L4 IANA
profile                  136         L4 IANA
mpm-flags                44          L4 IANA
mpm                      45          L4 IANA
mpm-snd                  46          L4 IANA
ni-ftp                   47          L4 IANA
auditd                   48          L4 IANA
emfis-data               140         L4 IANA
re-mail-ck               50          L4 IANA
la-maint                 51          L4 IANA
xns-time                 52          L4 IANA
emfis-cntl               141         L4 IANA
xns-ch                   54          L4 IANA
bl-idm                   142         L4 IANA
xns-auth                 56          L4 IANA
xns-mail                 58          L4 IANA
ni-mail                  61          L4 IANA
acas                     62          L4 IANA
covia                    64          L4 IANA
sql*net                  66          L4 IANA
bootps                   67          L4 IANA
bootpc                   68          L4 IANA
uaac                     145         L4 IANA
iso-tp0                  146         L4 IANA
netrjs-1                 71          L4 IANA
netrjs-2                 72          L4 IANA
netrjs-3                 73          L4 IANA
netrjs-4                 74          L4 IANA
deos                     76          L4 IANA
iso-ip                   147         L4 IANA
xfer                     82          L4 IANA
mit-ml-dev               83          L4 IANA
ctf                      84          L4 IANA
mfcobol                  86          L4 IANA
jargon                   148         L4 IANA
su-mit-tg                89          L4 IANA
dnsix                    90          L4 IANA
mit-dov                  91          L4 IANA
aed-512                  149         L4 IANA
dcp                      93          L4 IANA
objcall                  94          L4 IANA
supdup                   95          L4 IANA
dixie                    96          L4 IANA
swift-rvf                97          L4 IANA
tacnews                  98          L4 IANA
metagram                 99          L4 IANA
hostname                 101         L4 IANA
iso-tsap                 102         L4 IANA
acr-nema                 104         L4 IANA
csnet-ns                 105         L4 IANA
3com-tsmux               106         L4 IANA
sql-net                  150         L4 IANA
snagas                   108         L4 IANA
```

```
pop2                    109         L4 IANA
hems                    151         L4 IANA
mcidas                  112         L4 IANA
auth                    113         L4 IANA
sftp                    115         L4 IANA
ansanotify              116         L4 IANA
uucp-path               117         L4 IANA
sqlserv                 118         L4 IANA
cfdptkt                 120         L4 IANA
erpc                    121         L4 IANA
smakynet                122         L4 IANA
bftp                    152         L4 IANA
ansatrader              124         L4 IANA
locus-map               125         L4 IANA
nxedit                  126         L4 IANA
locus-con               127         L4 IANA
gss-xlicen              128         L4 IANA
pwdgen                  129         L4 IANA
cisco-fna               130         L4 IANA
sgmp                    153         L4 IANA
netsc-prod              154         L4 IANA
netsc-dev               155         L4 IANA
knet-cmp                157         L4 IANA
pcmail-srv              158         L4 IANA
nss-routing             159         L4 IANA
sgmp-traps              160         L4 IANA
cmip-man                163         L4 IANA
cmip-agent              164         L4 IANA
xns-courier             165         L4 IANA
s-net                   166         L4 IANA
namp                    167         L4 IANA
rsvd                    168         L4 IANA
send                    169         L4 IANA
print-srv               170         L4 IANA
multiplex               171         L4 IANA
xyplex-mux              173         L4 IANA
mailq                   174         L4 IANA
vmnet                   175         L4 IANA
genrad-mux              176         L4 IANA
nextstep                178         L4 IANA
ris                     180         L4 IANA
unify                   181         L4 IANA
audit                   182         L4 IANA
ocbinder                183         L4 IANA
ocserver                184         L4 IANA
remote-kis              185         L4 IANA
kis                     186         L4 IANA
mumps                   188         L4 IANA
qft                     189         L4 IANA
gacp                    190         L4 IANA
prospero                191         L4 IANA
osu-nms                 192         L4 IANA
srmp                    193         L4 IANA
dn6-nlm-aud             195         L4 IANA
dls                     197         L4 IANA
dls-mon                 198         L4 IANA
smux                    199         L4 IANA
src                     200         L4 IANA
at-rtmp                 201         L4 IANA
at-nbp                  202         L4 IANA
at-3                    203         L4 IANA
at-echo                 204         L4 IANA
at-5                    205         L4 IANA
at-zis                  206         L4 IANA
at-7                    207         L4 IANA
at-8                    208         L4 IANA
qmtp                    209         L4 IANA
z39.50                  210         L4 IANA
914c/g                  211         L4 IANA
anet                    212         L4 IANA
vmpwscs                 214         L4 IANA
softpc                  215         L4 IANA
CAIlic                  216         L4 IANA
```

```
dbase                     217         L4 IANA
mpp                       218         L4 IANA
uarps                     219         L4 IANA
fln-spx                   221         L4 IANA
rsh-spx                   222         L4 IANA
cdc                       223         L4 IANA
masqdialer                224         L4 IANA
sur-meas                  243         L4 IANA
inbusiness                244         L4 IANA
dsp3270                   246         L4 IANA
subntbcst_tftp            247         L4 IANA
bhfhs                     248         L4 IANA
set                       257         L4 IANA
esro-gen                  259         L4 IANA
openport                  260         L4 IANA
nsiiops                   261         L4 IANA
arcisdms                  262         L4 IANA
hdap                      263         L4 IANA
bgmp                      264         L4 IANA
x-bone-ctl                265         L4 IANA
sst                       266         L4 IANA
td-service                267         L4 IANA
td-replica                268         L4 IANA
http-mgmt                 280         L4 IANA
personal-link             281         L4 IANA
cableport-ax              282         L4 IANA
rescap                    283         L4 IANA
corerjd                   284         L4 IANA
k-block                   287         L4 IANA
novastorbakcup            308         L4 IANA
bhmds                     310         L4 IANA
asip-webadmin             311         L4 IANA
vslmp                     312         L4 IANA
magenta-logic             313         L4 IANA
opalis-robot              314         L4 IANA
dpsi                      315         L4 IANA
decauth                   316         L4 IANA
zannet                    317         L4 IANA
pkix-timestamp            318         L4 IANA
ptp-event                 319         L4 IANA
cisco-tna                 131         L4 IANA
cisco-sys                 132         L4 IANA
statsrv                   133         L4 IANA
ingres-net                134         L4 IANA
Konspire2b                6085         L4 IANA
Total protocols:          721
```

The table below describes the significant fields shown in the display.

***Table 75: show ip nbar protocol-id Field Descriptions***

| Field | Description |
|---|---|
| Protocol Name | Name of the NBAR protocol. |
| id | Unique identifier assigned to the NBAR protocol. |
| type | Indicates whether the protocol is standard or customized. |

## Related Commands

| Command | Description |
|---|---|
| **ip nbar custom** | Extends the capability of NBAR Protocol Discovery to classify and monitor additional static port applications or allows NBAR to classify nonsupported static port traffic. |

# show ip nbar protocol-pack

To display protocol pack information, use the **show ip nbar protocol-pack** command in user EXEC or privileged EXEC mode.

**show ip nbar protocol-pack** {*protocol-pack*| **active**} **[detail]**

## Syntax Description

| | |
|---|---|
| *protocol-pack* | Protocol pack file path and name. |
| **active** | Displays active protocol pack information. |
| **detail** | (Optional) Displays detailed protocol pack information. |

## Command Modes

User EXEC (>)

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.3S | This command was introduced. |
| 15.2(2)T | This command was integrated into Cisco IOS Release 15.2(2)T. |

## Usage Guidelines

The protocol pack is a single compressed file that contains multiple Protocol Description Language (PDL) files and a manifest file. Before the protocol pack was introduced, PDLs had to be loaded separately. With network-based application recognition (NBAR) protocol pack, a set of required protocols can be loaded, which helps NBAR to recognize additional protocols for classification on your network.

## Examples

The following sample output from the **show ip nbar protocol-pack** command shows information about the active protocol pack:

```
Router# show ip nbar protocol-pack active
ACTIVE protocol pack:
Name:                            Default Protocol Pack
Version:                         1.0
Publisher:                       Cisco Systems Inc.
```

The following sample output from the **show ip nbar protocol-pack** command shows detailed information about the active protocol pack:

```
Router# show ip nbar protocol-pack active detail
ACTIVE protocol pack:
Name:                            Default Protocol Pack
Version:                         1.0
```

```
Publisher:                      Cisco Systems Inc.
Protocols:
base                            Mv: 4
ftp                             Mv: 5
http                            Mv: 18
static                          Mv: 6
socks                           Mv: 2
nntp                            Mv: 2
tftp                            Mv: 2
exchange                        Mv: 3
vdolive                         Mv: 1
sqlnet                          Mv: 2
netshow                         Mv: 3
sunrpc                          Mv: 3
streamwork                      Mv: 2
citrix                          Mv: 11
fasttrack                       Mv: 3
gnutella                        Mv: 7
kazaa2                          Mv: 11
```

The table below describes the significant fields shown in the display.

***Table 76: show ip nbar protocol-pack Field Descriptions***

| Field | Description |
|---|---|
| Name | Name of the protocol pack. |
| Version | Protocol pack version. |
| Publisher | Name of the publisher of the protocol pack. |
| Protocols | List of protocols present in the protocol pack. |

## Related Commands

| Command | Description |
|---|---|
| **default ip nbar protocol-pack** | Loads the base version of the protocol pack and removes all other loaded protocol packs. |
| **ip nbar protocol-pack** | Loads a protocol pack. |

# show ip nbar resources flow

To display the current configuration and the utilization of resources in the Network-Based Application Recognition (NBAR), use the **show ip nbar resources flow** command in privileged EXEC mode.

**show ip nbar resources flow**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.4S | This command was introduced. |

## Examples

The following is the sample output from the **show ip nbar resources flow** command. The fields in the display are self-explanatory.

```
Router# show ip nbar resources flow

NBAR flow statistics
        Maximum no of sessions allowed : 3500000
        Maximum memory usage allowed   : 734003 KBytes
        Active sessions                : 3499950
        Active memory usage            : 665364 KBytes
        Peak session                   : 3499950
        Peak memory usage              : 672396 KBytes
```

## Related Commands

| Command | Description |
|---|---|
| **ip nbar resources flow max-session** | Configures the maximum flow sessions to be allowed in a flow table. |

# show ip nbar statistics

To display failure statistics, the number of packets per flow, and different types of classifications on a device that runs Network-Based Application Recognition (NBAR), use the **show ip nbar statistics** command in privileged EXEC mode.

**show ip nbar statistics**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.2(4)M | This command was introduced. |

## Examples

The following is sample output from the **show ip nbar statistics** command. The fields in the output are self-explanatory.

```
Device# show ip nbar statistics

Compiler statistics
Malloc failure = 0
Control-plane statistics
Malloc failure = 0
Invalid iterators = 0
Data-plane statistics
Malloc failure = 0
FO create failure = 0
CFT Age set failure = 0
```

# show ip nbar trace

To display the path traversed by a packet on a data plane, use the **show ip nbar trace** command in privileged EXEC mode.

**show ip nbar trace**{**detail**| **summary**}[**config**]

## Syntax Description

| | |
|---|---|
| **detail** | Displays the classification trace in detail. |
| **summary** | Displays the classification trace summary. |
| **config** | (Optional) Displays the configuration information for state-graph tracing. |

## Command Default

Information about all paths traversed by a packet is displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.2(4)M | This command was introduced. |

## Usage Guidelines

Trace and summary debugging must be enabled.

## Examples

The following is sample output from the **show ip nbar trace summary** command. The fields in the output are self-explanatory.

```
Device# show ip nbar trace summary

Classification: 76, flag: 163
Searched Source WKP
Searched Dest WKP
Classifying using Heuristic regexp
Classifying using Heuristic General
Classifying using MPE

Classification: 1, flag: 160
Searched Source WKP
Searched Dest WKP
Classifying using Heuristic regexp
Classifying using Heuristic General
Classifying using MPE
```

The following is sample output from the **show ip nbar trace detail** command. The fields in the output are self-explanatory.

```
Device# show ip nbar trace detail

Graph Id 1
Classification: 82, flag: 163
Packet No: 1
String: Searching Source V4 WKP
String: Searching Destination V4 WKP
String: Entering loop core from Heuristic Regex
State Node:http-verify-heuristic-entry-point-get
State Node:http-verify-heuristic-entry-point-get
State Node:HTTP-url-get-check
State Node:HTTP-url-get-check
State Node:HTTP-url-get-check
State Node:HTTP-url-get-check
State Node:youtube-found-url
State Node:http-check-url-fe
State Node:HTTP-request-advance-packet-pointer-to-next-http-header
State Node:HTTP-request-advance-packet-pointer-to-next-http-header
State Node:HTTP-request-advance-packet-pointer-to-next-http-header
State Node:HTTP-request-end-of-request-check
State Node:HTTP-request-check-end-of-packet
State Node:HTTP-request-check-end-of-packet
State Node:HTTP-request-headers-parser
State Node:HTTP-request-headers-parser
Graph Id 1
```

## Related Commands

| Command | Description |
|---|---|
| **clear ip nbar trace summary** | Clears classification modules. |
| **debug ip nbar config** | Enables debugging of all commands configured for activation and deactivation of the NBAR. |

# show ip nbar unclassified-port-stats

To display the network-based application recognition (NBAR) port statistics for unclassified packets, use the **showipnbarunclassified-port-stats**command in privileged EXEC mode.

**show ip nbar unclassified-port-stats** [*top-talkers*| **ip** [*protocol-number* [ *number-protocols* ]| **top** *top-talkers*]| [**tcp**| **udp**] [*port-number* [ *number-ports* ]| **top** *top-talkers*| **bottom** *bottom-talkers*]]

## Syntax Description

| | |
|---|---|
| *top-talkers* | (Optional) Number of top talkers to show. |
| ip | (Optional) Displays port statistics for unclassified non-TCP/non-UDP packets. |
| *protocol-number* | (Optional) Starting IP protocol number. |
| *number-protocols* | (Optional) Number of protocols to show. |
| top | (Optional) Specifies that a top-n is to be displayed. A top-n is the number of most active NBAR-supported protocols, where n is the number of protocols to be displayed. For instance, if top-n 3 is entered, the three most active NBAR-supported protocols are displayed. |
| tcp | (Optional) Displays port statistics for unclassified TCP packets. |
| udp | (Optional) Displays port statistics for unclassified UDP packets. |
| *port-number* | (Optional) Starting TCP or UDP port number. |
| *number-ports* | (Optional) Number of ports to show. |
| bottom | (Optional) Specifies that a bottom-n is to be displayed. A bottom-n is the number of least active NBAR-supported protocols, where n is the number of protocols to be displayed. For instance, if bottom-n 3 is entered, the three least active NBAR-supported protocols are displayed. |
| *bottom-talkers* | (Optional) Number of bottom talkers to show. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)XE2 | This command was introduced. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.1(13)E | This command was implemented on Cisco Catalyst 6000 family switches without FlexWAN modules. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(17a)SX1 | This command was integrated into Cisco IOS Release 12.2(17a)SX1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(18)ZYA | This command was integrated into Cisco IOS Release 12.2(18)ZYA. This command was modified to include information about VLANs (as applicable) and to provide support for both Layer 2 and Layer 3 Etherchannels (Cisco Catalyst switches only). |

## Usage Guidelines

By default, NBAR unclassified mechanisms are not enabled. Use the **debugipnbarunclassified-port-stats** command to configure the router to begin tracking the ports on which packets arrive. Then use the **showipnbarunclassified-port-stats** command to verify the collected information.

## Examples

The following is sample output from **showipnbarunclassified-port-stats** command:

```
Router# show ip nbar unclassified-port-stats

-tcp-
      80/tcp:48
    1443/tcp:3
    1423/tcp:2
    1424/tcp:2
    1425/tcp:2
-udp-
    1985/udp:158
    1029/udp:13
     496/udp:4
    1445/udp:3
    1449/udp:2
```

The table below describes the significant fields shown in the display.

***Table 77: show ip nbar unclassified-port-stats Field Descriptions***

| Field | Description |
|---|---|
| -tcp- | TCP Protocol. |

| Field | Description |
|---|---|
| 80/tcp:48 | 80 represents the port number, tcp the protocol and 48 the number of packets. |
| -udp- | UDP protocol. |
| 1985/udp:158 | 1855 represents the port number, udp the protocol and 158 the number of packets. |

The output displays the port number, the protocol and the number of packets. For example, in 80/tcp:48, 80 represents the port number, tcp the protocol and 48 the number of packets.

## Related Commands

| Command | Description |
|---|---|
| **ip nbar custom** | Extends the capability of NBAR Protocol Discovery to classify and monitor additional static port applications or to allow NBAR to classify nonsupported static port traffic. |
| **ip nbar pdlm** | Extends or enhances the list of protocols recognized by NBAR through a Cisco-provided PDLM. |
| **ip nbar port-map** | Configures NBAR to search for a protocol or protocol name using a port number other than the well-known port number. |
| **ip nbar protocol-discovery** | Configures NBAR to discover traffic for all protocols that are known to NBAR on a particular interface. |
| **ip nbar resources protocol** | Sets the expiration time for NBAR flow-link tables on a protocol basis. |
| **ip nbar resources system** | Sets the expiration time and memory requirements for NBAR flow-link tables on a systemwide basis. |
| **show ip nbar pdlm** | Displays the PDLM in use by NBAR. |
| **show ip nbar port-map** | Displays the current protocol-to-port mappings in use by NBAR. |
| **show ip nbar protocol-discovery** | Displays the statistics gathered by the NBAR Protocol Discovery feature. |
| **show ip nbar version** | Displays information about the version of the NBAR software in your Cisco IOS release or the version of an NBAR PDLM on your Cisco IOS router. |

# show ip nbar version

To display information about the version of the network-based application recognition (NBAR) software in your Cisco IOS release or the version of an NBAR Packet Description Language Module (PDLM) on your Cisco IOS router, use the **showipnbarversion**command in p**rivilegedEXEC**mode.

**show ip nbar version** [ *PDLM-name* ]

## Syntax Description

| | |
|---|---|
| *PDLM-name* | (Optional) Specifies the name of a specific PDLM whose information will be displayed. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.3(4)T | This command was introduced. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(17a)SX1 | This command was integrated into Cisco IOS Release 12.2(17a)SX1. |
| 15.1(3)T | This command was integrated into Cisco IOS Release 15.1(3)T. |

## Usage Guidelines

The **showipnbarversion** command treats all protocols that were added to NBAR after the initial NBAR release as PDLMs, including protocols that were added into the Cisco IOS software without a user having to download a PDLM from Cisco.com. PDLMs downloaded from Cisco.com and incorporated into NBAR by the user also appear when the**showipnbarversion** command is entered.

When using NBAR, various elements within NBAR are assigned versioning numbers. These versioning numbers become significant when you want to download a PDLM. PDLMs, which are also versioned, can be downloaded only to NBAR on a particular Cisco IOS release if the PDLM versioning numbers are compatible with the NBAR version numbers in the Cisco IOS software.

The following NBAR-related version information is available:

- NBAR Software Version--Version of NBAR software running on the current version of Cisco IOS software.
- Resident Module Version--Version of the NBAR-supported PDLM protocol.

The following version number is kept by the PDLM:

- NBAR Software Version--Minimum version of the NBAR software that is required to load this PDLM.

The **showipnbarversion** command provides version information for PDLMs already loaded onto the Cisco IOS software.

## Examples

The following is sample output from the show ip nbar version command:

```
Router# show ip nbar version
NBAR software version:  3
1   base                 Mv: 2
2   ftp                  Mv: 2
3   http                 Mv: 7, Nv: 3; slot1:http_vers.pdlm
4   static-port          Mv: 6
5   tftp                 Mv: 1
6   exchange             Mv: 1
7   vdolive              Mv: 1
8   sqlnet               Mv: 1
9   rcmd                 Mv: 1
10  netshow              Mv: 1
11  sunrpc               Mv: 2
12  streamwork           Mv: 1
13  citrix               Mv: 5
14  fasttrack            Mv: 2
15  gnutella             Mv: 1
16 kazaa                Mv: 6, Nv: 3; slot1:kazaa2_vers.pdlm
17 custom-protocols     Mv: 1
18 rtsp                 Mv: 1
19  rtp                  Mv: 2
20  mgcp                 Mv: 1
21  skinny               Mv: 1
22 h323                 Mv: 1
23 sip                  Mv: 1
24 rtcp                 Mv: 1
```

The table below describes the significant fields shown in the display.

***Table 78: show ip nbar version Command Field Descriptions***

| Field | Description |
|---|---|
| NBAR Software Version | NBAR software version running in the current Cisco IOS software. In this particular example, version 3 is the NBAR software running on the current version of the Cisco IOS software. |
| Mv | Resident Module Version. The Resident Module Version is the version of the NBAR-supported PDLM protocol and, therefore, varies by protocol. The Resident Module Version of TFTP, for example, is 1. |
| Nv | Minimum version of the NBAR software that is required to load a nonnative PDLM. This number is available only for nonnative PDLMs that were loaded onto the router such as the Kazaa PDLM (protocol 17); in that case, the Nv version is 3. |

For the same network setup, the following example shows the output if a specific protocol with a PDLM is specified in the**showipnbarversion** CLI:

```
Router# show ip nbar version http
http                 Mv: 7, Nv: 3; slot1:http_vers.pdlm
```

## Related Commands

| Command | Description |
|---|---|
| **ip nbar pdlm** | Downloads a PDLM onto a router to add support for additional protocols in NBAR. |

# show ip rsvp

To display information about the Resource Reservation Protocol (RSVP), use the **showiprsvp**command in user EXEC or privileged EXEC mode.

**show ip rsvp**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.2(13)T | This command was modified. The **listeners** and **policy**keywords were added, and this command was modified to display RSVP global settings when no keywords or arguments are entered. |
| 12.2(33)SRB | This command was modified. The command output was modified to display fast local repair (FLR) information. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SRC | This command was modified. The command output was modified to display the following:<br>• RSVP quality of service (QoS) and Multiprotocol Label Switching (MPLS) traffic engineering (TE) information.<br>• RSVP aggregation information. |
| 15.0(1)M | This command was modified.<br>The [**atm-peak-rate-limit** \| **counters** \| **host** \| **installed** \| **interface** \| **listeners** \| **neighbor** \| **policy** \| **precedence** \| **request** \| **reservation** \| **sbm** \| **sender** \| **signalling** \| **tos**] syntax was removed from the command. The keyword options are represented in the following individual command files: show ip rsvp **atm-peak-rate-limit,**show ip rsvp **counters,**show ip rsvp **host,**show ip rsvp installed, show ip rsvp interface, show ip rsvp listeners, show ip rsvp neighbor, show ip rsvp policy, show ip rsvp precedence, show ip rsvp request, show ip rsvp reservation, show ip rsvp sbm, show ip rsvp sender, show ip rsvp signalling, and show ip rsvp tos commands. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Examples

The following is sample output from the **showiprsvp** command:

```
Router# show ip rsvp
RSVP: enabled (on 1 interface(s))
   RSVP QoS signalling enabled
   MPLS/TE signalling enabled
Signalling:
   Refresh interval (msec): 30000
   Refresh misses: 4
Rate Limiting: enabled
   Burst: 8
   Limit: 37
   Maxsize: 2000
   Period (msec): 20
   Max rate (msgs/sec): 400
Refresh Reduction: disabled
   ACK delay (msec): 250
   Initial retransmit delay (msec): 1000
   Local epoch: 0xCE969B
   Message IDs: in use 0, total allocated 0, total freed 0
Neighbors: 0
   Raw IP encap: 0  UDP encap: 0  Raw IP, UDP encap: 0
RFC 3175 Aggregation: Enabled
   Level: 1
   Default QoS service: Controlled-Load
   Router ID: 10.22.22.22
   Number of signaled aggregate reservations:     0
   Number of signaled E2E reservation:            0
   Number of configured map commands:             0
   Number of configured reservation commands:     0
Hello:
   RSVP Hello for Fast-Reroute/Reroute: Disabled
     Statistics: Disabled
   BFD for Fast-Reroute/Reroute: Disabled
   RSVP Hello for Graceful Restart: Disabled
Graceful Restart: Disabled
   Refresh interval: 10000 msecs
   Refresh misses: 4
   DSCP: 0x30
   Advertised restart time: 5 msecs
   Advertised recovery time: 0 msecs
   Maximum wait for recovery: 3600000 msecs
Fast-Reroute:
   PSBs w/ Local protection desired
     Yes: 0
     No:  0
Fast Local Repair: enabled
   Max repair rate (paths/sec): 400
   Max processed   (paths/run): 1000
Local policy:
COPS:
Generic policy settings:
     Default policy: Accept all
     Preemption:     Disabled
```

The table below describes the significant fields shown in the display.

*Table 79: show ip rsvp Field Descriptions*

| Field | Description |
|---|---|
| RSVP | The state of RSVP, QoS, and MPLS TE signaling; values are enabled (activated) or disabled (deactivated).<br>**Note** This field is disabled only if an internal error occurred when registering with RIB. |
| Signalling | The RSVP signaling parameters in effect are as follows:<br>• Refresh interval--Time, in milliseconds (ms), between sending refreshes for each RSVP state.<br>• Refresh misses--Number of successive refresh messages that can be missed before RSVP considers the state expired and tears it down. |
| Rate Limiting: enabled or disabled | The RSVP rate-limiting parameters in effect are as follows:<br>• Burst--Maximum number of RSVP messages allowed to be sent to a neighboring router during an interval.<br>• Limit--Maximum number of RSVP messages to send per queue interval.<br>• Maxsize--Maximum size of the message queue, in bytes.<br>• Period--Length of an interval (time frame), in milliseconds (ms).<br>• Max rate--Maximum number of messages allowed to be sent per second. |

| Field | Description |
|---|---|
| Refresh Reduction: enabled or disabled | The RSVP refresh-reduction parameters in effect are as follows:<br>• ACK delay (msec)--How long, in milliseconds, before the receiving router sends an acknowledgment (ACK).<br>• Initial retransmit delay (msec)--How long, in milliseconds, before the router retransmits a message.<br>• Local epoch--The RSVP message identifier (ID); randomly generated each time a node reboots or the RSVP process restarts.<br>• Message IDs--The number of message IDs in use, the total number allocated, and the total number available (freed). |
| Neighbors | The total number of neighbors and the types of encapsulation in use including RSVP and User Datagram Protocol (UDP). |
| RFC 3175 Aggregation | The state of aggregation as defined in RFC 3175, *AggregationofRSVPforIPv4andIPv6Reservations*; values are the following:<br>• Enabled--Active.<br>• Disabled--Inactive. |
| Level | Aggregation level of the reservations; common values are the following:<br>• 0 = End-to-end (E2E) reservations.<br>• 1 = Aggregated reservations.<br>Level x reservations can be aggregated to form reservations at level $x$ +1. |

| Field | Description |
|---|---|
| Default QoS service | Type of QoS configured; values are the following:<br>• Controlled-Load--Allows applications to reserve bandwidth to meet their requirements. For example, RSVP with Weighted Random Early Detection (WRED) provides this kind of service.<br>• Guaranteed-Rate--Allows applications to have low delay and high throughput even during times of congestion. For example, weighted fair queueing (WFQ) with RSVP provides this kind of service. |
| Number of signaled aggregate reservations | Cumulative number of signaled aggregate reservations. |
| Number of signaled E2E reservations | Cumulative number of signaled E2E reservations. |
| Number of configured map commands | Cumulative number of configured map commands. |
| Number of configured reservation commands | Cumulative number of configured reservation commands. |
| Hello | Subsequent fields describe the processes for which hello is enabled or disabled. Choices are Fast Reroute, reroute (hello for state timer), bidirectional forwarding detection (BFD), and Graceful Restart for a node with restart capability. |
| Statistics | Status of hello statistics. Valid values are as follows:<br>• Enabled--Statistics are configured. Hello packets are time-stamped when they arrive in the hello input queue for the purpose of recording the time it takes until they are processed.<br>• Disabled--Hello statistics are not configured.<br>• Shutdown--Hello statistics are configured, but not operational. The input queue is too long (that is, more than 10,000 packets are queued). |

| Field | Description |
|---|---|
| Graceful Restart: Enabled or Disabled | The RSVP Graceful Restart parameters in effect are as follows:<br>• Refresh interval--Frequency, in milliseconds (ms), with which a node sends a hello message to its neighbor.<br>• Refresh misses--Number of missed hello messages that trigger a neighbor-down event upon which stateful switchover (SSO) procedures are started.<br>• DSCP--Differentiated services code point (DSCP) value in the IP header of a hello message.<br>• Advertised restart time--Time, in milliseconds, required for the sender to restart the RSVP-traffic engineering component and exchange hello messages after a failure.<br>• Advertised recovery time--Time, in milliseconds, within which a recovering node wants its neighbor router to resynchronize the RSVP or MPLS forwarding state after SSO. A zero value indicates that the RSVP or MPLS forwarding state is not preserved after SSO.<br>• Maximum wait for recovery--Maximum amount of time, in milliseconds, that a router waits for a neighbor to recover. |
| Fast-Reroute | The Fast Reroute parameters in effect are as follows:<br>• PSBs w/ Local protection desired--Yes means that path state blocks (PSBs) are rerouted when a tunnel goes down and packet flow is not interrupted; No means that PSBs are not rerouted. |
| Fast Local Repair: enabled or disabled | The Fast Local Repair parameters in effect are as follows:<br>• Max repair rate (paths/sec)--Maximum repair rate, in paths per second.<br>• Max processed (paths/run)--Maximum notification elements processed, in paths per run. |
| Local policy | The local policy currently configured. |

| Field | Description |
|---|---|
| COPS | The Common Open Policy Service (COPS) currently in effect. |
| Generic policy settings | Policy settings that are not specific to COPS or the local policy.<br>• Default policy: 'Accept all' means that all RSVP messages are accepted and forwarded. 'Reject all' means all RSVP messages are rejected.<br>• Preemption: 'Disabled' means that RSVP is not prioritizing reservations and allocating bandwidth accordingly. 'Enabled' means that RSVP is prioritizing reservations and allocating more bandwidth to those with the highest priority. |

## Related Commands

| Command | Description |
|---|---|
| **debug ip rsvp** | Displays debug messages for RSVP categories. |
| **show ip rsvpatm-peak-rate-limit** | Displays the current peak rate limit set for an interface or for all interfaces. |
| **show ip rsvpcounters** | Displays the number of RSVP messages sent and received on each interface. |
| **show ip rsvp host** | Displays specific information for an RSVP host. |
| **show ip rsvp installed** | Displays RSVP related installed filters and corresponding bandwidth information. |
| **show ip rsvp interface** | Displays information about interfaces on which RSVP is enabled. |
| **show ip rsvp listeners** | Displays the RSVP listeners for a specified port or protocol. |
| **show ip rsvp neighbor** | Displays information about the current RSVP neighbors. |
| **show ip rsvp policy** | Displays information about the currently configured RSVP policies. |
| **show ip rsvp precedence** | Displayes IP precedence information about the interfaces on which RSVP is enabled. |

| Command | Description |
|---|---|
| **show ip rsvp request** | Displays current RSVP-related request information. |
| **show ip rsvp reservation** | Displays current RSVP-related receiver information. |
| **show ip rsvp sbm** | Displays SBM configuration information about RSVP-enabled interfaces. |
| **show ip rsvp sender** | Displays the RSVP PATH-related sender information |
| **show ip rsvp signalling** | Displays RSVP signaling information. |
| **show ip rsvp tos** | Displayes IP ToS information about the interfaces on which RSVP is enabled. |

# show ip rsvp aggregation ip

To display Resource Reservation Protocol (RSVP) summary aggregation information, use the **showiprsvpaggregationip** command in user EXEC or privileged EXEC mode.

**show ip rsvp aggregation ip** [**endpoints [detail]** [**dscp** *value*] [**remote** *ip-address*] [**role** {**aggregator**| **deaggregator**}]| **interface** [ *if-name* ]| **map** [**dscp** *value*]| **reservation** [**dscp** *value* [**aggregator** *ip-address*]]]

## Syntax Description

| | |
|---|---|
| **endpoints** | (Optional) Specifies the aggregator and deaggregator nodes for the aggregation region. |
| **interface** *if-name* | (Optional) Specifies the interface name. |
| **map** | (Optional) Displays the map configuration rules. |
| **dscp** *value* | (Optional) Specifies the differentiated services code point (DSCP) for the **map** keyword. Values can be the following:<br>• 0 to 63--Numerical DSCP values. The default value is 0.<br>• af11 to af43--Assured forwarding (AF) DSCP values.<br>• cs1 to cs7--Type of service (ToS) precedence values.<br>• default--Default DSCP value.<br>• ef--Expedited forwarding (EF) DSCP values. |
| **reservation** | (Optional) Displays the reservation configuration. |
| **dscp** *value* | (Optional) Specifies the differentiated services code point (DSCP) for the **reservation** keyword. Values can be the following:<br>• 0 to 63--Numerical DSCP values. The default value is 0.<br>• af11 to af43--Assured forwarding (AF) DSCP values.<br>• cs1 to cs7--Type of service (ToS) precedence values.<br>• default--Default DSCP value.<br>• ef--Expedited forwarding (EF) DSCP values. |

| | | |
|---|---|---|
| **aggregator** | *ip-address* | (Optional) Specifies the IP address of the aggregator. |

## Command Default

If you enter the **showiprsvpaggregationip**command without an optional keyword, the command displays summary information for all aggregate reservations.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRC | This command was introduced. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

Use the **showiprsvpaggregationip**command to display summary information for aggregation, including the number of aggregate, map, and reservation configurations.

## Examples

## Examples

The following is sample output from the **showiprsvpaggregationip** command:

```
Router# show ip rsvp aggregation ip
RFC 3175 Aggregation:  Enabled
  Level: 1
  Default QoS service: Controlled-Load
  Number of signaled aggregate reservations:  2
  Number of signaled E2E reservations:        8
  Number of configured map commands:          4
  Number of configured reservation commands:  1
```

The table below describes the significant fields shown in the display.

***Table 80: show ip rsvp aggregation ip Field Descriptions***

| Field | Description |
|---|---|
| RFC 3175 Aggregation | The state of aggregation as defined in RFC 3175, *AggregationofRSVPforIPv4andIPv6Reservations*; values are the following:<br>• Enabled--Active.<br>• Disabled--Inactive. |

| Field | Description |
|---|---|
| Level | Aggregation level of the reservations; common values are the following:<br>• 0 = End-to-end (E2E) reservations.<br>• 1 = Aggregated reservations.<br>**Note** Level x reservations can be aggregated to form reservations at the next higher level; for example, level x+1. |
| Default QoS service | Type of quality of service (QoS) configured; values are the following:<br>• Controlled-Load--Allows applications to reserve bandwidth to meet their requirements. For example, RSVP with Weighted Random Early Detection (WRED) provides this kind of service.<br>• Guaranteed-Rate--Allows applications to have low delay and high throughput even during times of congestion. For example, Weighted Fair Queueing (WFQ) with RSVP provides this kind of service. |
| Number of signaled aggregate reservations | Cumulative number of signaled aggregate reservations. |
| Number of signaled E2E reservations | Cumulative number of signaled E2E reservations. |
| Number of configured map commands | Cumulative number of configured map commands. |
| Number of configured reservation commands | Cumulative number of configured reservation commands. |

## Examples

The following is sample output from the **showiprsvpaggregationipinterface** command:

```
Router# show ip rsvp aggregation ip interface
Interface Name       Role
-------------------- --------
Ethernet0/0          interior
Serial2/0            exterior
Serial3/0            exterior
```

The table below describes the significant fields shown in the display.

*Table 81: show ip rsvp aggregation ip interface Field Descriptions*

| Field | Description |
|---|---|
| Interface Name | Name and number of the interface. |
| Role | Configuration of a router's interfaces; values are interior and exterior. |

The following is sample output from the **showiprsvpaggregationipinterface** command with a specified interface:

```
Router# show ip rsvp aggregation ip interface Ethernet0/0
Interface Name       Role
-------------------- --------
Ethernet0/0          interior
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp aggregation ip** | Enables RSVP aggregation on a router. |

# show ip rsvp aggregation ip endpoints

To display Resource Reservation Protocol (RSVP) information about aggregator and deaggregator routers, use the **showiprsvpaggregationipendpoints** command in user EXEC or privileged EXEC mode.

**show ip rsvp aggregation ip endpoints [detail]** [**dscp** *value*] [**remote** *ip-address*] [**role** {**aggregator**| **deaggregator**}]

## Syntax Description

| | |
|---|---|
| **detail** | (Optional) Displays additional information about the aggregators and deaggregators. |
| **dscp** *value* | (Optional) Specifies the differentiated services code point (DSCP) for the aggregator and deaggregator routers. Values can be the following:<br>• 0 to 63--Numerical DSCP values. The default value is 0.<br>• af11 to af43--Assured forwarding (AF) DSCP values.<br>• cs1 to cs7--Type of service (ToS) precedence values.<br>• default--Default DSCP value.<br>• ef--Expedited forwarding (EF) DSCP values. |
| **remote** | (Optional) Specifies the remote deaggregator. |
| *ip-address* | IP address of the remote deaggregator. |
| **role** | (Optional) Specifies a router's position in the aggregation region. |
| **aggregator** | (Optional) Specifies the router at the beginning of the aggregation region. |
| **deaggregator** | (Optional) Specifies the router at the end of the aggregation region. |

## Command Default

If you enter the **showiprsvpaggregationipendpoints**command without an optional keyword, the command displays information for all aggregate reservations.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRC | This command was introduced. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

Use the **showiprsvpaggregationipendpoints**command to display any of the following output at aggregator and deaggregator routers:

- All aggregate reservations.
- All aggregate reservations for which a node is the aggregator.
- All aggregate reservations for which a node is the deaggregator.
- All aggregate reservations for which the remote node is identified with an IP address.
- All aggregate reservations for a given DSCP.
- Any combination of the preceding options; for example, all aggregates with a given DSCP for which a node is an aggregator and the remote node as specified in the IP address.
- Any of the preceding options with detailed information.

## Examples

The following is sample output from the **showiprsvpaggregationipendpointsdetail** command:

```
Router# show ip rsvp aggregation ip endpoints detail
Role  DSCP Aggregator      Deaggregator    State  Rate    Used    QBM PoolID
----- ---- --------------- --------------- ------ ------- ------- ----------
Agg   46   10.3.3.3         10.4.4.4         ESTABL 100K    100K    0x00000003
   Aggregate Reservation for the following E2E Flows (PSBs):
To             From          Pro DPort Sport  Prev Hop       I/F      BPS
10.4.4.4       10.1.1.1       UDP 1     1     10.23.20.3     Et1/0    100K
   Aggregate Reservation for the following E2E Flows (RSBs):
To             From          Pro DPort Sport  Next Hop       I/F      Fi Serv BPS
10.4.4.4       10.1.1.1       UDP 1     1     10.4.4.4       Se2/0    FF RATE 100K
   Aggregate Reservation for the following E2E Flows (Reqs):
To             From          Pro DPort Sport  Next Hop       I/F      Fi Serv BPS
10.4.4.4       10.1.1.1       UDP 1     1     10.23.20.3     Et1/0    FF RATE 100K
```

The table below describes the significant fields shown in the display.

***Table 82: show ip rsvp aggregation ip endpoints detail Field Descriptions***

| Field | Description |
|---|---|
| Role | The router's function; values are aggregator or deaggregator. |
| DSCP | DSCP value. |
| Aggregator | IP address of the aggregator. |

| Field | Description |
|---|---|
| Deaggregator | IP address of the deaggregator. |
| State | Status of the reservation. Each aggregate reservation can be in one of the following states:<br>• PATH_WAIT--Valid at the deaggregator only. The aggregate reservation at the deaggregator enters this state after the deaggregator has sent a PATHERROR message requesting a new aggregate needed.<br>• RESV_WAIT--Valid at the aggregator only. The aggregate reservation at the aggregator enters this state after the aggregator has sent a PATH message for the aggregate reservation.<br>• RESVCONF_WAIT--Valid at the deaggregator only. The aggregate reservation at the deaggregator enters this state after the deaggregator has sent a RESV message for the aggregate reservation.<br>• ESTABLISHED--Valid at both the aggregator and the deaggregator. The aggregator enters this state after a RESVCONF message has been sent. The deaggregator enters this state after it receives a RESVCONF message for the aggregate reservation.<br>• SHUT_DELAY--Valid at both the aggregator and the deaggregator. The aggregator and the deaggregator enter this state after the last end-to-end (E2E) reservation has been removed. |
| Rate | Allocated bandwidth in bits per second (BPS). |
| Used | Amount of bandwidth used in bits per second (BPS). |
| QBM Pool ID | The quality of service (QoS) bandwidth manager (QBM) ID for the reservation. |
| Aggregate Reservation for the following E2E Flows | Information for the reservation:<br>PSB--path state block. Contains data used for forwarding PATH messages downstream;<br>RSB--reservation state block. Contains data for the incoming RESV message.<br>Reqs--requests. Contain data required to forward a RESV message upstream to the node that sent the PATH message. |

| Field | Description |
|---|---|
| To | IP address of the receiver. |
| From | IP address of the sender. |
| Pro | Protocol code. Code indicates IP protocol such as TCP or User Datagram Protocol (UDP). |
| DPort | Destination port number. |
| Sport | Source port number. |
| Prev Hop or Next Hop | IP address of the previous or next hop. |
| I/F | Interface of the previous or next hop. |
| Fi | Filter (Wildcard Filter, Shared-Explicit, or Fixed-Filter). |
| Serv | Service (RATE or LOAD). |
| BPS | Bandwidth used by the aggregate reservation in bits per second (BPS). |

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp aggregation ip** | Enables RSVP aggregation on a router. |

# show ip rsvp atm-peak-rate-limit

To display the current peak rate limit set for an interface or for all interfaces, if any, use the **showiprsvpatm-peak-rate-limit** command in EXEC mode.

**show ip rsvp atm-peak-rate-limit** [*interface-type interface-number*]

## Syntax Description

| | |
|---|---|
| *interface-type interface-number* | (Optional) Interface type and interface number. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

The **showiprsvpatm-peak-rate-limit**command displays the configured peak rate using the following notations for brevity:

- Kilobytes is shown as K bytes; for example, 1200 kilobytes is displayed as 1200K bytes.
- 1000 kilobytes is displayed as 1M bytes.

If no interface name is specified, configured peak rates for all Resource Reservation Protocol (RSVP)-enabled interfaces are displayed.

## Examples

The following example depicts results of the **showiprsvpatm-peak-rate-limit** command, presuming that the ATM subinterface 2/0/0.1 was configured with a reservation peak rate limit of 100 KB using the **iprsvpatm-peak-rate-limit** command.

The following is sample output from the **showiprsvpatm-peak-rate-limit** command using the *interface-type interface-number* arguments:

```
Router# show ip rsvp atm-peak-rate-limit atm2/0/0.1
RSVP: Peak rate limit for ATM2/0/0.1 is 100K bytes
```

The following samples show output from the **showiprsvpatm-peak-rate-limit** command when no interface name is given:

```
Router# show ip rsvp atm-peak-rate-limit

Interface name         Peak rate limit
Ethernet0/1/1         not set
ATM2/0/0              not set
```

```
ATM2/0/0.1            100K
Router# show ip rsvp atm-peak-rate-limit
Interface name        Peak rate limit
Ethernet0/1           not set
ATM2/1/0              1M
ATM2/1/0.10           not set
ATM2/1/0.11           not set
ATM2/1/0.12           not set
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp atm-peak-rate-limit** | Sets a limit on the peak cell rate of reservations for all newly created RSVP SVCs established on the current interface or any of its subinterfaces. |

# show ip rsvp authentication

To display the security associations that Resource Reservation Protocol (RSVP) has established with other RSVP neighbors, use the show **iprsvpauthentication**command in user EXEC or privileged EXEC mode.

**show ip rsvp authentication [detail]** [**from** {*ip-address*| *hostname*}] [**to** {*ip-address*| *hostname*}]

## Syntax Description

| | |
|---|---|
| **detail** | (Optional) Displays additional information about RSVP security associations. |
| **from** | (Optional) Specifies the starting point of the security associations. |
| **to** | (Optional) Specifies the ending point of the security associations. |
| **ip-address** | (Optional) Information about a neighbor with a specified IP address. |
| **hostname** | (Optional) Information about a particular host. |

## Command Modes

User EXEC (<) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(15)T | This command was introduced. |
| 12.0(29)S | The optional**from**and **to**keywords were added. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

## Usage Guidelines

Use the show ip rsvp authentication command to display the security associations that RSVP has established with other RSVP neighbors. You can display all security associations or specify an IP address or hostname of a particular RSVP neighbor, which restricts the size of the display.

The difference between the *ip-address* and*hostname* arguments is whether you specify the neighbor by its IP address or by its name.

## Examples

The following is sample output from the **showiprsvpauthenticationcommand**:

```
Router# show ip rsvp authentication
Codes: S - static, D - dynamic, N - neighbor, I -interface, C - chain
From            To              I/F      Mode    Key-Source Key-ID       Code
192.168.102.1   192.168.104.3   Et2/2    Send    RSVPKey    1            DNC
192.168.104.1   192.168.104.3   Et2/2    Send    RSVPKey    1            DNC
192.168.104.1   192.168.104.3   AT1/0.1  Send    RSVPKey    1            DNC
192.168.106.1   192.168.104.3   AT1/0.1  Send    RSVPKey    1            DNC
192.168.106.1   192.168.106.2   AT1/0.1  Send    RSVPKey    1            DNC
192.168.106.2   192.168.104.1   AT1/0.1  Receive RSVPKey    1            DNC
192.168.106.2   192.168.106.1   AT1/0.1  Receive RSVPKey    1            DNC
```

The table below describes the significant fields shown in the display.

***Table 83: show ip rsvp authentication Field Descriptions***

| Field | Description |
|---|---|
| Codes | Keys can be either static (manually configured) or dynamic (created from a per-ACL key or obtained from a key management server such as Kerberos). Cisco IOS software does not currently support dynamic keys from key management servers. If the field contains the string per-neighbor, it means the security association is using a per-neighbor key; if the field contains the string per-interface, it means the security association is using a per-interface key. If the field contains the string chain, it means the key for the security association comes from the key chain specified in the Key Source. |
| From | Starting point of the security association. |
| To | Ending point of the security association. |
| I/F | Name and number of the interface over which the security association is being maintained. |
| Mode | Separate associations maintained for sending and receiving RSVP messages for a specific RSVP neighbor. Possible values are **Send**or**Receive**. |
| Key-Source | Indicates where the key was configured. |

| Field | Description |
|---|---|
| Key-ID | A string which, along with the IP address, uniquely identifies a security association. The key ID is automatically generated in Cisco IOS software by using the per-interface **iprsvpauthenticationkey**command, but it is configured in Cisco IOS software when using key chains for per-neighbor or per-interface RSVP keys. The key ID may be configurable on other RSVP platforms. A key ID is provided in every RSVP authenticated message initiated by a sender and is stored by every RSVP receiver.<br>**Note** **Key Expired** in this field means that all possible keys used for this neighbor have expired. |
| Code | Indicates the type of key ID used. |

The following is sample output from the s**howiprsvpauthentication** detail command:

```
Router# show ip rsvp authentication detail
From:                   192.168.102.1
To:                     192.168.104.3
Neighbor:               192.168.102.2
Interface:              Ethernet2/2
Mode:                   Send
Key ID:                 1
Key ACL:                R2 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 01000411
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:17:08
Challenge:              Supported
Window size:            1
Last seq # sent:        14167519095569779135
From:                   192.168.104.1
To:                     192.168.104.3
Neighbor:               192.168.102.2
Interface:              Ethernet2/2
Mode:                   Send
Key ID:                 1
Key ACL:                R2 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 0400040F
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:22:06
Challenge:              Supported
Window size:            1
Last seq # sent:        14167520384059965440
From:                   192.168.104.1
To:                     192.168.104.3
Neighbor:               192.168.106.2
Interface:              ATM1/0.1
Mode:                   Send
Key ID:                 1
Key ACL:                R3 (populated)
Key Source:             RSVPKey (enabled)
```

```
Key Type:               Dynamic per-neighbor chain
Handle:                 02000404
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:16:37
Challenge:              Supported
Window size:            1
Last seq # sent:        14167518979605659648
From:                   192.168.106.1
To:                     192.168.104.3
Neighbor:               192.168.106.2
Interface:              ATM1/0.1
Mode:                   Send
Key ID:                 1
Key ACL:                R3 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 01000408
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:11:37
Challenge:              Supported
Window size:            1
Last seq # sent:        14167517691115473376
From:                   192.168.106.1
To:                     192.168.106.2
Neighbor:               192.168.106.2
Interface:              ATM1/0.1
Mode:                   Send
Key ID:                 1
Key ACL:                R3 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 8D00040E
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:29:29
Challenge:              Supported
Window size:            1
Last seq # sent:        14167808344437293057
From:                   192.168.106.2
To:                     192.168.104.1
Neighbor:               192.168.106.2
Interface:              ATM1/0.1
Mode:                   Receive
Key ID:                 1
Key ACL:                R3 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 CD00040A
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:29:33
Challenge:              Not configured
Window size:            1
Last seq # rcvd:        14167808280012783626
From:                   192.168.106.2
To:                     192.168.106.1
Neighbor:               192.168.106.2
Interface:              ATM1/0.1
Mode:                   Receive
Key ID:                 1
Key ACL:                R3 (populated)
Key Source:             RSVPKey (enabled)
Key Type:               Dynamic per-neighbor chain
Handle:                 C0000412
Hash Type:              MD5
Lifetime:               00:30:00
Expires:                00:29:33
Challenge:              Not configured
Window size:            1
Last seq # rcvd:        14167808280012783619
```

The table below describes the significant fields shown in the display.

***Table 84: show ip rsvp authentication detail Field Descriptions***

| Field | Description |
|---|---|
| From | Starting point of the security association. |
| To | Ending point of the security association. |
| Neighbor | IP address of the RSVP neighbor with which the security association is being maintained. |
| Interface | Name and number of the interface over which the security association is being maintained. |
| Mode | Separate associations maintained for sending and receiving RSVP messages for a specific RSVP neighbor. Possible values are Send or Receive. |
| Key ID | A string which, along with the IP address, uniquely identifies a security association. The key ID is automatically generated in Cisco IOS software by using the per-interface **iprsvpauthenticationkey** command, but it is configured in Cisco IOS software when using key chains for per-neighbor or per-interface RSVP keys. The key ID may be configurable on other RSVP platforms. A key ID is provided in every RSVP authenticated message initiated by a sender and is stored by every RSVP receiver.<br>**Note** **Key Expired** in this field means that all possible keys used for this neighbor have expired. |
| Key ACL | For key types that say dynamic and chain, this field indicates which ACL matched that neighbor, and therefore, which key chain to use. Possible values include:<br>• **populated** = ACL has entries in it.<br>• **removed** = ACL has been removed from the configuration. |
| Key Source | Indicates where the key was configured and whether it is enabled or disabled. For key chains, this indicates the name of the key chain; the Key ID field indicates which key in the chain is currently being used. For per-interface keys, this field contains the name of the interface that was configured with the key. |

| Field | Description |
|---|---|
| Key Type | Static (manually configured) or dynamic (created from a per-ACL key or obtained from a key management server such as Kerberos).<br>**Note** Cisco IOS software does not currently support dynamic keys from key management servers. |
| Handle | Internal database ID assigned to the security association by RSVP for bookkeeping purposes. |
| Hash Type | Type of secure hash algorithm being used with that neighbor. |
| Lifetime | Maximum amount of time (in hours, minutes, and seconds) that can elapse before a security association is expired.<br>**Note** This is not how long a key is valid; to obtain duration times for keys, use the **showkeychain** command. |
| Expires | Amount of time remaining (in days, hours, minutes, and seconds) before the security association expires.<br>**Note** This is not when the current key expires; to obtain expiration times for keys, use the **showkeychain** command. |
| Challenge | For receive-type security associations, possible values are **NotConfigured**, **Completed**, **InProgress**, and **Failed**. For send-type security associations, the value is **Supported**. Cisco IOS software can always respond to challenges; however, there may be non-Cisco neighbors that do not implement challenges. |
| Window size | Indicates the size of the window for receive-type security associations and the maximum number of authenticated RSVP messages that can be received out-of-order before a replay attack is to be suspected. |
| Last seq # sent | Displayed only for send-type security associations. It indicates the sequence number used to send the last authenticated message to the RSVP neighbor. Use this information to troubleshoot certain types of authentication problems. |

| Field | Description |
|---|---|
| Last valid seq # rcvd | Displayed only for receive-type security associations. It indicates the authentication sequence number of the last valid RSVP message received from the neighbor. By default, it shows only one sequence number. However, if you use the ip rsvp authentication window-size command to increase the authentication window size to n, then the last n valid received sequence numbers are displayed. Use this information to troubleshoot certain types of authentication problems. |

## Related Commands

| Command | Description |
|---|---|
| **clear ip rsvp authentication** | Eliminates RSVP security associations before their lifetimes expire. |

# show ip rsvp counters

To display the number of Resource Reservation Protocol (RSVP) messages that were sent and received on each interface, use the **showiprsvpcounters** command in user EXEC or privileged EXEC mode.

**show ip rsvp counters [authentication] [interface** *type number*| **neighbor** [**vrf** {*****| *vrf-name*}]| **state teardown**| **summary**]

## Syntax Description

| | |
|---|---|
| **authentication** | (Optional) Displays a list of RSVP authentication counters. |
| **interface** *type number* | (Optional) Displays the number of RSVP messages sent and received for the specified interface name. |
| **neighbor** | (Optional) Displays the number of RSVP messages sent and received by the specified neighbor. |
| vrf * | (Optional) Displays all the configured virtual routing and forwarding (VRF) instances. |
| **vrf** *vrf-name* | (Optional) Displays the name of a specified VRF. |
| **state teardown** | (Optional) Displays the number of RSVP message states and the reasons for teardown. |
| **summary** | (Optional) Displays the cumulative number of RSVP messages sent and received by the router over all interfaces. |

## Command Default

If you enter the **showiprsvpcounters** command without an optional keyword, the command displays the number of RSVP messages that were sent and received for each interface on which RSVP is configured.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(14)ST | This command was introduced. |
| 12.2(13)T | The **neighbor** keyword was added, and the command was integrated into Cisco IOS Release 12.2(13)T. |

| Release | Modification |
|---|---|
| 12.2(15)T | The command output was modified to show the errors counter incrementing whenever an RSVP message is received on an interface with RSVP authentication enabled, but the authentication checks failed on that message. |
| 12.2(11)S | This command was integrated into Cisco IOS Release 12.2(11)S. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. |
| 12.0(29)S | The **authentication**keyword was added, and the command output was modified to include hello and message queues information. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |
| 15.0(1)M | This command was modified. The **vrf** and ***keywords and the *vrf-name* argument were added. |

## Examples

## Examples

The following example shows the values for the number of RSVP messages of each type that were sent and received by the router over all interfaces, including the hello and message queues information:

```
Router# show ip rsvp counters summary
All Interfaces          Recv      Xmit                        Recv      Xmit
    Path                 110        15    Resv                   50        28
    PathError              0         0    ResvError               0         0
    PathTear               0         0    ResvTear                0         0
    ResvConf               0         0    RTearConf               0         0
    Ack                    0         0    Srefresh                0         0
    Hello               5555      5554    IntegrityChalle         0         0
    IntegrityRespon        0         0    DSBM_WILLING            0         0
    I_AM_DSBM              0         0
    Unknown                0         0    Errors                  0         0
Recv Msg Queues                Current       Max
    RSVP                             0         2
    Hello (per-I/F)                  0         1
    Awaiting Authentication          0         0
```

The table below describes the significant fields shown in the display.

*Table 85: show ip rsvp counters summary Field Descriptions*

| Field | Description |
|---|---|
| All Interfaces | Types of messages displayed for all interfaces.<br>**Note** Hello is a summary of graceful restart, reroute (hello state timer), and Fast Reroute messages. |
| Recv | Number of messages received on the specified interface or on all interfaces. |
| Xmit | Number of messages transmitted from the specified interface or from all interfaces. |
| Recv Msg Queues | Queues for received messages for RSVP, hello per interface, and awaiting authentication.<br>• Current--Number of messages queued.<br>• Max--Maximum number of messages ever queued. |

## Examples

The following example shows the values for the number of RSVP messages for a specified neighbor with a VRF named myvrf:

```
Router# show ip rsvp counters neighbor vrf myvrf
VRF: myvrf
Neighbor: 10.10.15.13
      Rate-Limiting:
        Output queue overflow, number of dropped RSVP messages: 0
      Refresh-Reduction:
        Number of RSVP messages received out of order: 0
        Number of retransmitted RSVP messages: 0
```

The table below describes the significant fields shown in the display.

*Table 86: show ip rsvp counters neighbor vrf Field Descriptions*

| Field | Description |
|---|---|
| VRF | Name of the VRF. |
| Neighbor | IP address of the neighbor. |
| Rate-Limiting | The rate-limiting parameters in effect are as follows:<br>• Output queue overflow, number of dropped RVSP messages--Number of messages dropped by the neighbor when the queue overflowed. |

| Field | Description |
|---|---|
| Refresh-Reduction | The refresh-reduction parameters in effect are as follows:<br>• Number of RSVP messages received out of order--Messages that were dropped because they were out of sequential order.<br>• Number of retransmitted RSVP messages--Number of messages retransmitted to the neighbor. |

## Related Commands

| Command | Description |
|---|---|
| **clear ip rsvp counters** | Clears (sets to zero) all IP RSVP counters that are being maintained. |

# show ip rsvp counters state teardown

To display counters for Resource Reservation Protocol (RSVP) events that caused a state to be torn down, use the **showiprsvpcountersstateteardown**command in user EXEC or privileged EXEC mode.

**show ip rsvp counters state teardown**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(29)S | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

Use the **showiprsvpcountersstateteardown** command when a label-switched path (LSP) is down. If graceful restart triggered the state teardown, the numbers in the Path, Resv-In, and Resv-Out columns in the " Examples" section are greater than 0.

## Examples

The following is sample output from the **showiprsvpcountersstateteardown** command:

```
Router# show ip rsvp counters state teardown
States
  Reason for Teardown                          State torn down
                                                 Path    Resv-In   Resv-Out
  PathTear arrival                                  0          0          0
  ResvTear arrival                                  0          0          0
  Local application requested tear                  0          0          0
  Output or Input I/F went down                     0          0          0
  Missed refreshes                                  0          0          0
  Preemption                                        0          0          0
  Backup tunnel failed for FRR Active LSP           0          0          0
  Reroutabilty changed for FRR Active LSP           0          0          0
  Hello RR Client (HST) requested tear              0          0          0
  Graceful Restart (GR) requested tear              0          0          0
  Downstream neighbor SSO-restarting                0          0          0
  Resource unavailable                              0          0          0
  Policy rejection                                  0          0          0
  Policy server sync failed                         0          0          0
  Traffic control error                             0          0          0
  Error in received message                         0          0          0
  Non RSVP HOP upstream, TE LSP                     0          0          0
  Other                                             0          0          0
```

The table below describes the significant fields shown in the display.

*Table 87: show ip rsvp counters state teardown Field Descriptions*

| Field | Description |
|---|---|
| States | RSVP state, including path state block (PSB) and reservation state block (RSB) information. |
| Reason for Teardown | Event triggering the teardown. |

## Related Commands

| Command | Description |
|---|---|
| **clear ip rsvp counters** | Clears (sets to zero) the IP RSVP counters that are being maintained. |

# show ip rsvp fast bw-protect

To display information about whether backup bandwidth protection is enabled and the status of backup tunnels that may be used to provide that protection, use the **showiprsvpfastbw-protect** command in user EXEC or privileged EXEC mode.

**show ip rsvp fast bw-protect [detail]** [**filter** [**destination** *ip-address*| *hostname*] [**dst-port** *port-number*] [**source** *ip-address*| *hostname*] [**src-port** *port-number*]]

## Syntax Description

| | |
|---|---|
| **detail** | (Optional) Specifies additional receiver information. |
| **filter** | (Optional) Specifies a subset of the receivers to display . |
| **destination** *ip-address* | (Optional) Specifies the destination IP address of the receiver. |
| *hostname* | (Optional) Specifies the hostname of the receiver. |
| **dst-port** *port-number* | (Optional) Specifies the destination port number. Valid destination port numbers must be in the range from 0 to 65535. |
| **source** *ip-address* | (Optional) Specifies the source IP address of the receiver. |
| **src-port** *port-number* | (Optional) Specifies the source port number. Valid source port numbers must be in the range from 0 to 65535. |

## Command Default

The backup bandwidth protection and backup tunnel status information is not displayed.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(29)S | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

| Release | Modification |
|---|---|
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T |

## Examples

The following is sample output from the **showiprsvpfastbw-protect** command:

```
Router# show ip rsvp fast bw-protect

Primary          Protect  BW         Backup
Tunnel           I/F      BPS:Type   Tunnel:Label  State   BW-P    Type
--------------   -------  --------   ----------    -----   ----    ----
PRAB-72-5_t500   PO2/0    500K:S     Tu501:19      Ready   ON      Nhop
PRAB-72-5_t601   PO2/0    103K:S     Tu501:20      Ready   OFF     Nhop
PRAB-72-5_t602   PO2/0    70K:S      Tu501:21      Ready   ON      Nhop
PRAB-72-5_t603   PO2/0    99K:S      Tu501:22      Ready   ON      Nhop
PRAB-72-5_t604   PO2/0    100K:S     Tu501:23      Ready   OFF     Nhop
PRAB-72-5_t605   PO2/0    101K:S     Tu501:24      Ready   OFF     Nhop
```

The table below describes the significant fields shown in the display.

***Table 88: show ip rsvp fast bw-protect Field Descriptions***

| Field | Description |
|---|---|
| Primary Tunnel | Identification of the tunnel being protected. |
| Protect I/F | Interface name. |
| BW BPS:Type | Bandwidth, in bits per second, and type of bandwidth. Possible values are the following:<br>• S--Subpool<br>• G--Global pool |
| Backup Tunnel:Label | Identification of the backup tunnel. |
| State | Status of backup tunnel. Valid values are the following:<br>• Ready--Data is passing through the primary tunnel, but the backup tunnel is ready to take over if the primary tunnel goes down.<br>• Active--The primary tunnel is down, so the backup tunnel is used for traffic.<br>• None--There is no backup tunnel. |
| BW-P | Status of backup bandwidth protection. Possible values are ON and OFF. |

| Field | Description |
|---|---|
| Type | Type of backup tunnel. Possible values are the following:<br>• Nhop--Next hop<br>• NNHOP--Next-next hop |

## Related Commands

| Command | Description |
|---|---|
| **tunnel mpls traffic-eng fast-reroute bw-protect** | Enables an MPLS TE tunnel to use an established backup tunnel in the event of a link or node failure. |

# show ip rsvp fast detail

To display specific information for Resource Reservation Protocol (RSVP) categories, use the **showiprsvpfastdetail**command in user EXEC or privileged EXEC mode.

**show ip rsvp fast detail** [**filter** [**destination** *ip-address*| *hostname*] [**dst-port** *port-number*] [**source** *ip-address*| *hostname*] [**src-port** *port-number*]]

## Syntax Description

| | |
|---|---|
| **filter** | (Optional) Specifies a subset of the receivers to display . |
| **destination** *ip-address* | (Optional) Specifies the destination IP address of the receiver. |
| *hostname* | (Optional) Specifies the hostname of the receiver. |
| **dst-port** *port-number* | (Optional) Specifies the destination port number. Valid destination port numbers must be in the range from 0 to 65535. |
| **source** *ip-address* | (Optional) Specifies the source IP address of the receiver. |
| **src-port** *port-number* | (Optional) Specifies the source port number. Valid source port numbers must be in the range from 0 to 65535. |

## Command Default

Specific information for RSVP categories is not displayed.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(24)S | This command was introduced. |
| 12.0(29)S | Bandwidth Prot desired was added in the Flag field of the command output. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Examples

The following is sample output from the **showiprsvpfastdetail** command:

```
Router# show ip rsvp fast detail

PATH:
  Tun Dest:   10.0.0.7  Tun ID: 500  Ext Tun ID: 10.0.0.5
  Tun Sender: 10.0.0.5  LSP ID: 8
  Path refreshes:
    sent:     to   NHOP 10.5.6.6 on POS2/0
  Session Attr:
    Setup Prio: 7, Holding Prio: 7
    Flags: Local Prot desired, Label Recording, SE Style, Bandwidth Prot desired
    Session Name: PRAB-72-5_t500
  ERO: (incoming)
    10.0.0.5 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.5.6 (Strict IPv4 Prefix, 8 bytes, /32)
    10.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
  ERO: (outgoing)
    10.5.6.6 (Strict IPv4 Prefix, 8 bytes, /32)
    10.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
  Traffic params - Rate: 500K bits/sec, Max. burst: 1K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
  Fast-Reroute Backup info:
    Inbound  FRR: Not active
    Outbound FRR: Ready -- backup tunnel selected
      Backup Tunnel: Tu501      (label 19)
      Bkup Sender Template:
        Tun Sender: 10.5.6.5  LSP ID: 8
      Bkup FilerSpec:
        Tun Sender: 10.5.6.5, LSP ID: 8
  Path ID handle: 04000405.
  Incoming policy: Accepted. Policy source(s): MPLS/TE
  Status: Proxied
  Output on POS2/0. Policy status: Forwarding. Handle: 02000406
```

The table below describes the significant fields shown in the display.

***Table 89: show ip rsvp fast detail Field Descriptions***

| Field | Description |
|---|---|
| Tun Dest | IP address of the receiver. |
| Tun ID | Tunnel identification number. |
| Ext Tun ID | Extended tunnel identification number. |
| Tun Sender | IP address of the sender. |
| LSP ID | Label-switched path identification number. |
| Setup Prio | Setup priority. |
| Holding Prio | Holding priority. |
| Flags | Backup bandwidth protection has been configured for the label-switched path (LSP). |

| Field | Description |
|---|---|
| Session Name | Name of the session. |
| ERO (incoming) | EXPLICIT_ROUTE object of incoming path messages. |
| ERO (outgoing) | EXPLICIT_ROUTE object of outgoing path messages. |
| Traffic params Rate | Average rate, in bits per second. |
| Max. burst | Maximum burst size, in bytes. |
| Min Policed Unit | Minimum policed units, in bytes. |
| Max Pkt Size | Maximum packet size, in bytes. |
| Inbound FRR | Status of inbound Fast Reroute (FRR) backup tunnel. If this node is downstream from a rerouted LSP (for example, at a merge point for this LSP), the state is Active. |
| Outbound FRR | Status of outbound FRR backup tunnel. If this node is a point of local repair (PLR) for an LSP, there are three possible states:<br>• Active--This LSP is actively using its backup tunnel, presumably because there has been a downstream failure.<br>• No Backup--This LSP does not have local (Fast Reroute) protection. No backup tunnel has been selected for it to use in case of a failure.<br>• Ready--This LSP is ready to use a backup tunnel in case of a downstream link or node failure. A backup tunnel has been selected for it to use. |
| Backup Tunnel | If the Outbound FRR state is Ready or Active, this field indicates the following:<br>• Which backup tunnel has been selected for this LSP to use in case of a failure.<br>• The inbound label that will be prepended to the LSP's data packets for acceptance at the backup tunnel tail (the merge point). |

| Field | Description |
|---|---|
| Bkup Sender Template | If the Outbound FRR state is Ready or Active, SENDER_TEMPLATE and FILTERSPEC objects are shown. These objects will be used in RSVP messages sent by the backup tunnel if or when the LSP starts actively using the backup tunnel. They differ from the original (prefailure) objects only in that the node (the PLR) substitutes its own IP address for that of the original sender. For example, path and pathTear messages will contain the new SENDER_TEMPLATE. Resv and resvTear messages will contain the new FILTERSPEC object. If this LSP begins actively using the backup tunnel, the display changes. |
| Bkup FilerSpec | If the Outbound FRR state is Ready or Active, SENDER_TEMPLATE and FILTERSPEC objects are shown. These objects will be used in RSVP messages sent by the backup tunnel if or when the LSP starts actively using the backup tunnel. They differ from the original (prefailure) objects only in that the node (the PLR) substitutes its own IP address for that of the original sender. For example, path and pathTear messages will contain the new SENDER_TEMPLATE. Resv and resvTear messages will contain the new FILTERSPEC object. If this LSP begins actively using the backup tunnel, the display changes. |
| Path ID handle | Protection Switch Byte (PSB) identifier. |
| Incoming policy | Policy decision of the LSP. If RSVP policy was not granted for the incoming path message for the tunnel, the LSP does not come up. Accepted is displayed. |
| Policy source(s) | For FRR LSPs, this value always is MPLS/TE for the policy source. |
| Status | For FRR LSPs, valid values are as follows:<br>• Proxied--Headend routers.<br>• Proxied Terminated--Tailend routers.<br>For midpoint routers, the field always is blank. |

## Related Commands

| Command | Description |
|---|---|
| **mpls traffic-eng fast-reroute backup-prot-preemption** | Changes the backup protection preemption algorithm to minimize the amount of bandwidth that is wasted. |

# show ip rsvp fast-reroute

To display information about fast reroutable primary tunnels and their corresponding backup tunnels that provide protection, use the **showiprsvpfast-reroute**command in user EXEC or privileged EXEC mode.

**show ip rsvp fast-reroute** [**filter** [**session-type** {*session-type-number*| **all**}]]

## Syntax Description

| | |
|---|---|
| **filter** | (Optional) Specifies a subset of the tunnel to display . |
| **session-type** *session-type-number* | (Optional) Specifies the type of tunnels to display. Valid values are:<br>• **7** for IPv4 point-to-point (P2P) traffic engineering (TE) label switched path (LSP) tunnel sessions.<br>• **13** for IPv4 point-to-multipoint (P2MP) TE LSP tunnel sessions. |
| **session-type all** | (Optional) Specifies all types of tunnel sessions. |

## Command Default

If no arguments are specified, the display information about all fast reroutable primary tunnels is displayed.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(27)S | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |
| 12.2(33)SRE | This command was modified. The **filter** keyword was added to display tunnel information categorized by point-to-point and point-to-multipoint. The output was updated to display Multiprotocol Label Switching (MPLS) TE P2MP information. |
| 15.0(1)M | This command was modified. Support for classic IP RSVP (session type 1) was removed. |

## Examples

The following is sample output of fast reroutable primary tunnels and their corresponding backup tunnels that provide protection:

```
Router# show ip rsvp fast-reroute
Primary                 Protect BW         Backup
Tunnel                  I/F     BPS:Type   Tunnel:Label  State  Level  Type
------                  ------- --------   ------------- ------ -----  ---
GSR1---R2---_t65336     PO1/0   0:G        Tu1002:0      Ready  any-unl Nhop
GSR1---R2---_t65338     PO4/0   0:G        Tu1004:0      Ready  any-unl Nhop
```

The table below describes the significant fields shown in the display.

***Table 90: show ip rsvp fast-reroute Field Descriptions***

| Field | Description |
|---|---|
| Primary Tunnel | Hostname and tunnel ID. |
| Protect I/F | Interface that is being protected. |
| BW BPS:Type | Bandwidth, in bits per second, and the pool from which the bandwidth comes. Valid values are G, global pool, S, and subpool. |
| Backup Tunnel:Label | Backup tunnel ID and label. |
| State | Status of protection. Valid values are Ready, Active, and None. |
| Level | Level of bandwidth. Valid values are any and unl (unlimited). |
| Type | Type of backup tunnel: Nhop (next hop) or NNhop (next-next hop). |

The following example shows fast reroutable primary tunnels and their corresponding backup tunnels. The information is organized by P2P LSPs and P2MP sub-LSPs. The following example shows that Tunnel 22 has six sub-LSPs, three that are protected on Ethernet interface 0/0, and three that are not protected on Ethernet interface 0/1:

```
Router# show ip rsvp fast-reroute
P2P                         Protect BW         Backup
Protected LSP               I/F     BPS:Type   Tunnel:Label  State  Level   Type
-------------               ------- --------   ------------- ------ -----   ------
R201_t1                     Et0/1   500K:G     Tu777:16      Ready  any-lim Nhop
P2MP
Protected Sub-LSP                          Protect BW         Backup
src_lspid[subid]->dst_tunid                I/F     BPS:Type   Tunnel:Label  State
---------------------------                ------- --------   ------------- ------
10.1.1.201_1[1]->10.1.1.203_22               Et0/0   500K:G     Tu666:20      Ready
10.1.1.201_1[2]->10.1.1.206_22               Et0/0   500K:G     Tu666:20      Ready
10.1.1.201_1[3]->10.1.1.213_22               Et0/0   500K:G     Tu666:20      Ready
10.1.1.201_1[4]->10.1.1.214_22               Et0/1   500K:G     None          None
10.1.1.201_1[5]->10.1.1.216_22               Et0/1   500K:G     None          None
10.1.1.201_1[6]->10.1.1.217_22               Et0/1   500K:G     None          None
```

The following example displays information about fast reroutable primary tunnels and their corresponding backup tunnels for Cisco IOS Release 12.4(24)T and earlier releases. The output is organized by session type.

```
Rrouter# show ip rsvp fast-reroute filter session-type all

Session Type 1 (rsvp)
P2P                       Protect BW         Backup
Protected LSP             I/F     BPS:Type   Tunnel:Label  State  Level   Type
-------------             ------- --------   ------------- ------ -----   ------
Session Type 7 (te-p2p-lsp)
P2P                       Protect BW         Backup
Protected LSP             I/F     BPS:Type   Tunnel:Label  State  Level   Type
-------------             ------- --------   ------------- ------ -----   ------
R201_t1                   Et0/1   500K:G     Tu777:16      Ready  any-lim Nhop
Session Type 13 (te-p2mp-lsp)
P2MP
Protected Sub-LSP                          Protect BW         Backup
src_lspid[subid]->dst_tunid                I/F     BPS:Type   Tunnel:Label  State
---------------------------                ------- --------   ------------- ------
10.1.1.201_1[1]->10.1.1.203_22               Et0/0   500K:G     Tu666:20      Ready
10.1.1.201_1[2]->10.1.1.206_22               Et0/0   500K:G     Tu666:20      Ready
10.1.1.201_1[3]->10.1.1.213_22               Et0/0   500K:G     Tu666:20      Ready
10.1.1.201_1[4]->10.1.1.214_22               Et0/1   500K:G     None          None
10.1.1.201_1[5]->10.1.1.216_22               Et0/1   500K:G     None          None
10.1.1.201_1[6]->10.1.1.217_22               Et0/1   500K:G     None          None
```

The table below describes the significant fields shown in the display.

***Table 91: show ip rsvp fast-reroute Point-to-Multipoint Field Descriptions***

| Field | Description |
|---|---|
| Protected LSP | LSP being protected and the tunnel ID. |
| Protected Sub-LSP src_lspid[subid]->dst_tunid | The source and destination address of the sub-LSP being protected. The P2MP ID is appended to the source address. The tunnel ID is appended to the destination address. |

The following example displays information about fast reroutable primary tunnels and their corresponding backup tunnels that provide protection for Cisco IOS Release 15.0(1)M and later releases.

```
Rrouter# show ip rsvp fast-reroute filter session-type all

Session Type 7 (te-p2p-lsp)
P2P                       Protect BW         Backup
Protected LSP             I/F     BPS:Type   Tunnel:Label  State  Level   Type
-------------             ------- --------   ------------- ------ -----   ------
p2mp-2_t12                Se3/0   500K:G     Tu700:0       Ready  any-unl Nhop
p2mp-2_t13                Se3/0   500K:G     Tu700:0       Ready  any-unl Nhop
Session Type 13 (te-p2mp-lsp)
P2MP
*Protected Sub-LSP                         Protect BW         Backup
src_lspid[subid]->dst_tunid                I/F     BPS:Type   Tunnel:Label  State
---------------------------                ------- --------   ------------- ------
10.2.0.1_12[1]->10.1.0.1_1                 Se5/0   1M:G       None          None
10.2.0.1_12[3]->10.2.3.3_1                 Se3/0   1M:G       Tu700:16      Ready
10.2.0.1_12[5]->10.3.0.1_1                 Se3/0   1M:G       Tu700:16      Ready
10.2.0.1_12[6]->10.3.4.3_1                 Se3/0   1M:G       Tu700:16      Ready
10.2.0.1_12[8]->10.2.5.3_1                 Se6/0   1M:G       Tu100:17      Ready
```

## Related Commands

| Command | Description |
|---|---|
| **mpls traffic-eng auto-tunnel primary config** | Enables IP processing without an explicit address. |
| **mpls traffic-eng auto-tunnel primary config mpls ip** | Enables LDP on primary autotunnels. |
| **mpls traffic-eng auto-tunnel primary onehop** | Automatically creates primary tunnels to all next hops. |
| **mpls traffic-eng auto-tunnel primary timers** | Configures how many seconds after a failure primary autotunnels are removed. |
| **mpls traffic-eng auto-tunnel primary tunnel-num** | Configures the range of tunnel interface numbers for primary autotunnels. |

# show ip rsvp fast-reroute bw-protect

To display information about whether backup bandwidth protection is enabled and the status of backup tunnels that may be used to provide that protection, use the **showiprsvpfast-reroutebw-protect** command in user EXEC or privileged EXEC mode.

**show ip rsvp fast-reroute bw-protect [detail]** [**filter** [**session-type** {*session-type-number*| **all**}] [**destination** *ip-address*| *hostname*] [**dst-port** *port-number*] [**source** *ip-address*| *hostname*] [**src-port** *port-number*]]

## Syntax Description

| | |
|---|---|
| **detail** | (Optional) Specifies additional receiver information. |
| **filter** | (Optional) Specifies a subset of the receivers to display . |
| **session-type** *session-type-number* | (Optional) Specifies the type of Resource Reservation Protocol (RSVP) sessions to display. Valid values are:<br>• **1** for IPv4 sessions<br>• **7** for IPv4 point-to-point traffic engineering (TE) label switched path (LSP) tunnel sessions<br>• **13** for IPv4 point-to-multipoint TE LSP tunnel sessions |
| **all** | (Optional) Specifies all types of RSVP sessions. |
| **destination** *ip-address* | (Optional) Specifies the destination IP address of the receiver. |
| *hostname* | (Optional) Specifies the hostname of the receiver. |
| **dst-port** *port-number* | (Optional) Specifies the destination port number. Valid destination port numbers must be in the range from 0 to 65535. |
| **source** *ip-address* | (Optional) Specifies the source IP address of the receiver. |
| **src-port** *port-number* | (Optional) Specifies the source port number. Valid source port numbers must be in the range from 0 to 65535. |

## Command Default

The backup bandwidth protection and backup tunnel status information is not displayed.

**Command Modes** User EXEC (>) Privileged EXEC (#)

**Command History**

| Release | Modification |
|---|---|
| 12.0(29)S | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |
| 12.2(33)SRE | This command was modified. The **session-type** keyword was added to display specific types of tunnels. The output was modified to display Multiprotocol Label Switching (MPLS) traffic engineering (TE) point-to-multipoint (P2MP) information. |

**Examples** The following is sample output from the **showiprsvpfast-reroutebw-protect** command:

```
Router# show ip rsvp fast-reroute bw-protect

Primary          Protect  BW         Backup
Tunnel           I/F      BPS:Type   Tunnel:Label  State   BW-P    Type
--------------   -------  --------   ----------    -----   ----    ----
PRAB-72-5_t500   PO2/0    500K:S     Tu501:19      Ready   ON      Nhop
PRAB-72-5_t601   PO2/0    103K:S     Tu501:20      Ready   OFF     Nhop
PRAB-72-5_t602   PO2/0    70K:S      Tu501:21      Ready   ON      Nhop
PRAB-72-5_t603   PO2/0    99K:S      Tu501:22      Ready   ON      Nhop
PRAB-72-5_t604   PO2/0    100K:S     Tu501:23      Ready   OFF     Nhop
PRAB-72-5_t605   PO2/0    101K:S     Tu501:24      Ready   OFF     Nhop
```

The table below describes the significant fields shown in the display.

***Table 92: show ip rsvp fast-reroute bw-protect Field Descriptions***

| Field | Description |
|---|---|
| Primary Tunnel | Identification of the tunnel being protected. |
| Protect I/F | Interface name. |
| BW BPS:Type | Bandwidth, in bits per second, and type of bandwidth. Possible values are the following:<br>• S--Subpool<br>• G--Global pool |
| Backup Tunnel:Label | Identification of the backup tunnel. |

| Field | Description |
|---|---|
| State | Status of backup tunnel. Valid values are the following:<br>• Ready--Data is passing through the primary tunnel, but the backup tunnel is ready to take over if the primary tunnel goes down.<br>• Active--The primary tunnel is down, so the backup tunnel is used for traffic.<br>• None--There is no backup tunnel. |
| BW-P | Status of backup bandwidth protection. Possible values are ON and OFF. |
| Type | Type of backup tunnel. Possible values arethe following:<br>• Nhop--Next hop<br>• NNHOP--Next-next hop |

The following example shows fast reroutable primary tunnels and their corresponding backup tunnels that provide protection. The information is organized by point-to-point (P2P) labe switched paths (LSPs) and P2MP sub-LSPs. The following example shows that Tunnel 22 has six sub-LSPs, three that are protected on Ethernet interface 0/0, and three that are not protected on Ethernet interface 0/1:

```
Router# show ip rsvp fast-reroute bw-protect

P2P                         Protect BW         Backup
Protected LSP               I/F     BPS:Type   Tunnel:Label  State  BW-P    Type
-------------               ------- --------   ------------- ------ -----   ------
R201_t1                     Et0/1   500K:G     Tu777:16      Ready  ON      Nhop
P2MP
Protected Sub-LSP                           Protect BW         Backup
src_lspid[subid]->dst_tunid                 I/F     BPS:Type   Tunnel:Label  BW-P
--------------------------                  ------- --------   ------------- ------
10.1.1.201_1[1]->10.1.1.203_22                Et0/0   500K:G     Tu666:20      ON
10.1.1.201_1[2]->10.1.1.206_22                Et0/0   500K:G     Tu666:20      ON
10.1.1.201_1[3]->10.1.1.213_22                Et0/0   500K:G     Tu666:20      ON
10.1.1.201_1[4]->10.1.1.214_22                Et0/1   500K:G     None          None
10.1.1.201_1[5]->10.1.1.216_22                Et0/1   500K:G     None          None
10.1.1.201_1[6]->10.1.1.217_22                Et0/1   500K:G     None          None
```

The table below describes the significant fields shown in the display.

***Table 93: show ip rsvp fast-reroute bw-protect Point-to-Multipoint Field Descriptions***

| Field | Description |
|---|---|
| Protected LSP | LSP being protected and the tunnel ID. |

| Field | Description |
|---|---|
| Protected Sub-LSP src_lspid[subid]->dst_tunid | The source and destination address of the sub-LSP being protected. The P2MP ID is appended to the source address. The tunnel ID is appended to the destination address. |

## Related Commands

| Command | Description |
|---|---|
| **tunnel mpls traffic-eng fast-reroute bw-protect** | Enables an MPLS TE tunnel to use an established backup tunnel in the event of a link or node failure. |

# show ip rsvp fast-reroute detail

To display specific information for Resource Reservation Protocol (RSVP) categories, use the **showiprsvpfast-reroutedetail**command in user EXEC or privileged EXEC mode.

**show ip rsvp fast-reroute detail** [**filter** [**session-type** {*session-type-number*| **all**}] [**destination** *ip-address*| *hostname*] [**dst-port** *port-number*] [**source** *ip-address*| *hostname*] [**src-port** *port-number*]]

## Syntax Description

| | |
|---|---|
| **filter** | (Optional) Specifies a subset of the receivers to display . |
| **session-type** *session-type-number* | (Optional) Specifies the type of RSVP sessions to display. Valid values are:<br>• **1** for IPv4 sessions<br>• **7** for IPv4 point-to-point (P2P) traffic engineering (TE) label switched path (LSP) tunnel sessions<br>• **13** for IPv4 point-to-multipoint (P2MP) TE LSP tunnel sessions. |
| **all** | (Optional) Specifies all types of RSVP sessions. |
| **destination** *ip-address* | (Optional) Specifies the destination IP address of the receiver. |
| *hostname* | (Optional) Specifies the hostname of the receiver. |
| **dst-port** *port-number* | (Optional) Specifies the destination port number. Valid destination port numbers must be in the range from 0 to 65535. |
| **source** *ip-address* | (Optional) Specifies the source IP address of the receiver. |
| **src-port** *port-number* | (Optional) Specifies the source port number. Valid source port numbers must be in the range from 0 to 65535. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(24)S | This command was introduced. |
| 12.0(29)S | Bandwidth Prot desired was added in the Flag field of the command output. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |
| 12.2(33)SRE | This command was modified. The **session-type** keyword was added to display specific types of tunnels. The output was modified to display MPLS TE P2MP information. |

## Examples

The following is sample output from the **showiprsvpfast-reroutedetail** command:

```
Router# show ip rsvp fast-reroute detail

PATH:
  Tun Dest:   10.0.0.7  Tun ID: 500  Ext Tun ID: 10.0.0.5
  Tun Sender: 10.0.0.5  LSP ID: 8
  Path refreshes:
    sent:     to   NHOP 10.5.6.6 on POS2/0
  Session Attr:
    Setup Prio: 7, Holding Prio: 7
    Flags: Local Prot desired, Label Recording, SE Style, Bandwidth Prot desired
    Session Name: PRAB-72-5_t500
  ERO: (incoming)
    10.0.0.5 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.5.6 (Strict IPv4 Prefix, 8 bytes, /32)
    10.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
  ERO: (outgoing)
    10.5.6.6 (Strict IPv4 Prefix, 8 bytes, /32)
    10.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
  Traffic params - Rate: 500K bits/sec, Max. burst: 1K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
  Fast-Reroute Backup info:
    Inbound  FRR: Not active
    Outbound FRR: Ready -- backup tunnel selected
      Backup Tunnel: Tu501      (label 19)
      Bkup Sender Template:
        Tun Sender: 10.5.6.5  LSP ID: 8
      Bkup FilerSpec:
        Tun Sender: 10.5.6.5, LSP ID: 8
  Path ID handle: 04000405.
  Incoming policy: Accepted. Policy source(s): MPLS/TE
  Status: Proxied
  Output on POS2/0. Policy status: Forwarding. Handle: 02000406
```

The table below describes the significant fields shown in the display.

***Table 94: show ip rsvp fast-reroute detail Field Descriptions***

| Field | Description |
|---|---|
| Tun Dest | IP address of the receiver. |

| Field | Description |
|---|---|
| Tun ID | Tunnel identification number. |
| Ext Tun ID | Extended tunnel identification number. |
| Tun Sender | IP address of the sender. |
| LSP ID | Label switched path identification number. |
| Setup Prio | Setup priority. |
| Holding Prio | Holding priority. |
| Flags | Backup bandwidth protection has been configured for the label switched path. |
| Session Name | Name of the session. |
| ERO (incoming) | EXPLICIT_ROUTE object of incoming path messages. |
| ERO (outgoing) | EXPLICIT_ROUTE object of outgoing path messages. |
| Traffic params Rate | Average rate, in bits per second. |
| Max. burst | Maximum burst size, in bytes. |
| Min Policed Unit | Minimum policed units, in bytes. |
| Max Pkt Size | Maximum packet size, in bytes. |
| Inbound FRR | Status of inbound Fast Reroute (FRR) backup tunnel. If this node is downstream from a rerouted LSP (for example, at a merge point for this LSP), the state is Active. |

| Field | Description |
|---|---|
| Outbound FRR | Status of outbound FRR backup tunnel. If this node is a point of local repair (PLR) for an LSP, there are three possible states:<br>• Active--This LSP is actively using its backup tunnel, presumably because there has been a downstream failure.<br>• No Backup--This LSP does not have local (Fast Reroute) protection. No backup tunnel has been selected for it to use in case of a failure.<br>• Ready--This LSP is ready to use a backup tunnel in case of a downstream link or node failure. A backup tunnel has been selected for it to use. |
| Backup Tunnel | If the Outbound FRR state is Ready or Active, this field indicates the following:<br>• Which backup tunnel has been selected for this LSP to use in case of a failure.<br>• The inbound label that will be prepended to the LSP's data packets for acceptance at the backup tunnel tail (the merge point). |
| Bkup Sender Template | If the Outbound FRR state is Ready or Active, SENDER_TEMPLATE and FILTERSPEC objects are shown. These objects will be used in RSVP messages sent by the backup tunnel if or when the LSP starts actively using the backup tunnel. They differ from the original (prefailure) objects only in that the node (the PLR) substitutes its own IP address for that of the original sender. For example, path and pathTear messages will contain the new SENDER_TEMPLATE. Resv and resvTear messages will contain the new FILTERSPEC object. If this LSP begins actively using the backup tunnel, the display changes. |

| Field | Description |
|---|---|
| Bkup FilerSpec | If the Outbound FRR state is Ready or Active, SENDER_TEMPLATE and FILTERSPEC objects are shown. These objects will be used in RSVP messages sent by the backup tunnel if or when the LSP starts actively using the backup tunnel. They differ from the original (prefailure) objects only in that the node (the PLR) substitutes its own IP address for that of the original sender. For example, path and pathTear messages will contain the new SENDER_TEMPLATE. Resv and resvTear messages will contain the new FILTERSPEC object. If this LSP begins actively using the backup tunnel, the display changes. |
| Path ID handle | Protection Switch Byte (PSB) identifier. |
| Incoming policy | Policy decision of the LSP. If RSVP policy was not granted for the incoming path message for the tunnel, the LSP does not come up. Accepted is displayed. |
| Policy source(s) | For FRR LSPs, this value always is MPLS/TE for the policy source. |
| Status | For FRR LSPs, valid values are as follows:<br>• Proxied--Headend routers.<br>• Proxied Terminated--Tailend routers.<br>For midpoint routers, the field always is blank. |

The following example shows P2MP data:

```
Router# show ip rsvp fast-reroute detail

PATH:
  P2MP ID: 22  Tun ID: 22  Ext Tun ID: 10.1.1.201
  Tun Sender: 10.1.1.201  LSP ID: 1  SubGroup Orig: 10.1.1.201
  SubGroup ID: 2
  S2L Destination : 10.1.1.206
  Path refreshes:
    sent:     to   NHOP 10.0.0.205 on Ethernet0/0
  Session Attr:
    Setup Prio: 7, Holding Prio: 7
    Flags: (0xF) Local Prot desired, Label Recording, SE Style, Bandwidth Prot desired
    Session Name: R201_t22
  ERO: (incoming)
    10.1.1.201 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.0.201 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.0.206 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.1.206 (Strict IPv4 Prefix, 8 bytes, /32)
  ERO: (outgoing)
    10.0.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
```

```
  10.1.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
  10.1.0.206 (Strict IPv4 Prefix, 8 bytes, /32)
  1o.1.1.206 (Strict IPv4 Prefix, 8 bytes, /32)
Traffic params - Rate: 500K bits/sec, Max. burst: 1K bytes
  Min Policed Unit: 1 bytes, Max Pkt Size 2147483647 bytes
Fast-Reroute Backup info:
  Inbound  FRR: Not active
  Outbound FRR: Ready -- backup tunnel selected
    Backup Tunnel: Tu666      (label 20)
    Bkup Sender Template:
      Tun Sender: 10.0.2.201  LSP ID: 1  SubGroup Orig: 10.1.1.201
      SubGroup ID: 2
    Bkup FilerSpec:
      Tun Sender: 10.0.2.201, LSP ID: 1, SubGroup Orig: 10.1.1.201
      SubGroup ID: 2
Path ID handle: 01000417.
Incoming policy: Accepted. Policy source(s): MPLS/TE
Status: Proxied
```

The table below describes the significant fields shown in the display.

***Table 95: show ip rsvp fast-reroute detail P2MP Field Descriptions***

| Field | Description |
|---|---|
| P2MP ID | A 32-bit number that identifies the set of destinations of the P2MP tunnel. |
| Tun ID | Tunnel identification number. |
| Ext Tun ID | Extended tunnel identification number. |
| Tun Sender | IP address of the sender. |
| LSP ID | Label switched path identification number. |
| SubGroup Orig | LSP headend router ID address. |
| SubGroup ID | An incremental number assigned to each sub-LSP signaled from the headend router. |
| S2L Destination | LSP tailend router ID address. |

## Related Commands

| Command | Description |
|---|---|
| **mpls traffic-eng fast-reroute backup-prot-preemption** | Changes the backup protection preemption algorithm to minimize the amount of bandwidth that is wasted. |

# show ip rsvp hello

To display hello status and statistics for Fast Reroute, reroute (hello state timer), and graceful restart, use the **showiprsvphello** command in user EXEC or privileged EXEC mode.

**show ip rsvp hello**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(22)S | This command was introduced. |
| 12.0(29)S | The command output was modified to include graceful restart, reroute (hello state timer), and Fast Reroute information. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(33)SRA | The command output was modified to show whether graceful restart is configured and full mode was added. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SRC | The command output was modified to include Bidirectional Forwarding Detection (BFD) protocol information. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |

## Examples

The following is sample output from the **showiprsvphello** command:

```
Router# show ip rsvp hello
Hello:
 RSVP Hello for Fast-Reroute/Reroute: Enabled
  Statistics: Disabled
 BFD for Fast-Reroute/Reroute: Enabled
 RSVP Hello for Graceful Restart: Disabled
```

The table below describes the significant fields shown in the display. The fields describe the processes for which hello is enabled or disabled.

*Table 96: show ip rsvp hello Field Descriptions*

| Field | Description |
|---|---|
| RSVP Hello for Fast-Reroute/Reroute | Status of Fast-Reroute/Reroute:<br>• Disabled--Fast reroute and reroute (hello for state timer) are not activated (disabled).<br>• Enabled--Fast reroute and reroute (hello for state timer) are activated (enabled). |
| Statistics | Status of hello statistics:<br>• Disabled--Hello statistics are not configured.<br>• Enabled--Statistics are configured. Hello packets are time-stamped when they arrive in the hello input queue for the purpose of recording the time required until they are processed.<br>• Shutdown--Hello statistics are configured but not operational. The input queue is too long (that is, more than 10,000 packets are queued). |
| BFD for Fast-Reroute/Reroute | Status of BFD for Fast-Reroute/Reroute:<br>• Disabled--BFD is not configured.<br>• Enabled--BFD is configured. |
| Graceful Restart | Restart capability:<br>• Disabled--Restart capability is not activated.<br>• Enabled--Restart capability is activated for a router (full mode) or its neighbor (help-neighbor). |

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello (configuration)** | Enables hello globally on the router. |
| **ip rsvp signalling hello statistics** | Enables hello statistics on the router. |
| **show ip rsvp hello statistics** | Displays how long hello packets have been in the hello input queue. |

# show ip rsvp hello client lsp detail

To display detailed information about Resource Reservation Protocol (RSVP) traffic engineering (TE) client hellos for label-switched paths (LSPs), use the**showiprsvphelloclientlspdetail**command in user EXEC or privileged EXEC mode.

**show ip rsvp hello client lsp detail** [**filter** [**destination** *hostname*]]

## Syntax Description

| | |
|---|---|
| **filter** | (Optional) Specifies filters to limit the display of output. |
| **destination** | (Optional) Displays the filters configured on the destination (tunnel tail). |
| *hostname* | (Optional) IP address or name of destination (tunnel tail). |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(33)S | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

Use the **showiprsvphelloclientlspdetail**command to display information about the LSPs, including IP addresses and their types.

## Examples

The following is sample output from the **showiprsvphelloclientlspdetail**command:

```
Router# show ip rsvp hello client lsp detail
Hello Client LSPs (all lsp tree)
  Tun Dest: 10.0.1.1  Tun ID: 14  Ext Tun ID: 172.16.1.1
  Tun Sender: 172.16.1.1  LSP ID: 31
    Lsp flags: 0x32
    Lsp GR DN nbr: 192.168.1.1
    Lsp RR DN nbr: 10.0.0.3 HST
```

The table below describes the significant fields shown in the display.

*Table 97: show ip rsvp hello client lsp detail Field Descriptions*

| Field | Description |
|---|---|
| Hello Client LSPs | Current clients include graceful restart (GR), reroute (RR) (hello state timer), and fast reroute (FRR). |
| Tun Dest | IP address of the destination tunnel. |
| Tun ID | Identification number of the tunnel. |
| Ext Tun ID | Extended identification number of the tunnel. Usually, this is the same as the source address. |
| Tun Sender | IP address of the tunnel sender. |
| LSP ID | Identification number of the LSP. |
| Lsp flags | LSP database information. |
| Lsp GR DN nbr | IP address of the LSP graceful restart downstream neighbor. |
| Lsp RR DN nbr | IP address of the LSP reroute downstream neighbor; HST--hello state timer. |

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp hello** | Displays hello status and statistics for fast reroute, reroute (hello state timer), and graceful restart. |

# show ip rsvp hello client lsp summary through show lane qos database


- show ip rsvp hello client lsp summary, page 1295
- show ip rsvp hello client nbr detail, page 1297
- show ip rsvp hello client neighbor detail, page 1300
- show ip rsvp hello client neighbor summary, page 1303
- show ip rsvp hello graceful-restart, page 1305
- show ip rsvp hello instance detail, page 1308
- show ip rsvp hello instance summary, page 1312
- show ip rsvp hello statistics, page 1315
- show ip rsvp high-availability counters, page 1317
- show ip rsvp high-availability database, page 1323
- show ip rsvp high-availability summary, page 1342
- show ip rsvp host, page 1347
- show ip rsvp host vrf, page 1351
- show ip rsvp ingress, page 1353
- show ip rsvp installed, page 1355
- show ip rsvp interface, page 1366
- show ip rsvp interface detail, page 1384
- show ip rsvp listeners, page 1387
- show ip rsvp neighbor, page 1390
- show ip rsvp p2mp counters, page 1394
- show ip rsvp policy, page 1396
- show ip rsvp policy cops, page 1398
- show ip rsvp policy identity, page 1399

- show ip rsvp policy local, page 1402
- show ip rsvp policy vrf, page 1409
- show ip rsvp precedence, page 1412
- show ip rsvp request, page 1414
- show ip rsvp reservation, page 1422
- show ip rsvp sbm, page 1433
- show ip rsvp sender, page 1436
- show ip rsvp signalling, page 1467
- show ip rsvp signalling blockade, page 1470
- show ip rsvp signalling fast-local-repair, page 1474
- show ip rsvp signalling rate-limit, page 1480
- show ip rsvp signalling refresh, page 1482
- show ip rsvp snooping, page 1484
- show ip rsvp tos, page 1485
- show ip rsvp transport, page 1487
- show ip rsvp transport sender, page 1490
- show ip rtp header-compression, page 1493
- show ip tcp header-compression, page 1496
- show ip vrf, page 1500
- show lane qos database, page 1504

# show ip rsvp hello client lsp summary

To display summary information about Resource Reservation Protocol (RSVP) traffic engineering (TE) client hellos for label-switched paths (LSPs), use the**showiprsvphelloclientlspsummary**command in user EXEC or privileged EXEC mode.

**show ip rsvp hello client lsp summary**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SB | This command was introduced. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

Use the **showiprsvphelloclientlspsummary**command to display information about the LSPs, including IP addresses and identification numbers.

## Examples

The following is sample output from the **showiprsvphelloclientlspsummary**command:

```
Router# show ip rsvp hello client lsp summary
Local           Remote          tun_id  lsp_id  FLAGS
10.1.1.1        172.16.1.1        14      31      0x32
```

The table below describes the significant fields shown in the display.

***Table 98: show ip rsvp hello client lsp summary Field Descriptions***

| Field | Description |
|---|---|
| Local | IP address of the tunnel sender. |
| Remote | IP address of the tunnel destination. |
| tun_id | Identification number of the tunnel. |
| lsp_id | Identification number of the LSP. |
| FLAGS | Database information. |

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp hello** | Displays hello status and statistics for fast reroute, reroute (hello state timer), and graceful restart. |

# show ip rsvp hello client nbr detail

To display detailed information about Resource Reservation Protocol (RSVP) traffic engineering (TE) client hellos for neighbors, use the**showiprsvphelloclientnbrdetail**command in user EXEC or privileged EXEC mode.

**show ip rsvp hello client nbr detail** [**filter** [**destination** *hostname*]]

## Syntax Description

| | |
|---|---|
| **filter** | (Optional) Specifies filters to limit the display of output. |
| **destination** | (Optional) Displays the filters configured on the destination (tunnel tail). |
| *hostname* | (Optional) IP address or name of destination (tunnel tail). |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(33)S | This command was introduced. |
| 12.2(33)SRC | This command was integrated in Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

Use the **showiprsvphelloclientnbrdetail**command to display information about the neighbors (nbr).

## Examples

The following is sample output from the **showiprsvphelloclientnbrdetail**command:

```
Router# show ip rsvp hello client nbr detail
Hello Client Neighbors
  Remote addr 10.0.0.1,  Local addr  10.0.0.3
    Nbr State: Normal    Type: Reroute
    Nbr Hello State: Up
    LSPs protecting: 1
    I/F: Et1/3
  Remote addr 172.16.1.1,  Local addr  192.168.1.1
    Nbr State: Normal    Type: Graceful Restart
    Nbr Hello State: Lost
    LSPs protecting: 1
```

The table below describes the fields shown in the display

*Table 99: show ip rsvp hello client nbr detail Field Descriptions*

| Field | Description |
|---|---|
| Remote addr | IP address of the remote neighbor. For graceful restart, this is the neighbor router's ID; for fast reroute and hello state timer (reroute), this is one of the neighbor's interface addresses. |
| Local addr | IP address of the local neighbor. For graceful restart, this is the neighbor router's ID; for fast reroute and hello state timer (reroute), this is one of the neighbor's interface addresses. |
| Nbr state | State of the neighbor; values can be the following:<br>• Normal--Neighbor is functioning normally.<br>• Restarting--Neighbor is restarting.<br>• Recover Nodal--Neighbor is recovering from node failure.<br>• HST_GR_LOST--HST (hello state timer for reroute) is lost; waiting to see if GR (graceful restart) is also lost.<br>• WAIT PathTear--PathTear message is delayed to allow traffic in the pipeline to be transmitted. |
| Type | Type of client: graceful restart (GR), reroute RR (hello state timer), or fast reroute (FRR). |
| Nbr Hello State | State of hello instances for the neighbor. Values are as follows:<br>• Up--Node is communicating with its neighbor.<br>• Lost--Communication has been lost.<br>• Init--Communication is being established. |
| LSPs protecting | Number of LSPs being protected. |
| I/F | Interface name and number associated with the hello instance. |

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp hello** | Displays hello status and statistics for fast reroute, reroute (hello state timer), and graceful restart. |

| Command | Description |
|---|---|
| **show ip rsvp hello client neighbor summary** | Displays summary information about RSVP TE client hellos for neighbors. |

# show ip rsvp hello client neighbor detail

To display detailed information about Resource Reservation Protocol (RSVP) traffic engineering (TE) client hellos for neighbors, use the**showiprsvphelloclientneighbordetail**command in user EXEC or privileged EXEC mode.

**show ip rsvp hello client neighbor detail**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(29)S | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

Use the **showiprsvphelloclientneighbordetail**command to display information about the hello neighbors, including their state and type.

## Examples

The following is sample output from the **showiprsvphelloclientneighbordetail**command:

```
Router# show ip rsvp hello client neighbor detail
Hello Client Neighbors
  Remote addr 10.0.0.1,  Local addr  10.0.0.3
    Nbr State: Normal    Type: Reroute
    Nbr Hello State: Up
    LSPs protecting: 1
    I/F: Et1/3
  Remote addr 172.16.1.1,  Local addr  192.168.1.1
    Nbr State: Normal    Type: Graceful Restart
    Nbr Hello State: Lost
    LSPs protecting: 1
```

The table below describes the significant fields shown in the display. The fields provide information that uniquely identifies the neighbors. Clients can include graceful restart, reroute (hello state timer), and fast reroute.

*Table 100: show ip rsvp hello client neighbor detail Field Descriptions*

| Field | Description |
|---|---|
| Remote addr | IP address of the remote neighbor. For graceful restart, this is the neighbor router's ID; for fast reroute and hello state timer (reroute), this is one of the neighbor's interface addresses. |
| Local addr | IP address of the local neighbor. For graceful restart, this is the neighbor router's ID; for fast reroute and hello state timer (reroute), this is one of the neighbor's interface addresses. |
| Nbr State | State of the neighbor; values can be the following:<br>• Normal = neighbor is functioning normally.<br>• Restarting = neighbor is restarting.<br>• Recover Nodal = neighbor is recovering from node failure.<br>• HST_GR_LOST = HST (hello state timer for reroute) is lost; waiting to see if graceful restart (GR) is also lost.<br>• WAIT PathTear = PathTear message is delayed to allow traffic in the pipeline to be transmitted. |
| Type | Type of client; graceful restart, Reroute (hello state timer), or Fast Reroute. |
| Nbr Hello State | State of hellos for the neighbor. Values are as follows:<br>• Up--Node is communicating with its neighbor.<br>• Lost--Communication has been lost.<br>• Init--Communication is being established. |
| LSPs protecting | Number of LSPs being protected. |
| I/F | Interface name and number associated with the hello instance. |

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp hello** | Displays hello status and statistics for fast reroute, reroute (hello state timer), and graceful restart. |

# show ip rsvp hello client neighbor summary

To display summary information about Resource Reservation Protocol (RSVP) traffic engineering (TE) client hellos for neighbors, use the**showiprsvphelloclientneighborsummary**command in user EXEC or privileged EXEC mode.

**show ip rsvp hello client neighbor summary**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(29)S | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

Use the **showiprsvphelloclientneighborsummary**command to display information about the neighbors, including state, type, and hello instance status.

## Examples

The following is sample output from the**showiprsvphelloclientneighborsummary**command:

```
Router# show ip rsvp hello client neighbor summary
Local Remote Type NBR_STATE HI_STATE LSPs
10.0.0.1 10.0.0.3 RR Normal Up 1
172.16.1.1 192.168.1.1 GR Normal Lost 1
```

The table below describes the significant fields shown in the display.

***Table 101: show ip rsvp hello client neighbor summary Field Descriptions***

| Field | Description |
|---|---|
| Local | IP address of the tunnel sender. |
| Remote | IP address of the tunnel destination. |
| Type | Type of client; graceful restart (GR), reroute (RR (hello state timer)), or fast reroute (FRR). |

| Field | Description |
|---|---|
| NBR_STATE | State of the neighbor; values can be the following:<br>• Normal--Neighbor is functioning normally.<br>• Restarting--Neighbor is restarting.<br>• Recover Nodal--Neighbor is recovering from node failure.<br>• HST_GR_LOST--HST (hello state timer for reroute) is lost; waiting to see if graceful restart (GR) is also lost.<br>• WAIT PathTear--PathTear message is delayed to allow traffic in the pipeline to be transmitted. |
| HI_STATE | State of hello instances for the neighbor. Values are as follows:<br>• Up--Node is communicating with its neighbor.<br>• Lost--Communication has been lost.<br>• Init--Communication is being established. |
| LSPs | Number of LSPs going to or coming from the neighbor. |

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp hello** | Displays hello status and statistics for fast reroute, reroute (hello state timer), and graceful restart. |

# show ip rsvp hello graceful-restart

To display information about Resource Reservation Protocol (RSVP) traffic engineering (TE) graceful restart hellos, use the**showiprsvphellograceful-restart** command in user EXEC or privileged EXEC mode.

**show ip rsvp hello graceful-restart**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(29)S | This command was introduced. |
| 12.2(33)SRA | The command output was modified to show whether graceful restart is configured and full mode was added. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

Use the **showiprsvphellograceful-restart** command to display the status of graceful restart and related statistics.

## Examples

The following is sample output from the **showiprsvphellograceful-restart**command:

```
Router# show ip rsvp hello graceful-restart
Graceful Restart: Enabled (full mode)
  Refresh interval: 10000 msecs
  Refresh misses: 4
  DSCP: 0x30
  Advertised restart time: 30000 msecs
  Advertised recovery time: 120000 msecs
  Maximum wait for recovery: 3600000 msecs
```

The table below describes the significant fields shown in the display.

*Table 102: show ip rsvp hello graceful-restart Field Descriptions*

| Field | Description |
|---|---|
| Graceful Restart | Restart capability:<br>• Enabled--Restart capability is activated for a router (full mode) or its neighbor (help-neighbor).<br>• Disabled--Restart capability is not activated. |
| Refresh interval | Frequency in milliseconds (ms) with which a node sends a hello message to its neighbor. |
| Refresh misses | Number of missed hello messages that trigger a neighbor down event upon which stateful switchover (SSO) procedures are started. |
| DSCP | The differentiated services code point (DSCP) value in the IP header of the hello messages. |
| Advertised restart time | The time, in ms, that is required for the sender to restart the RSVP-TE component and exchange hello messages after a failure. |
| Advertised recovery time | The time, in ms, within which a recovering node wants its neighbor router to resynchronize the RSVP or Multiprotocol Label Switching (MPLS) forwarding state after SSO.<br>**Note** A zero value indicates that the RSVP or MPLS forwarding state is not preserved after SSO. |
| Maximum wait for recovery | The maximum amount of time, in ms, that the router waits for a neighbor to recover. |

## Related Commands

| Command | Description |
|---|---|
| **clear ip rsvp high-availability counters** | Clears (sets to zero) the RSVP-TE HA counters that are being maintained by an RP. |
| **ip rsvp signalling hello graceful-restart mode** | Enables RSVP-TE graceful restart support capability on an RP. |
| **ip rsvp signalling hello graceful-restart neighbor** | Enables RSVP-TE graceful restart support capability on a neighboring router. |

| Command | Description |
|---|---|
| **show ip rsvp hello** | Displays hello status and statistics for fast reroute, reroute (hello state timer), and graceful restart. |

# show ip rsvp hello instance detail

To display detailed information about a hello instance, use the **showiprsvphelloinstancedetail**command in user EXEC or privileged EXEC mode.

**show ip rsvp hello instance detail** [**filter destination** *ip-address*]

## Syntax Description

| | |
|---|---|
| **filter destination** *ip-address* | (Optional) IP address of the neighbor node. |

## Command Modes

User EXEC Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(22)S | This command was introduced. |
| 12.0(29)S | The command output was modified to include graceful restart, hello state timer (reroute), and fast reroute information. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

Use the **showiprsvphelloinstancedetail** command to display information about the processes (clients) currently configured.

## Examples

The following is sample output from the **showiprsvphelloinstancedetail** command:

```
Router# show ip rsvp hello instance detail
Neighbor 10.0.0.3  Source  10.0.0.2
    Type: Active    (sending requests)
    I/F:  Serial2/0
    State:   Up        (for 2d19h2d19h)
    Clients: ReRoute
    LSPs protecting: 1
    Missed acks: 4, IP DSCP: 0x30
    Refresh Interval (msec)
      Configured: 6000
      Statistics: (from 40722 samples)
        Min:      6000
        Max:      6064
        Average:  6000
        Waverage: 6000 (Weight = 0.8)
```

```
      Current:  6000
  Last sent Src_instance: 0xE617C847
  Last recv nbr's Src_instance: 0xFEC28E95
  Counters:
    Communication with neighbor lost:
      Num times:                    0
      Reasons:
        Missed acks:                0
        Bad Src_Inst received:      0
        Bad Dst_Inst received:      0
        I/F went down:              0
        Neighbor disabled Hello:    0
    Msgs Received:   55590
         Sent:       55854
         Suppressed: 521
Neighbor 10.0.0.8 Source  10.0.0.7
  Type: Passive   (responding to requests)
  I/F:  Serial2/1
  Last sent Src_instance: 0xF7A80A52
  Last recv nbr's Src_instance: 0xD2F1B7F7
  Counters:
    Msgs Received:   199442
         Sent:       199442
```

The table below describes the significant fields shown in the display.

***Table 103: show ip rsvp hello instance detail Field Descriptions***

| Field | Description |
|---|---|
| Neighbor | IP address of the adjacent node. |
| Source | IP address of the node that is sending the hello message. |
| Type | Values are Active (node is sending a request) and Passive (node is responding to a request). |
| I/F | Interface from which hellos are sent for this instance. Any means that the hellos can be sent out any interface. |
| State | Status of communication. Values are as follows:<br>• Up--Node is communicating with its neighbor.<br>• Lost--Communication has been lost.<br>• Init--Communication is being established. |
| Clients | Clients that created this hello instance; they include graceful restart, ReRoute (hello state timer), and Fast Reroute. |
| LSPs protecting | Number of LSPs that are being protected by this hello instance. |
| Missed acks | Number of times that communication was lost due to missed acknowledgments (ACKs). |

| Field | Description |
|---|---|
| IP DSCP | IP differentiated services code point (DSCP) value used in the hello IP header. |
| Refresh Interval (msec) | The frequency (in milliseconds) with which a node generates a hello message containing a Hello Request object for each neighbor whose status is being tracked. |
| Configured | Configured refresh interval. |
| Statistics | Refresh interval statistics from a specified number of samples (packets). |
| Min | Minimum refresh interval. |
| Max | Maximum refresh interval. |
| Average | Average refresh interval. |
| Waverage | Weighted average refresh interval. |
| Current | Current refresh interval. |
| Last sent Src_instance | The last source instance sent to a neighbor. |
| Last recv nbr's Src_instance | The last source instance field value received from a neighbor.<br>(0 means none received.) |
| Counters | Incremental information relating to communication with a neighbor. |
| Num times | Total number of times that communication with a neighbor was lost. |
| Reasons | Subsequent fields designate why communication with a neighbor was lost. |
| Missed acks | Number of times that communication was lost due to missed ACKs. |
| Bad Src_Inst received | Number of times that communication was lost due to bad source instance fields. |
| Bad Dst_Inst received | Number of times that communication was lost due to bad destination instance fields. |
| I/F went down | Number of times that the interface became unoperational. |

| Field | Description |
|---|---|
| Neighbor disabled Hello | Number of times that a neighbor disabled hello messages. |
| Msgs Received | Number of messages that were received. |
| Sent | Number of messages that were sent. |
| Suppressed | Number of messages that were suppressed due to optimization. |

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello (configuration)** | Enables hello globally on the router. |
| **ip rsvp signalling hello statistics** | Enables hello statistics on the router. |
| **show ip rsvp hello** | Displays hello status and statistics for Fast reroute, reroute (hello state timer), and graceful restart. |
| **show ip rsvp hello instance summary** | Displays summary information about a hello instance. |

# show ip rsvp hello instance summary

To display summary information about a hello instance, use the **showiprsvphelloinstancesummary** command in user EXEC or privileged EXEC mode.

**show ip rsvp hello instance summary**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(22)S | This command was introduced. |
| 12.0(29)S | The command output was modified to include graceful restart, reroute (hello state timer), and fast reroute information. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Examples

The following is sample output from the **showiprsvphelloinstancesummary** command:

```
Router# show ip rsvp hello instance summary
Active Instances:
  Client  Neighbor        I/F        State      LostCnt  LSPs Interval
  RR      10.0.0.3        Se2/0      Up               0     1 6000
  GR      10.1.1.1        Any        Up              13     1 10000
  GR      10.1.1.5        Any        Lost             0     1 10000
  GR      10.2.2.1        Any        Init             1     0 5000
Passive Instances:
  Neighbor        I/F
  10.0.0.1        Se2/1
Active = Actively tracking neighbor state on behalf of clients:
         RR = ReRoute, FRR = Fast ReRoute, or GR = Graceful Restart
Passive = Responding to hello requests from neighbor
```

The table below describes the significant fields shown in the display.

***Table 104: show ip rsvp hello instance summary Field Descriptions***

| Field | Description |
|---|---|
| Active Instances | Active nodes that are sending hello requests. |

| Field | Description |
|---|---|
| Client | Clients on behalf of which hellos are sent; they include GR (graceful restart), RR (reroute = hello state timer), and FRR (Fast Reroute). |
| Neighbor | IP address of the adjacent node. For graceful restart, this is the neighbor router's ID; for Fast Reroute and hello state timer (reroute), this is one of the neighbor's interface addresses. |
| I/F | Interface from which hellos are sent for this instance. Any means that the hellos can be sent out any interface. |
| State | Status of communication. Values are as follows:<br>• Up--Node is communicating with its neighbor.<br>• Lost--Communication has been lost.<br>• Init--Communication is being established. |
| LostCnt | Number of times that communication was lost with the neighbor. |
| LSPs | Number of label-switched paths (LSPs) protected by this hello instance. |
| Interval | Hello refresh interval in milliseconds. |
| Passive Instances | Passive nodes that are responding to hello requests. |
| Neighbor | IP address of adjacent node. For graceful restart, this is the neighbor router's ID; for Fast Reroute and hello state timer (reroute), this is one of the neighbor's interface addresses. |
| I/F | Interface from which hellos are sent for this instance. Any means that the hellos can be sent out any interface. |

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling hello (configuration)** | Enables hello globally on the router. |
| **ip rsvp signalling hello statistics** | Enables hello statistics on the router. |

| Command | Description |
|---|---|
| **show ip rsvp hello** | Displays hello status and statistics for fast reroute, reroute (hello state timer), and graceful restart. |
| **show ip rsvp hello instance detail** | Displays detailed information about a hello instance. |

# show ip rsvp hello statistics

To display how long hello packets have been in the Hello input queue, use the **showiprsvphellostatistics**command in privileged EXEC mode.

**show ip rsvp hello statistics**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Information about how long hello packets have been in the Hello input queue is not displayed.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(22)S | This command was introduced. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T |

## Usage Guidelines

You can use this command to determine if the Hello refresh interval is too small. If the interval is too small, communication may falsely be declared as lost.

## Examples

The following is sample output from the **showiprsvphellostatistics** command:

```
Router# show ip rsvp hello statistics

Status: Enabled
  Packet arrival queue:
    Wait times (msec)
      Current:0
      Average:0
      Weighted Average:0 (weight = 0.8)
      Max:4
    Current length: 0 (max:500)
  Number of samples taken: 2398525
```

The table below describes the significant fields shown in the display.

*Table 105: show ip rsvp hello statistics Field Descriptions*

| Field | Description |
|---|---|
| Status | Indicator of whether Hello has been enabled globally on the router. |
| Current | Amount of time, in milliseconds, that the current hello packet has been in the Hello input queue. |
| Average | Average amount of time, in milliseconds, that hello packets are in the Hello input queue. |
| Max | Maximum amount of time, in milliseconds, that hello packets have been in the Hello input queue. |
| Current length | Current amount of time, in milliseconds, that hello packets have been in the Hello input queue. |
| Number of samples taken | Number of packets for which these statistics were compiled. |

## Related Commands

| Command | Description |
|---|---|
| **clear ip rsvp hello instance statistics** | Clears Hello statistics for an instance. |
| **clear ip rsvp hello statistics** | Globally clears Hello statistics. |
| **ip rsvp signalling hello refresh interval** | Configures the Hello request interval. |
| **ip rsvp signalling hello statistics** | Enables Hello statistics on the router. |

# show ip rsvp high-availability counters

To display all Resource Reservation Protocol (RSVP) traffic engineering (TE) high availability (HA) counters that are being maintained by a Route Processor (RP), use the **show ip rsvp high-availability counters** command in user EXEC or privileged EXEC mode.

**show ip rsvp high-availability counters**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC (>)

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was introduced. |
| 12.2(33)SRB | Support for In-Service Software Upgrade (ISSU) was added. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 15.0(1)S | This command was modified. The output was updated to display information for point-to-point (P2P) and point-to-multipoint traffic engineering (P2MP) counters. |
| 15.2(2)S | This command was modified. The output was enhanced to show checkpoint information for MPLS traffic engineering autotunnel and automesh stateful switchover (SSO) tunnels. |
| Cisco IOS XE Release 3.6S | This command was modified. The output was enhanced to show checkpoint information for MPLS traffic engineering autotunnel and automesh stateful switchover (SSO) tunnels. |

## Usage Guidelines

Use the **show ip rsvp high-availability counters** command to display the HA counters, which include state, ISSU, checkpoint messages, resource failures, and errors.

The command output differs depending on whether the RP is active or standby. (See the “Examples” section for more information.)

Use the **clear ip rsvp high-availability counters** command to clear all counters.

## Examples

The following is sample output from the **show ip rsvp high-availability counters** command on the active RP:

```
Router# show ip rsvp high-availability counters

State: Active
P2P LSPs for which recovery:
  Attempted: 1
  Succeeded: 1
  Failed:    0
P2MP subLSPs for which recovery:
  Attempted: 2
  Succeeded: 2
  Failed:    0
Bulk sync
  initiated: 1
Send timer
  started: 2
Checkpoint Messages (Items) Sent
  Succeeded:      2  (8)
    Acks accepted:2  (8)
    Acks ignored:     (0)
    Nacks:        0  (0)
  Failed:         0  (0)
  Buffer alloc:   2
  Buffer freed:   4
ISSU:
  Checkpoint Messages Transformed:
    On Send:
      Succeeded:         2
      Failed:            0
      Transformations:   0
    On Recv:
      Succeeded:         2
      Failed:            0
      Transformations:   0
  Negotiation:
    Started:              2
    Finished:             2
    Failed to Start:      0
    Messages:
      Sent:
        Send succeeded:   14
        Send failed:      0
        Buffer allocated:        14
        Buffer freed:            0
        Buffer alloc failed:     0
      Received:
        Succeeded:        10
        Failed:           0
        Buffer freed:     10
  Init:
    Succeeded:            1
    Failed:               0
  Session Registration:
    Succeeded:            1
    Failed:               0
  Session Unregistration:
    Succeeded:            1
    Failed:               0
Errors:
  None
Historical: (When Active was Standby)
Checkpoint Messages (Items) Received
  Valid:        2  (11)
  Invalid:      0  (0)
Buffer freed: 2
```

The table below describes the significant fields shown in the display.

*Table 106: show ip rsvp high-availability counters—Active RP Field Descriptions*

| Field | Description |
|---|---|
| State | The RP state:<br>• Active—Active RP. |
| Bulk sync | The number of requests made by the standby RP to the active RP to resend all write database entries:<br>• Initiated—The number of bulk sync operations initiated by the standby RP since reboot. |
| Send timer | The write database timer. |
| Checkpoint Messages (Items) Sent | The details of the bundle messages or items sent since booting. |
| Succeeded | The number of bundle messages or items sent from the active RP to the standby RP since booting. Values are the following:<br>• Acks accepted—The number of bundle messages or items sent from the active RP to the standby RP.<br>• Acks ignored—The number of bundle messages or items sent by the active RP, but rejected by the standby RP.<br>• Nacks—The number of bundle messages or items given to the checkpointing facility (CF) on the active RP for transmitting to the standby RP, but failed to transmit. |
| Failed | The number of bundle messages or items the active RP attempted to send the standby RP when the send timer updated, but received an error back from CF. |
| Buffer alloc | Storage space allocated. |
| Buffer freed | Storage space available. |
| ISSU | In-Service Software Upgrade (ISSU) counters. |
| Checkpoint Messages Transformed | The details of the bundle messages or items transformed (upgraded or downgraded for compatibility) since booting so that the active RP and the standby RP can interoperate. |

| Field | Description |
|---|---|
| On Send | The number of messages sent by the active RP that succeeded, failed, or were transformations. |
| On Recv | The number of messages received by the active RP that succeeded, failed, or were transformations. |
| Negotiation | The number of times that the active RP and the standby RP have negotiated their interoperability parameters. |
| Started | The number of negotiations started. |
| Finished | The number of negotiations finished. |
| Failed to Start | The number of negotiations that failed to start. |
| Messages | The number of negotiation messages sent and received. These messages can be succeeded or failed.<br>• Send succeeded—Number of messages sent successfully.<br>• Send failed—Number of messages sent unsuccessfully.<br>• Buffer allocated—Storage space allowed.<br>• Buffer freed—Storage space available.<br>• Buffer alloc failed—No storage space available. |
| Init | The number of times the RSVP ISSU client has successfully and unsuccessfully (failed) initialized. |
| Session Registration | The number of session registrations, succeeded and failed, performed by the active RP whenever the standby RP reboots. |
| Session Unregistration | The number of session unregistrations, succeeded and failed, before the standby RP resets. |
| Errors | The details of errors or caveats. |

The following is sample output from the **show ip rsvp high-availability counters** command on the standby RP:

```
Router# show ip rsvp high-availability counters

State: Standby
```

```
Checkpoint Messages (Items) Received
  Valid:        1  (2)
  Invalid:      0  (0)
  Buffer freed: 1

ISSU:
  Checkpoint Messages Transformed:
    On Send:
      Succeeded:         0
      Failed:            0
      Transformations:   0
    On Recv:
      Succeeded:         1
      Failed:            0
      Transformations:   0

  Negotiation:
    Started:              1
    Finished:             1
    Failed to Start:      0
    Messages:
      Sent:
        Send succeeded:   5
        Send failed:      0
        Buffer allocated:        5
        Buffer freed:            0
        Buffer alloc failed:     0
      Received:
        Succeeded:        7
        Failed:           0
        Buffer freed:     7

  Init:
    Succeeded:            1
    Failed:               0

  Session Registration:
    Succeeded:            0
    Failed:               0

  Session Unregistration:
    Succeeded:            0
    Failed:               0

Errors:
  None
```

The table below describes the significant fields shown in the display.

***Table 107: show ip rsvp high-availability counters—Standby RP Field Descriptions***

| Field | Description |
|---|---|
| State | The RP state:<br>• Standby—Standby (backup) RP. |

| Field | Description |
|---|---|
| Checkpoint Messages (Items) Received | The details of the messages or items received by the standby RP. Values are the following:<br>• Valid—The number of valid messages or items received by the standby RP.<br>• Invalid—The number of invalid messages or items received by the standby RP.<br>• Buffer freed—Amount of storage space available. |
| ISSU | ISSU counters.<br>**Note** For descriptions of the ISSU fields, see the table above. |
| Errors | The details of errors or caveats. |

## Related Commands

| Command | Description |
|---|---|
| **clear ip rsvp high-availability counters** | Clears (sets to zero) the RSVP-TE HA counters that are being maintained by an RP. |
| **show ip rsvp high-availability database** | Displays the contents of the RSVP-TE HA read and write databases used in TE SSO. |
| **show ip rsvp high-availability summary** | Displays summary information for an RSVP-TE HA RP. |

# show ip rsvp high-availability database

To display contents of Resource Reservation Protocol (RSVP) high availability (HA) read and write databases used in traffic engineering (TE), use the **show ip rsvp high-availability database** command in user EXEC or privileged EXEC mode.

**show ip rsvp high-availability database** {**hello**| **if-autotun**| **link-management** {**interfaces** [**fixed**| **variable**]| **system**}| **lsp** [**filter** [**destination** *ip-address*]| [**lsp-id** *lsp-id*]| [**source** *ip-address*]| [**tunnel-id** *tunnel-id*]]| **lsp-head** [**filter** *number*]| **summary**}

## Syntax Description

| | |
|---|---|
| **hello** | Displays information about hello entries in read and write databases. |
| **if-autotun** | Displays information about TE HA autotunnel interface entries in read and write databases. |
| **link-management** | Displays information about link-management entries in the read and write databases. |
| **interfaces** | Displays information about link-management interfaces in the read and write databases. |
| **fixed** | (Optional) Displays information about link-management fixed interfaces in the read and write databases. |
| **variable** | (Optional) Displays information about link-management variable interfaces in the read and write databases. |
| **system** | Displays information about the link-management system in the read and write databases. |
| **lsp** | Displays information about label switched path (LSP) entries in the read and write databases. |
| **filter destination** *ip-address* | (Optional) Displays filtered information on the IP address of the destination (tunnel tail). |
| **filter lsp-id** *lsp-id* | (Optional) Displays filtered information on a specific LSP ID designated by a number from 0 to 65535. |
| **filter source** *ip-address* | (Optional) Displays filtered information on the IP address of the source (tunnel head). |
| **filter tunnel-id** *tunnel-id* | (Optional) Displays filtered information on a specific tunnel ID designated by a number from 0 to 65535. |

| | |
|---|---|
| **lsp-head** | Displays information about LSP-head entries in the read and write databases. |
| **filter** *number* | (Optional) Displays filtered information on a specific LSP-head router designated by a number from 0 to 65535. |
| **summary** | Displays cumulative information about entries in read and write databases. |

## Command Modes

User EXEC (>)

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was introduced. |
| 12.2(33)SRB | The command output was modified to display the result of a loose hop expansion performed on the router. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. The command output was modified to include path protection information specified by the **lsp-head** keyword. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |
| 15.0(1)S | This command was integrated into Cisco IOS Release 15.0(1)S. The command output was modified to distinguish database-entry information for point-to-point (P2P) tunnels from that for point-to-multipoint (P2MP) tunnels and to display error database information. |
| 12.2(50)SY | This command was integrated into Cisco IOS Release 12.2(50)SY. |
| Cisco IOS XE Release 3.5S | This command was integrated into Cisco IOS XE Release 3.5S. |
| 15.2(2)S | This command was modified. The **if-autotun** keyword was added. The output for the **show ip rsvp high-availability database lsp**, the **show ip rsvp high-availability database lsp-head**, and the **show ip rsvp high-availability database summary** commands was enhanced to display checkpoint information for MPLS TE autotunnel and automesh stateful switchover (SSO) tunnels. |

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.6S | This command was modified. The **if-autotun** keyword was added. The output for the **show ip rsvp high-availability database lsp**, the **show ip rsvp high-availability database lsp-head**, and the **show ip rsvp high-availability database summary** commands was enhanced to display checkpoint information for MPLS TE autotunnel and automesh stateful switchover (SSO) tunnels. |

## Usage Guidelines

Use the **show ip rsvp high-availability database** command to display information about entries in the read and write databases.

Use the **show ip rsvp high-availability database lsp** command to display loose hop information. A loose hop expansion can be performed on a router when the router processes the explicit router object (ERO) for an incoming path message. After the router removes all local IP addresses from the incoming ERO, it finds the next hop. If the ERO specifies that the next hop is loose instead of strict, the router consults the TE topology database and routing to determine the next hop and output interface to forward the path message. The result of the calculation is a list of hops; the list is placed in the outgoing ERO and checkpointed with the LSP data as the loose hop information.

In Cisco IOS Release 15.0(1)S and later releases, the **show ip rsvp high-availability database lsp** command displays sub-LSP information. If any sub-LSP, whether P2MP or P2P, fails to recover after a stateful switchover (SSO), the failure is noted in an error database for troubleshooting. You can use the **show ip rsvp high-availability database lsp** command to display error database entries.

You can use the **show ip rsvp high-availability database lsp-head** command only on a headend router; this command gives no information on other routers

## Examples

## Examples

The following is sample output from the **show ip rsvp high-availability database hello** command on an active Route Processor (RP):

```
Router# show ip rsvp high-availability database hello

HELLO WRITE DB
   Header:
     State: Checkpointed     Action: Add
     Seq #: 1                Flags: 0x0
   Data:
     Last sent Src_instance: 0xDE435865
HELLO READ DB
```

The table below describes the significant fields shown in the display.

***Table 108: show ip rsvp high-availability database hello—Active RP Field Descriptions***

| Field | Description |
|---|---|
| HELLO WRITE DB | Storage area for active RP hello data consisting of checkpointed RSVP-TE information that is sent to the standby RP when it becomes the active RP and needs to recover LSPs. This field is blank on a standby RP. |

| Field | Description |
|---|---|
| Header | Header information. |
| State | Status of an entry. Values are as follows:<br>• Ack-Pending—Entries have been sent but not acknowledged.<br>• Checkpointed—Entries have been sent and acknowledged by the standby RP.<br>• Send-Pending—Entries are waiting to be sent. |
| Action | Action taken. Values are as follows:<br>• Add—Adding an item to the standby RP.<br>• Delete—Deleting an item from the standby RP. This is a temporary action that takes place while the active RP awaits an acknowledgment (ack) of the delete operation.<br>• Modify—Modifying an item on the standby RP.<br>• Remove—Removing an item from the standby RP. |
| Seq # | Number used by the active and standby RPs to synchronize message acknowledgments (acks) and negative acknowledgments (nacks) to sent messages. |
| Flags | Attribute used to identify or track data. |
| Data | Information about the last transmission. |
| Last sent Src_instance | Last sent source instance identifier. |
| HELLO READ DB | Storage area for standby RP hello data. This field is blank on an active RP, except when it is in recovery mode. |

## Examples

The following is sample output from the **show ip rsvp high-availability database hello** on a standby RP:

```
Router# show ip rsvp high-availability database hello

HELLO WRITE DB
HELLO READ DB
   Header:
     State: Checkpointed     Action: Add
     Seq #: 1                Flags: 0x0
   Data:
     Last sent Src_instance: 0xDE435865
```

These fields are the same as those for the active RP described in the table except they are now in the read database for the standby RP.

## Examples

The following is sample output from the **show ip rsvp high-availability database if-autotun** command on an active RP.

```
Router# show ip rsvp high-availability database if-autotun
IF_AUTOTUN WRITE DB

  Header:
    State: Checkpointed     Action: Add
    Seq #: 1                Flags: 0x0
  Data:
    Tunnel ID: 1000 (if_handle: 85), prot_if_handle: 14
    template_unit: n/a, dest: 22.22.22.22, flags=0x0

  Header:
    State: Checkpointed     Action: Add
    Seq #: 61               Flags: 0x0
  Data:
    Tunnel ID: 2000 (if_handle: 86), prot_if_handle: 14
    template_unit: n/a, dest: 22.22.22.22, flags=0x1

  Header:
    State: Checkpointed     Action: Add
    Seq #: 1                Flags: 0x0
  Data:
    Tunnel ID: 3000 (if_handle: 87), prot_if_handle: 0
    template_unit: 1, dest: 22.22.22.22, flags=0x2

  Header:
    State: Checkpointed     Action: Add
    Seq #: 1                Flags: 0x0
  Data:
    Tunnel ID: 3001 (if_handle: 88), prot_if_handle: 0
    template_unit: 1, dest: 172.16.255.128, flags=0x2

  Header:
    State: Checkpointed     Action: Add
    Seq #: 1                Flags: 0x0
  Data:
    Tunnel ID: 3002 (if_handle: 89), prot_if_handle: 0
    template_unit: 1, dest: 200.0.0.0, flags=0x2


IF_AUTOTUN READ DB
```

The table below describes the significant fields shown in the display.

***Table 109: show ip rsvp high-availability database if-autotun—Active RP Field Descriptions***

| Field | Description |
|---|---|
| IF_AUTOTUN WRITE DB | Storage area for active RP autotunnel interface information. This field is blank on a standby RP. |
| Header | Header information. |

| Field | Description |
|---|---|
| State | Status of an entry. Values are as follows:<br>• Ack-Pending—Entries have been sent but not acknowledged.<br>• Checkpointed—Entries have been sent and acknowledged by the standby RP.<br>• Send-Pending—Entries are still waiting to be sent. |
| Action | Action taken. Values are as follows:<br>• Add—Adding an item to the standby RP.<br>• Delete—Deleting an item from the standby RP. This action appears temporarily while the active RP awaits an ack of the delete operation.<br>• Modify—Modifying an item on the standby RP.<br>• Remove—Removing an item from the standby RP. |
| Seq # | Number used by the active and standby RPs to synchronize message acks and nacks to sent messages. |
| Flags | Attributes used to identify or track data. |
| Data | Information about the last transmission. |
| Tunnel ID | Tunnel identifier. |
| if_handle | Internal number representing the autotunnel interface. For the same tunnel ID, this if_handle value should always be the same for the record in the Standby READ DB as in the Active WRITE DB. |
| prot_if_handle | For autotunnel mesh tunnels, this value should always be zero. For autotunnel primary tunnels, this is an internal number representing the egress interface of the autotunnel primary. For autotunnel backup tunnels, this is an internal number representing the interface that the backup is protecting. In all three cases, for the same tunnel ID, this value should always be the same for the record in the Standby READ DB as in the Active WRITE DB. |

| Field | Description |
|---|---|
| template_unit | For autotunnel mesh, this represents the auto-template interface number that the mesh tunnel was created from. For autotunnel primary and backup, this should be "n/a." |
| dest | Destination IP address of the autotunnel. |
| flags | Encodings have these values:<br>• 0 = autotunnel primary<br>• 1 = autotunnel backup<br>• 2 = autotunnel mesh |
| IF_AUTOTUN READ DB | Storage area for standby RP autotunnel interface information. This field is blank on an active RP. |

The fields for a standby RP are the same as those described in the table except that they are now in the interface autotunnel read database instead of the interface autotunnel write database that is used by an active RP.

## Examples

The following is sample output from the **show ip rsvp high-availability database link-management interfaces** command on an active RP:

```
Router# show ip rsvp high-availability database link-management interfaces

TE LINK WRITE DB
Flooding Protocol: ospf  IGP Area ID: 0  Link ID: 0 (GigabitEthernet3/2)
  Header:
    State: Checkpointed     Action: Add
    Seq #: 4                Flags: 0x0
  Data:
        Ifnumber: 5  Link Valid Flags: 0x193B
        Link Subnet Type: Broadcast
        Local Intfc ID: 0  Neighbor Intf ID: 0
        Link IP Address: 172.16.3.1
        Neighbor IGP System ID: 172.16.3.2  Neighbor IP Address: 10.0.0.0
        IGP Metric: 1  TE Metric: 1
        Physical Bandwidth: 1000000 kbits/sec
        Res. Global BW: 3000 kbits/sec
        Res. Sub BW: 0 kbits/sec
        Upstream::
                                 Global Pool   Sub Pool
                                 -----------   ----------
        Reservable Bandwidth[0]:           0            0 kbits/sec
        Reservable Bandwidth[1]:           0            0 kbits/sec
        Reservable Bandwidth[2]:           0            0 kbits/sec
        Reservable Bandwidth[3]:           0            0 kbits/sec
        Reservable Bandwidth[4]:           0            0 kbits/sec
        Reservable Bandwidth[5]:           0            0 kbits/sec
        Reservable Bandwidth[6]:           0            0 kbits/sec
        Reservable Bandwidth[7]:           0            0 kbits/sec
        Downstream::
                                 Global Pool   Sub Pool
                                 -----------   ----------
        Reservable Bandwidth[0]:        3000            0 kbits/sec
        Reservable Bandwidth[1]:        3000            0 kbits/sec
```

```
Reservable Bandwidth[2]:        3000            0 kbits/sec
Reservable Bandwidth[3]:        3000            0 kbits/sec
Reservable Bandwidth[4]:        3000            0 kbits/sec
Reservable Bandwidth[5]:        3000            0 kbits/sec
Reservable Bandwidth[6]:        3000            0 kbits/sec
Reservable Bandwidth[7]:        2900            0 kbits/sec
Affinity Bits: 0x0
Protection Type: Capability 0,  Working Priority 0
Number of TLVs: 0
```

The table below describes the significant fields shown in the display.

***Table 110: show ip rsvp high-availability database link-management interfaces—Active RP Field Descriptions***

| Field | Description |
|---|---|
| TE LINK WRITE DB | Storage area for active TE RP link data. This field is blank on a standby RP. |
| Flooding Protocol | Protocol that is flooding information for this area. OSPF = Open Shortest Path First. |
| IGP Area ID | Interior Gateway Protocol (IGP) identifier for the area being flooded. |
| Link ID | Link identifier and interface for the area being flooded. |
| Header | Header information. |
| State | Status of an entry. Values are as follows:<br>• Ack-Pending—Entries have been sent but not acknowledged.<br>• Checkpointed—Entries have been sent and acknowledged by the standby RP.<br>• Send-Pending—Entries are waiting to be sent. |
| Action | Action taken. Values are as follows:<br>• Add—Adding an item to the standby RP.<br>• Delete—Deleting an item from the standby RP. This action appears temporarily while the active RP awaits an ack of the delete operation.<br>• Modify—Modifying an item on the standby RP.<br>• Remove—Removing an item from the standby RP. |
| Seq # | Number used by the active and standby RPs to synchronize message acks and nacks to sent messages. |

| Field | Description |
|---|---|
| Flags | Attribute used to identify or track data. |
| Data | Information about the last transmission. |
| Ifnumber | Interface number. |
| Link Valid Flags | Attributes used to identify or track links. |
| Link Subnet Type | Subnet type of the link. Values are as follows:<br>• Broadcast—Data for multiple recipients.<br>• Nonbroadcast Multiaccess--A network in which data is transmitted directly from one computer to another over a virtual circuit or across a switching fabric.<br>• Point-to-Multipoint—Unidirectional connection in which a single source end system (known as a root node) connects to multiple destination end systems (known as leaves).<br>• Point-to-Point—Unidirectional or bidirectional connection between two end systems.<br>• Unknown subnet type—Subnet type not identified. |
| Local Intfc ID | Local interface identifier. |
| Neighbor Intf ID | Neighbor's interface identifier. |
| Link IP Address | IP address of the link. |
| Neighbor IGP System ID | Neighbor system identifier configured using IGP. |
| Neighbor IP Address | Neighbor's IP address. |
| IGP Metric | Metric value for the TE link configured using IGP. |
| TE Metric | Metric value for the TE link configured using Multiprotocol Label Switching (MPLS) TE. |
| Physical Bandwidth | Link bandwidth capacity in kilobits per second (kb/s). |
| Res. Global BW | Amount of reservable global pool bandwidth (in kb/s) on this link. |
| Res. Sub BW | Amount of reservable subpool bandwidth (in kb/s) on this link. |

| Field | Description |
|---|---|
| Upstream | Header for the following section of bandwidth values. |
| Global Pool | Global pool bandwidth (in kb/s) on this link. |
| Sub Pool | Subpool bandwidth (in kb/s) on this link. |
| Reservable Bandwidth [1] | Amount of bandwidth (in kb/s) available for reservations in the global TE topology and subpools. |
| Downstream | Header for the following section of bandwidth values. |
| Affinity Bits | Link attributes required in tunnels. |
| Protection Type | LSPs protected by fast reroute (FRR).<br>• Capability = LSPs capable of using FRR.<br>• Working Priority = LSPs actually using FRR. |
| Number of TLVs | Number of type, length, values (TLVs). |

The fields for a standby RP are the same as those described in the table except that they are now in the TE link read database instead of the TE link write database that is used by an active RP.

## Examples

The following is sample output from the **show ip rsvp high-availability database link-management system** command on an active RP:

```
Router# show ip rsvp high-availability database link-management system

TE SYSTEM WRITE DB
Flooding Protocol: OSPF  IGP Area ID: 0
  Header:
    State: Checkpointed     Action: Modify
    Seq #: 4                Flags: 0x0
  Data:
    LM Flood Data::
      LSA Valid flags: 0x0  Node LSA flag: 0x0
      IGP System ID: 172.16.3.1  MPLS TE Router ID: 10.0.0.3
      Flooded links: 1  TLV length: 0 (bytes)
      Fragment id: 0
TE SYSTEM READ DB
```

The table below describes the significant fields shown in the display.

***Table 111: show ip rsvp high-availability database link-management system—Active RP Field Descriptions***

| Field | Description |
|---|---|
| TE SYSTEM WRITE DB | Storage area for active TE RP system data. This field is blank on a standby RP. |

| Field | Description |
|---|---|
| Flooding Protocol | Protocol that is flooding information for this area. OSPF = Open Shortest Path First. |
| IGP Area ID | IGP identifier for the area being flooded. |
| Header | Header information. |
| State | Status of an entry. Values are as follows:<br>• Ack-Pending—Entries have been sent but not acknowledged.<br>• Checkpointed—Entries have been sent and acknowledged by the standby RP.<br>• Send-Pending—Entries are waiting to be sent. |
| Action | Action taken. Values are as follows:<br>• Add—Adding an item to the standby RP.<br>• Delete—Deleting an item from the standby RP. This action appears temporarily while the active RP awaits an ack of the delete operation.<br>• Modify—Modifying an item on the standby RP.<br>• Remove—Removing an item from the standby RP. |
| Seq # | Number used by the active and standby RPs to synchronize message acks and nacks to messages sent. |
| Flags | Attribute used to identify or track data. |
| Data | Information about the last transmission. |
| LM Flood Data | Link management (LM) flood data. |
| LSA Valid flags | Link-state advertisement (LSA) attributes. |
| Node LSA flag | LSA attributes used by a router. |
| IGP System ID | Identification (IP address) that IGP flooding uses in this area to identify this node. |
| MPLS TE Router ID | MPLS TE router identifier (IP address). |
| Flooded links | Number of flooded links. |

| Field | Description |
|---|---|
| TLV length | TLV length in bytes. |
| Fragment id | Fragment identifier for this link. |
| TE SYSTEM READ DB | Storage area for standby TE RP system data. This field is blank on a standby RP. |

The fields for a standby RP are the same as those described in the table except that they are now in the TE system read database instead of the TE system write database that is used by an active RP.

## Examples

The following is sample output from the **show ip rsvp high-availability database lsp** command on an active RP for a P2P tunnel:

```
Router# show ip rsvp high-availability database lsp

Tun ID: 0   LSP ID: 10   (P2P)
  SubGrp ID:   -
  SubGrp Orig: -
  Dest:   10.3.0.1
  Sender: 10.1.0.1     Ext. Tun ID: 10.1.0.1
  Header:
    State: Checkpointed     Action: Add
    Seq #: 2                Flags: 0x0
  Data:
    PathSet ID: -
    Lspvif if_num: -
    InLabel: -
    Out I/F: Se2/0
    Next-Hop: 10.1.3.2
    OutLabel: 16
    Loose hop info: None (0)
```

## Examples

The following is sample output from the **show ip rsvp high-availability database lsp** command on an active RP for a P2MP tunnel:

```
Router# show ip rsvp high-availability database lsp

Tun ID: 1   LSP ID: 127   (P2MP)
  SubGrp ID:   1
  SubGrp Orig: 10.1.0.1
  Dest:   10.2.0.1
  Sender: 10.1.0.1     Ext. Tun ID: 10.1.0.1
  Header:
    State: Checkpointed     Action: Add
    Seq #: 30               Flags: 0x0
  Data:
    PathSet ID: 0x1A000003
    Lspvif if_num: 35 (Lspvif0)
    InLabel: 19
    Out I/F: None
    Next-Hop: -
    OutLabel: -
    Loose hop info: None (0)
```

The table below describes the significant fields shown in the display.

*Table 112: show ip rsvp high-availability database lsp—Active RP Field Descriptions*

| Field | Description |
|---|---|
| P2P/P2MP | Tunnel type. |
| Subgrp ID | Subgroup identifier (valid only for P2MP TE LSPs). |
| Subgrp Orig | Subgroup origin IP address (valid only for P2MP TE LSPs). |
| Lspvif if_num | Interface number of the LSPVIF (valid only for P2MP TE tailends). |
| PathSet ID | Path set identifier (valid only for P2MP TE LSPs) |
| LSP WRITE DB | Storage area for active RP LSP data. This field is blank on a standby RP. |
| Tun ID | Tunnel identifier. |
| LSP ID | LSP identifier. |
| Dest | Tunnel destination IP address. |
| Sender | Tunnel sender IP address. |
| Ext. Tun ID | Extended tunnel identifier; usually set to 0 or the sender's IP address. |
| Header | Header information. |
| State | Status of an entry. Values are as follows:<br>• Ack-Pending—Entries have been sent, but not acknowledged.<br>• Checkpointed—Entries have been sent and acknowledged by the standby RP.<br>• Send-Pending—Entries are waiting to be sent. |

| Field | Description |
|---|---|
| Action | Action taken. Values are as follows:<br>• Add—Adding an item to the standby RP.<br>• Delete—Deleting an item from the standby RP. This action appears temporarily while the active RP awaits an ack of the delete operation.<br>• Modify—Modifying an item on the standby RP.<br>• Remove—Removing an item from the standby RP. |
| Seq # | Number used by the active and standby RPs to synchronize message acks and nacks to messages sent. |
| Flags | Attribute used to identify or track data. |
| Data | Information about the last transmission. |
| InLabel | Incoming label identifier. |
| Out I/F | Outgoing interface. |
| Next-Hop | Next hop IP address. |
| OutLabel | Outgoing label identifier. |
| Loose hop info | Lists the loose hop expansions performed on the router, or specifies None. |
| LSP READ DB | Storage area for standby RP LSP data. This field is blank on an active RP. |

The fields for a standby RP are the same as those described in the table except that they are now in the LSP read database instead of the LSP write database that is used by an active RP.

## Examples

The following is sample output from the **show ip rsvp high-availability database lsp-head** command on an active RP for a P2P tunnel:

```
Router# show ip rsvp high-availability database lsp-head

LSP_HEAD WRITE DB
  Tun ID: 0  (P2P)
  Header:
    State: Checkpointed     Action: Add
    Seq #: 2                Flags: 0x0
  Data:
    lsp_id: 10, bandwidth: 5, thead_flags: 0x1, popt: 1
    feature flags: none
```

```
    output_if_num: 11, output_nhop: 10.1.3.2
    RRR path setup info
      Destination: 10.3.0.1, Id: 10.3.0.1 Router Node (ospf) flag:0x0
      IGP: ospf, IGP area: 0, Number of hops: 3, metric: 128
      Hop 0: 10.1.3.2, Id: 10.2.0.1 Router Node (ospf), flag:0x0
      Hop 1: 10.2.3.3, Id: 10.3.0.1 Router Node (ospf), flag:0x0
      Hop 2: 10.3.0.1, Id: 10.3.0.1 Router Node (ospf), flag:0x0
```

## Examples

The following is sample output from the **show ip rsvp high-availability database lsp-head** command on an active RP for a P2MP tunnel:

```
Router# show ip rsvp high-availability database lsp-head

LSP_HEAD WRITE DB
Tun ID: 1  (P2MP)
  Destination: 10.2.0.1
  Header:
    State: Checkpointed     Action: Add
    Seq #: 3                Flags: 0x0
  Data:
    lsp_id: 11, bandwidth: 100, thead_flags: 0x1, popt: 1
    Subgrp_id: 1
    feature flags: none
    output_if_num: 3, output_nhop: 10.1.2.2
    RRR path setup info
      Destination: 10.2.0.1, Id: 10.2.0.1 Router Node (ospf) flag:0x0
      IGP: ospf, IGP area: 0, Number of hops: 3, metric: 10
      Hop 0: 10.1.2.1, Id: 10.1.0.1 Router Node (ospf), flag:0x0
      Hop 1: 10.1.2.2, Id: 10.2.0.1 Router Node (ospf), flag:0x0
      Hop 2: 10.2.0.1, Id: 10.2.0.1 Router Node (ospf), flag:0x0
```

The table below describes the significant fields shown in the display.

***Table 113: show ip rsvp high-availability database lsp-head—Active RP Field Descriptions***

| Field | Description |
|---|---|
| LSP_HEAD WRITE DB | Storage area for active RP LSP-head data. This field is blank on a standby RP. |
| P2P/P2MP | Tunnel type. |
| Tun ID | Tunnel identifier. |
| Header | Header information. |
| State | Status of an entry. Values are as follows:<br>• Ack-Pending—Entries have been sent, but not acknowledged.<br>• Checkpointed—Entries have been sent and acknowledged by the standby RP.<br>• Send-Pending—Entries are waiting to be sent. |

| Field | Description |
|---|---|
| Action | Action taken. Values are as follows:<br>• Add—Adding an item to the standby RP.<br>• Delete—Deleting an item from the standby RP. This is a temporary action that takes place while the active RP awaits an ack of the delete operation.<br>• Modify—Modifying an item on the standby RP.<br>• Remove—Removing an item from the standby RP. |
| Seq # | Number used by the active and standby RPs to synchronize message acks and nacks to messages sent. |
| Flags | Attribute used to identify or track data. |
| Data | Information about the last transmission. |
| lsp_id | LSP identifier. |
| bandwidth | Bandwidth on the LSP (in kb/s). |
| thead_flags | Tunnel head attribute used to identify or track data. |
| popt | Parsing option number. |
| feature_flags | Indicates whether the LSP being used to forward traffic is the secondary LSP using the path protection path option. Valid values are as follows:<br>• none<br>• path protection active |
| output_if_num | Output interface number. |
| output_nhop | Output next hop IP address. |
| RRR path setup info | Routing with Resource Reservation (RRR) path information. |
| Destination | Destination IP address. |

| Field | Description |
|---|---|
| Id | IP address and protocol of the routing node. Values are as follows:<br>• ISIS = Intermediate System-to-Intermediate System<br>• OSPF = Open Shortest Path First |
| flag | Attribute used to track data. |
| IGP | Interior Gateway Protocol. OSPF = Open Shortest Path First. |
| IGP area | IGP area identifier. |
| Number of hops | Number of connections or routers. |
| metric | Routing cost. |
| Hop | Hop's number and IP address. |
| LSP_HEAD READ DB | Storage area for standby RP LSP-head data. This field is blank on an active RP. |

The fields for a standby RP are the same as those described in the table except that they are now in the LSP_head read database instead of the LSP_head write database that is used by an active RP.

## Examples

The following is sample output from the **show ip rsvp high-availability database summary** command on an active RP:

```
Router# show ip rsvp high-availability database summary

Write DB:
  Send-Pending:     0
  Ack-Pending :     0
  Checkpointed:    10
  Total       :    10
Read DB:
  Total       :     0
```

The table below describes the significant fields shown in the display.

***Table 114: show ip rsvp high-availability database summary—Active RP Field Descriptions***

| Field | Description |
|---|---|
| Write DB | Storage area for active RP summary data. This field is blank on a standby RP. |
| Send-Pending | Entries are waiting to be sent. |

| Field | Description |
|---|---|
| Ack-Pending | Entries have been sent, but are waiting to be acknowledged. |
| Checkpointed | Entries have been sent and acknowledged. |
| Total | Total number of entries in the write database. |
| Total | Total number of entries in the read database. |

## Examples

The following is sample output from the **show ip rsvp high-availability database summary** command on a standby RP:

```
Router# show ip rsvp high-availability database summary

Write DB:
  Send-Pending:     0
  Ack-Pending :     0
  Checkpointed:     0
  Total       :     0
Read DB:
  Total       :    10
```

The table below describes the significant fields shown in the display.

***Table 115: show ip rsvp high-availability database summary—Standby RP Field Descriptions***

| Field | Description |
|---|---|
| Write DB | Storage area for active RP summary data. |
| Send-Pending | Entries are waiting to be sent. |
| Ack-Pending | Entries have been sent but are waiting to be acknowledged. |
| Checkpointed | Entries have been sent and acknowledged. |
| Total | Total number of entries in the write database. |
| Total | Total number of entries in the read database. |

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp high-availability counters** | Displays all RSVP HA counters that are being maintained by an RP. |
| **show ip rsvp high-availability summary** | Displays summary information for an RSVP HA RP. |

# show ip rsvp high-availability summary

To display summary information for a Resource Reservation Protocol (RSVP) traffic engineering (TE) high availability (HA) Route Processor (RP), use the **show ip rsvp high-availability summary** command in user EXEC or privileged EXEC mode.

**show ip rsvp high-availability summary**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC (>)

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRA | This command was introduced. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 15.2(2)S | This command was modified. The output was enhanced to display checkpoint information for MPLS TE autotunnel and automesh stateful switchover (SSO) tunnels. |
| Cisco IOS XE Release 3.6S | This command was modified. The output was enhanced to display checkpoint information for MPLS TE autotunnel and automesh stateful switchover (SSO) tunnels. |

## Usage Guidelines

Use the **show ip rsvp high-availability summary**command to display information about the HA parameters currently configured on an RP.

The command output differs depending on whether the RP is active or standby.

## Examples

The following is sample output from the **show ip rsvp high-availability summary** command on an active RP:

```
Router# show ip rsvp high-availability summary

State:
Graceful-Restart: Enabled, mode: full
HA state: Active
Checkpointing: Allowed
Messages:
Send timer: not running (Interval: 1000 msec)
Items sent per Interval: 200
CF buffer size used: 2000
```

**Note** On a standby RP, only the first three lines of the output are displayed. On an active RP, all lines are displayed.

The table below describes the significant fields shown in the display.

***Table 116: show ip rsvp high-availability summary—Field Descriptions***

| Field | Description |
|---|---|
| State | Status of graceful restart and HA. |
| Graceful Restart | Restart capability:<br>• Enabled—Restart capability is activated for a router (full mode) or its neighbor (help-neighbor).<br>• Disabled—Restart capability is not activated. |
| HA state | The RP state, which is the following:<br>• Active—Active RP.<br>• Standby—Standby (backup) RP.<br>• Recovering—The active RP is in recovery period. |
| Checkpointing | The function that copies state information (write database entries) from the active RP to the standby RP. Values are the following:<br>• Allowed—Functioning normally.<br>• Not Allowed—Checkpointing is not allowed. Reasons may be that the RP is not present or not ready. |
| Messages | The checkpointed messages that the active RP sends to the standby RP during a specified interval. |

| Field | Description |
|---|---|
| Send timer | The write database timer. Values are the following:<br>• running—Entries are in the write database in the send-pending state and checkpointing is allowed.<br>• not running—Checkpointing is not allowed or the write database is empty.<br>**Note** Entries in the write database can be in the following states:<br>• Send-Pending—The entry has not been sent to the standby RP yet.<br>• Ack-Pending—The entry was sent to the standby RP, but no acknowledgment was received from the standby RP yet.<br>• Checkpointed—The checkpointing facility (CF) message has been acknowledged by the standby RP, which notifies the active RP. |
| Interval | Time, in milliseconds (ms), when the active RP sends messages to the standby RP. |
| Items sent per Interval | The number of database entries (data that has been taken from the write database and packed into bundle message for transmitting to the standby RP), which the active RP sends to the standby RP each time the write database timer activates. |
| CF buffer size used | Amount of storage space, in bytes, used by the checkpointing facility. |

In some cases, the checkpointing field displays Not Allowed. Here is an excerpt from sample output:

```
Checkpointing: Not Allowed
Peer RP Present : No
RF Comm. Up : No
Flow Control On : No
CF Comm. Up : No
RF Ready to Recv: No
```

**Note** If checkpointing is allowed, the attributes displayed in the sample output do not appear. Refer to the **show ip rsvp high-availability summary** command output on an active RP for more details.

The table below describes the significant fields shown in the display.

*Table 117: show ip rsvp high-availability summary—Checkpointing Field Descriptions*

| Field | Description |
|---|---|
| Peer RP Present : No | The active RP cannot communicate with any peer RP.<br>**Note** This can happen if the standby RP is removed, or if it is temporarily unavailable, such as during a restart. |
| RF Comm. Up : No | The redundant facility (RF) on the active RP is unable to communicate with the RF on the standby RP. |
| Flow Control On : No | The active RP cannot send Internet Protocol communications (IPC) messages (using checkpointing) to the standby RP because flow control is off. |
| CF Comm. Up : No | The TE CF client on the active RP is unable to communicate with the TE CF client on the standby RP. |
| RF Ready to Recv : No | The RF on the standby RP is not ready to receive checkpoint messages. |

The following is sample output from the **show ip rsvp high-availability summary** command after a stateful switchover (SSO) has occurred.

```
Router# show ip rsvp high-availability summary

State:
 Graceful-Restart: Enabled
 HA state: active
Checkpointing: Allowed
Recovery Time (msec)
 Advertised:    120000 msec
 Last recorded: 75012 msec
Messages:
 Send timer: not running (Interval:1000)
 Items sent per Interval: 200
```

The table below describes the significant fields shown in the display

*Table 118: show ip rsvp high-availability summary—After an SSO Field Descriptions*

| Field | Description |
|---|---|
| Advertised | The advertised recovery time, in milliseconds. |
| Last recorded | The last recorded recovery time, in milliseconds. |

## Related Commands

| Command | Description |
|---|---|
| **clear ip rsvp high-availability counters** | Clears (sets to zero) the RSVP-TE HA counters that are being maintained by an RP. |
| **show ip rsvp high-availability counters** | Displays the RSVP-TE HA counters that are being maintained by an RP. |
| **show ip rsvp high-availability database** | Displays the contents of the RSVP-TE HA read and write databases used in TE SSO. |

# show ip rsvp host

To display specific information for a Resource Reservation Protocol (RSVP) host, use the **showiprsvphost** command in user EXEC or privileged EXEC mode.

**show ip rsvp host** {**receivers**| **senders**} [*hostname*| *group-address*]

## Syntax Description

| | |
|---|---|
| **senders** | RSVP-related sender information currently in the database. |
| **receivers** | RSVP-related receiver information currently in the database. |
| *hostname* | (Optional) Hostname of the source or destination. |
| *group-address* | (Optional) IP address of the source or destination. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(3)T | This command was introduced. |
| 12.4(6)T | This command was modified. The command output was modified to display RSVP identity information when configured. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

Use the **showiprsvphost** command to display static RSVP senders and receivers. If a router has any local host receivers or senders that have RSVP identities configured, the application IDs that they use are also displayed.

## Examples

In the following example from the**showiprsvphostsenders**command, no RSVP identities are configured for the local sender:

```
Router# show ip rsvp host senders
To              From            Pro DPort Sport Prev Hop      I/F      BPS
192.168.104.3 192.168.104.1 UDP 1     1                           10K
  Mode(s): Host CLI
```

The table below describes the significant fields shown in the display.

*Table 119: show ip rsvp host senders (No RSVP Identities Configured) Field Descriptions*

| Field | Description |
|---|---|
| To | IP address of the receiver. |
| From | IP address of the sender. |
| Pro | Protocol code. IP protocol such as TCP or UDP. |
| DPort | Destination port number. Code 1 indicates an IP protocol such as TCP or UDP. |
| Sport | Source port number. Code 1 indicates an IP protocol such as TCP or UDP. |
| Prev Hop | IP address of the previous hop. Blank means no previous hop. |
| I/F | Interface of the previous hop. |
| BPS | Reservation rate, in bits per second (bps). |
| Mode(s) | Any of the following strings:<br>• Host--The router is acting as the host system or RSVP endpoint for this reservation.<br>• LSP-Tunnel--The reservation is for a traffic engineering (TE) tunnel.<br>• MIB--The reservation was created via an Simple Network Management Protocol (SNMP) SET directive from a remote management station.<br>• CLI--The reservation was created via a local RSVP command.<br>• Host CLI--A combination of the host and command line interface (CLI) strings meaning that the static sender being displayed was created by the **iprsvpsender-host** command. |

In the following example from the**showiprsvphostsenders**command, an RSVP identity is configured for the local sender:

```
Router# show ip rsvp host senders
To            From          Pro DPort Sport Prev Hop      I/F      BPS
192.168.104.3 192.168.104.1 UDP 1     1                            10K
  Mode(s): Host CLI
  Identity: voice100
    Locator: GUID=www.cisco.com,APP=voice,VER=100.0
    ID Type: Application
```

The table below describes the significant fields shown in the display.

***Table 120: show ip rsvp host senders (RSVP Identity Configured) Field Descriptions***

| Field | Description |
|---|---|
| To | IP address of the receiver. |
| From | IP address of the sender. |
| Pro | Protocol code. IP protocol such as TCP or UDP. |
| DPort | Destination port number. Code 1 indicates IP protocol such as TCP or UDP. |
| Sport | Source port number. Code 1 indicates IP protocol such as TCP or UDP. |
| Prev Hop | IP address of the previous hop. Blank means no previous hop. |
| I/F | Interface of the previous hop. |
| BPS | Reservation rate in bits per second (bps). |
| Mode(s) | Any of the following strings:<br>• CLI--The reservation was created via a local RSVP command.<br>• Host--The router is acting as the host system or RSVP endpoint for this reservation.<br>• Host CLI--A combination of the host and CLI strings meaning that the static sender being displayed was created by the **iprsvpsender-host** command.<br>• LSP-Tunnel--The reservation is for a Traffic Engineering (TE) tunnel.<br>• MIB--The reservation was created via an SNMP SET directive from a remote management station. |
| Identity | The alias string for the RSVP application ID. |
| Locator | The application ID that is being signaled in the RSVP PATH message for this statically-configured sender. |

| Field | Description |
|---|---|
| ID Type | Types of identities. RSVP defines two types: application IDs (Application) and user IDs (User). Cisco IOS software and Cisco IOS XE software support application IDs only. |

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp sender-host** | Enables a router to simulate a host generating an RSVP PATH message. |

# show ip rsvp host vrf

To display specific information for a Resource Reservation Protocol (RSVP) host configured with a virtual routing and forwarding (VRF) instance, use the **showiprsvphostvrf** command in user EXEC or privileged EXEC mode.

**show ip rsvp host vrf** {*| *vrf-name*} {**receivers**| **senders**} [*group-name*| *group-address*]

## Syntax Description

| | |
|---|---|
| * | Displays all VRFs. |
| *vrf-name* | Name of a specified VRF. |
| **receivers** | Displays RSVP-related receiver information currently in the database. |
| **senders** | Displays RSVP-related sender information currently in the database. |
| *group-name* | (Optional) Hostname of the source or destination. |
| *group-address* | (Optional) IP address of the source or destination. |

## Command Modes

User EXEC (<) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced. |

## Usage Guidelines

Use the **showiprsvphostvrf**command to display VRFs and static RSVP senders and receivers.

## Examples

In the following example from the**showiprsvphostvrf*senders**command, VRFs are displayed for the local senders:

```
Router# show ip rsvp host vrf * senders
VRF: vrf2
To                  From                Pro DPort Sport Prev Hop      I/F      BPS
192.168.104.4       198.168.104.12      UDP 10    10    none          none     10K
  Mode(s): Host CLI
VRF: vrf1
To                  From                Pro DPort Sport Prev Hop      I/F      BPS
192.168.105.4       198.168.105.12      UDP 10    10    none          none     10K
  Mode(s): Host CLI
```

The table below describes the significant fields shown in the display.

*Table 121: show ip rsvp host vrf senders Field Descriptions*

| Field | Description |
|---|---|
| VRF | Name of the VRF. |
| To | IP address of the receiver. |
| From | IP address of the sender. |
| Pro | Protocol code. IP protocol such as TCP or UDP. |
| DPort | Destination port number. Code 1 indicates an IP protocol such as TCP or UDP. |
| Sport | Source port number. Code 1 indicates an IP protocol such as TCP or UDP. |
| Prev Hop | IP address of the previous hop. Blank means no previous hop. |
| I/F | Interface of the previous hop. |
| BPS | Reservation rate in bits per second (bps). |
| Mode(s) | Any of the following strings:<br>• Host--The router is acting as the host system or RSVP endpoint for this reservation.<br>• LSP-Tunnel--The reservation is for a Traffic Engineering (TE) tunnel.<br>• MIB--The reservation was created via an SNMP SET directive from a remote management station.<br>• CLI--The reservation was created via a local RSVP CLI command.<br>• Host CLI--A combination of the host and CLI strings meaning that the static sender being displayed was created by the **iprsvpsender-host** CLI command. |

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp host** | Displays specific information for an RSVP host. |

# show ip rsvp ingress

To display information about the Resource Reservation Protocol (RSVP) ingress bandwidth configured on interfaces, use the **showiprsvpingress** command in privileged EXEC mode.

**show ip rsvp ingress interface [detail]** [*type number*]

## Syntax Description

| | |
|---|---|
| **interface** | Specifies the interface. |
| *type number* | (Optional) Interface type and interface or subinterface number. |
| **detail** | (Optional) Displays detailed information on the ingress bandwidth. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.1(3)T | This command was introduced. |
| 15.1(1)S | This command was integrated into Cisco IOS Release 15.1(1)S. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |

## Usage Guidelines

Use the **showiprsvpingress** command to display information on the RSVP ingress bandwidth configured on a specific interface or all interfaces. If you do not specify the optional keyword or arguments, the command displays information about the RSVP ingress bandwidth configured on all interfaces. Use the **detail** keyword to display the detailed information on ingress bandwidth for a specific interface or for all interfaces.

## Examples

The following is sample output from the **showiprsvpingressdetailethernet1/0** command:

```
Device# show ip rsvp ingress interface detail ethernet 1/0
interface    rsvp  in-allocated  in-i/f max  in-flow max  VRF
Et1/0        ena   0             7500K       7500K        0
```

The table below describes the significant fields shown in the display.

*Table 122: show ip rsvp ingress Field Descriptions*

| Field | Description |
|---|---|
| interface | Displays the interface on which the ingress bandwidth is configured. |
| rsvp | The state of RSVP. Values are enabled (activated) or disabled (deactivated).<br>**Note** This field is disabled only if an internal error occurs when registering with Routing Information Base (RIB). |
| in-allocated | Amount of bandwidth, in bits per second, currently allocated. |
| in-i/f max | Ingress reservable bandwidth, in Kb/s. |
| in-flow max | Percentage of interface bandwidth configured as RSVP ingress bandwidth. |
| VRF | VRF name. |

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp bandwidth** | Enables RSVP for IP on an interface. |
| **maximum bandwidth ingress** | Configures the bandwidth parameters for the ingress policy pool. |

# show ip rsvp installed

To display Resource Reservation Protocol (RSVP)-related installed filters and corresponding bandwidth information, use the **showiprsvpinstalled** command in user EXEC or privileged EXEC mode.

**show ip rsvp installed** [**vrf** {*| *vrf-name*}] [*interface-type interface-number*] **[detail]**

## Syntax Description

| | |
|---|---|
| vrf * | (Optional) Displays all the configured virtual routing and forwarding (VRF) instances. |
| **vrf** *vrf-name* | (Optional) Name of a specified VRF. |
| *interface-type* | (Optional) Type of the interface. |
| *interface-number* | (Optional) Number of the interface. |
| **detail** | (Optional) Displays additional information about interfaces and their reservations. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.2(2)T | This command was integrated into Cisco IOS Release 12.2(2)T. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(15)T | This command was modified. The command output was modified to display the resources required for a traffic control state block (TCSB) after compression has been taken into account. |
| 12.2(18)SXF2 | This command was integrated into Cisco IOS Release 12.2(18)SXF2. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SRC | This command was modified. The command output was modified to display RSVP aggregation information. |
| 15.0(1)M | This command was modified. The **vrf**and*keywords and the *vrf-name* argument were added. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelin

**Note** The syntax of the command depends on your platform and release. The **vrf***vrf-name*keyword and argument combination is not supported on Cisco ASR 1000 series routers.

The **showiprsvpinstalled**command displays information about interfaces and their reservations. Enter the optional **detail** keyword for additional information, including the reservation's traffic parameters, downstream hop, compression, VRFs, and resources used by RSVP to ensure quality of service (QoS) for this reservation.

## Examples

This section provides sample output from the **showiprsvpinstalled** commands. Depending upon the interface or platform in use and the options enabled, the output that you see may vary slightly from the examples shown below:

## Examples

The following is sample output from the **showiprsvpinstalled**command:

```
Router# show ip rsvp installed
RSVP: Ethernet1: has no installed reservations
RSVP: Serial0:
     kbps   To              From      Protocol DPort Sport Weight Conversation
     0      192.168.0.0     172.16.2.28     UDP 20    30    128   270
     150    192.168.0.1     172.16.2.1      UDP 20    30    128   268
     100    192.168.0.1     172.16.1.1      UDP 20    30    128   267
     200    192.168.0.1     172.16.1.25     UDP 20    30    256   265
     200    192.168.0.2     172.16.1.25     UDP 20    30    128   271
     0      192.168.0.2     172.16.2.28     UDP 20    30    128   269
     150    192.168.0.2     172.16.2.1      UDP 20    30    128   266
     350    192.168.0.3     172.16.0.0      UDP 20    30    128   26
```

The table below describes the significant fields shown in the display.

***Table 123: show ip rsvp installed Field Descriptions***

| Field | Description |
|---|---|
| kbps | Reserved rate in kilobits per second. |
| To | IP address of the source device. |
| From | IP address of the destination device. |
| Protocol | Protocol code. Code indicates IP protocol such as TCP or User Datagram Protocol (UDP). |
| DPort | Destination port number. |
| Sport | Source port number. |
| Weight | Weight used in Weighted Fair Queueing (WFQ). |

| Field | Description |
|---|---|
| Conversation | WFQ conversation number.<br>**Note** If WFQ is not configured on the interface, weight and conversation will be zero. |

## Examples

The following sample output from the **showiprsvpinstalled** detail command shows the compression parameters, including the compression method, the compression context ID, and the bytes saved per packet, on serial interface 3/0 in effect:

```
Router# show ip rsvp installed detail
RSVP:Ethernet2/1 has no installed reservations
RSVP:Serial3/0 has the following installed reservations
RSVP Reservation. Destination is 10.1.1.2. Source is 10.1.1.1,
  Protocol is UDP, Destination port is 18054, Source port is 19156
  Compression:(method rtp, context ID = 1, 37.98 bytes-saved/pkt avg)
  Admitted flowspec:
    Reserved bandwidth:65600 bits/sec, Maximum burst:328 bytes, Peak rate:80K bits/sec
    Min Policed Unit:164 bytes, Max Pkt Size:164 bytes
  Admitted flowspec (as required if compression were not applied):
    Reserved bandwidth:80K bits/sec, Maximum burst:400 bytes, Peak rate:80K bits/sec
    Min Policed Unit:200 bytes, Max Pkt Size:200 bytes
  Resource provider for this flow:
    WFQ on FR PVC dlci 101 on Se3/0: PRIORITY queue 24.  Weight:0, BW 66 kbps
  Conversation supports 1 reservations [0x1000405]
  Data given reserved service:3963 packets (642085 bytes)
  Data given best-effort service:0 packets (0 bytes)
  Reserved traffic classified for 80 seconds
  Long-term average bitrate (bits/sec):64901 reserved, 0 best-effort
  Policy:INSTALL. Policy source(s):Default
```

The following sample output from the **showiprsvpinstalled** detail command shows that compression is not predicted on the serial3/0 interface because no compression context IDs are available:

```
Router# show ip rsvp installed detail
RSVP:Ethernet2/1 has no installed reservations
RSVP:Serial3/0 has the following installed reservations
RSVP Reservation. Destination is 10.1.1.2. Source is 10.1.1.1,
  Protocol is UDP, Destination port is 18116, Source port is 16594
  Compression:(rtp compression not predicted:no contexts available)
  Admitted flowspec:
    Reserved bandwidth:80K bits/sec, Maximum burst:400 bytes, Peak rate:80K bits/sec
    Min Policed Unit:200 bytes, Max Pkt Size:200 bytes
  Resource provider for this flow:
    WFQ on FR PVC dlci 101 on Se3/0: PRIORITY queue 24.  Weight:0, BW 80 kbps
  Conversation supports 1 reservations [0x2000420]
  Data given reserved service:11306 packets (2261200 bytes)
  Data given best-effort service:0 packets (0 bytes)
  Reserved traffic classified for 226 seconds
  Long-term average bitrate (bits/sec):79951 reserved, 0 best-effort
  Policy:INSTALL. Policy source(s):Default
```

**Note** When no compression context IDs are available, use the **iprtpcompression-connections***number* command to increase the pool of compression context IDs.

## Examples

The following is sample output from the **showiprsvpinstalled** command when RSVP aggregation is configured:

```
Router# show ip rsvp installed

RSVP: Ethernet0/0 has no installed reservations
RSVP: Serial1/0
BPS    To              From            Protoc DPort  Sport
300K   192.168.50.1    192.168.40.1    0      46     0
RSVP: RSVP 3175 AggResv 192.168.40.1->192.168.50.1_ef(46)
BPS    To              From            Protoc DPort  Sport
80K    192.168.5.1     192.168.2.1     TCP    222    222
80K    192.168.6.1     192.168.2.1     TCP    223    223
```

The table below describes the significant fields shown in the display.

***Table 124: show ip rsvp installed Field Descriptions with RSVP Aggregation***

| Field | Description |
|---|---|
| RSVP | Reservation information for a specified interface. |
| BPS | Reserved rate in bits per second (BPS). |
| To | IP address of the source device. |
| From | IP address of the destination device. |
| Protoc | Protocol code.<br>• Code indicates IP protocol such as TCP or User Datagram Protocol (UDP) for end-to-end (E2E) reservations.<br>• Code is 0 for aggregate reservations. |
| DPort | Destination port number.<br>• Number indicates protocol destination port for E2E reservations.<br>• Number indicates differentiated services code point (DSCP) for aggregate reservations. |
| Sport | Source port number.<br>• Number indicates protocol source port for E2E reservations.<br>• Number is 0 for aggregate reservations. |

| Field | Description |
|---|---|
| RSVP | Individual E2E reservations mapped onto an aggregate. Information includes the following:<br>• IP address of the aggregate source.<br>• IP address of the aggregate destination.<br>• Differentiated services code point (DSCP) value. |

## Examples

The following is sample output from the **showiprsvpinstalleddetail** command when RSVP aggregation is configured and one E2E reservation that is mapped across an aggregate reservation as seen at the aggregator exists:

```
Router# show ip rsvp installed detail
RSVP: Ethernet0/0 has no installed reservations
RSVP: Serial1/0 has the following installed reservations
RSVP Reservation. Destination is 192.168.50.1. Source is 192.168.40.1,
  Protocol is 0  , Destination port is 46, Source port is 0
  Traffic Control ID handle: 35000403
  Created: 20:27:14 EST Thu Nov 29 2007
  Admitted flowspec:
    Reserved bandwidth: 300K bits/sec, Maximum burst: 300K bytes, Peak rate: 300K bits/sec
    Min Policed Unit: 20 bytes, Max Pkt Size: 0 bytes
  Resource provider for this flow: None
  Conversation supports 1 reservations [0x3000408]
  Data given reserved service: 0 packets (0 bytes)
  Data given best-effort service: 0 packets (0 bytes)
  Reserved traffic classified for 24558 seconds
  Long-term average bitrate (bits/sec): 0 reserved, 0 best-effort
  Policy: INSTALL. Policy source(s): Default
RSVP: RSVP 3175 AggResv 192.168.40.1->192.168.50.1_ef(46) has the following installed
reservations
RSVP Reservation. Destination is 192.168.5.1. Source is 192.168.2.1,
  Protocol is TCP, Destination port is 222, Source port is 222
  Traffic Control ID handle: 0500040B
  Created: 20:27:14 EST Thu Nov 29 2007
  Admitted flowspec:
    Reserved bandwidth: 80K bits/sec, Maximum burst: 5K bytes, Peak rate: 80K bits/sec
    Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  Resource provider for this flow:
    QBM
  Conversation supports 1 reservations [0x600040A]
  Data given reserved service: 0 packets (0 bytes)
  Data given best-effort service: 0 packets (0 bytes)
  Reserved traffic classified for 24558 seconds
  Long-term average bitrate (bits/sec): 0 reserved, 0 best-effort
  Policy: INSTALL. Policy source(s):
```

The table below describes the significant fields shown in the display.

***Table 125: show ip rsvp installed detail Field Descriptions with RSVP Aggregation***

| Field | Description |
|---|---|
| RSVP | Reservation information for a specified interface. |

| Field | Description |
| --- | --- |
| RSVP Reservation | |

| Field | Description |
|---|---|
| | Reservation information for the serial 1/0 interface that includes the following:<br>• Destination IP address.<br>  • Deaggregator for aggregate reservations.<br>• Source IP address.<br>  • Aggregator for aggregate reservations.<br>• Protocol used.<br>  • 0 for aggregate reservations.<br>  • TCP/UDP or protocol for E2E reservations.<br>• Destination port.<br>  • Differentiated services code (DSCP) for aggregate reservations.<br>  • Protocol port number for E2E reservations.<br>• Source port.<br>  • 0 for aggregate reservations.<br>  • Protocol port number for E2E reservations.<br>• Traffic control identifier assigned by RSVP for bookkeeping purposes.<br>• Creation date.<br>• Flowspec information that includes bandwidth, maximum burst, peak rate, policed unit size, and maximum packet size.<br>• Resource provider information.<br>  • None for aggregate reservations.<br>  • QoS bandwidth manager (BM) for E2E reservations.<br>• Type of service provided--reserved and best effort (always 0 packets in an RSVP/DiffServ node).<br>• Length of time traffic is classified. |

| Field | Description |
|---|---|
| | • Bitrate (always 0 on an RSVP/DiffServ node)<br>• Policies. |
| RSVP | Aggregate information that includes the following:<br>• IP address of the aggregate source.<br>• IP address of the aggregate destination.<br>• DSCP.<br>**Note** The remaining fields describe the aggregate's E2E reservations with values explained in preceding fields. |

## Examples

The following is sample output when a specific VRF is configured:

```
Router# show ip rsvp installed vrf myvrf detail
RSVP: FastEthernet2/0 has the following installed reservations
RSVP Reservation. Destination is 10.10.10.10. Source is 10.10.10.12,
  Protocol is UDP, Destination port is 10, Source port is 10
  Traffic Control ID handle: C8000407
  Created: 22:51:26 UTC Sun Feb 17 2008
  Admitted flowspec:
    Reserved bandwidth: 10K bits/sec, Maximum burst: 10K bytes, Peak rate: 10K bits/sec
    Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  Resource provider for this flow: None
  Conversation supports 1 reservations [0xBF000406]
  Data given reserved service: 0 packets (0 bytes)
  Data given best-effort service: 0 packets (0 bytes)
  Reserved traffic classified for 12783 seconds
  Long-term average bitrate (bits/sec): 0 reserved, 0 best-effort
  Policy: INSTALL. Policy source(s): Default
VRF : myvrf
```

The table below describes the significant fields shown in the display.

***Table 126: show ip rsvp installed detail Field Descriptions with VRFs***

| Field | Description |
|---|---|
| RSVP | Reservation information for a specified interface. |

| Field | Description |
| --- | --- |
| RSVP Reservation | |

| Field | Description |
|---|---|
| | Reservation information for the serial 1/0 interface that includes the following:<br>• Destination IP address.<br>  • Deaggregator for aggregate reservations.<br>• Source IP address.<br>  • Aggregator for aggregate reservations.<br>• Protocol used.<br>  • 0 for aggregate reservations.<br>  • TCP/UDP or protocol for E2E reservations.<br>• Destination port.<br>  • Differentiated services code (DSCP) for aggregate reservations.<br>  • Protocol port number for E2E reservations.<br>• Source port.<br>  • 0 for aggregate reservations.<br>  • Protocol port number for E2E reservations.<br>• Traffic control identifier assigned by RSVP for bookkeeping purposes.<br>• Creation date.<br>• Flowspec information that includes bandwidth, maximum burst, peak rate, policed unit size, and maximum packet size.<br>• Resource provider information.<br>  • None for aggregate reservations.<br>  • QoS bandwidth manager (BM) for E2E reservations.<br>• Type of service provided--reserved and best effort (always 0 packets in an RSVP/DiffServ node).<br>• Length of time traffic is classified. |

| Field | Description |
|---|---|
| | • Bitrate (always 0 on an RSVP/DiffServ node)<br>• Policies. |
| RSVP | Aggregate information that includes the following:<br>• IP address of the aggregate source.<br>• IP address of the aggregate destination.<br>• DSCP.<br>**Note** The remaining fields describe the aggregate's E2E reservations with values explained in preceding fields. |
| VRF | Name of the VRF. |

## Related Commands

| Command | Description |
|---|---|
| **ip rtp compression-connections** | Specifies the total number of RTP header compression connections that can exist on an interface. |
| **show ip rsvp interface** | Displays RSVP-related information. |
| **show queueing interface** | Displays interface queueing statistics for dataplane information. |

# show ip rsvp interface

To display information related to Resource Reservation Protocol (RSVP), use the **show ip rsvp interface** command in user EXEC or privileged EXEC mode.

**show ip rsvp interface** [**vrf** {*****| *vrf-name*}] **[detail]** [*interface-type interface-number*]

## Syntax Description

| | |
|---|---|
| **vrf *** | (Optional) Displays all the configured virtual routing and forwarding (VRF) instances. |
| **vrf** *vrf-name* | (Optional) Displays the specified VRF. |
| **detail** | (Optional) Displays additional information about interfaces. |
| *interface-type* | (Optional) Type of the interface. |
| *interface-number* | (Optional) Number of the interface. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.2(2)T | This command was modified. The **detail** keyword was added. |
| 12.2(4)T | This command was modified. This command was implemented on the Cisco 7500 series and the ATM permanent virtual circuit (PVC) interface. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(13)T | This command was modified. The following changes were made to this command:<br>• Rate-limiting and refresh-reduction information was added to the output display.<br>• RSVP global settings display when no keywords or arguments are entered. |

| Release | Modification |
|---|---|
| 12.2(15)T | This command was modified. The following modifications were made to this command:<br>• The effects of compression on admission control and the RSVP bandwidth limit counter were added to the display.<br>• Cryptographic authentication parameters were added to the display. |
| 12.2(18)SFX2 | This command was integrated into Cisco IOS Release 12.2(18)SFX2. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SRB | This command was modified. The command output was enhanced to display fast local repair (FLR) information. |
| 12.2(33)SRC | This command was modified. The command output was enhanced to display RSVP aggregation information. |
| 12.4(20)T | This command was modified. The command output was enhanced to display the RSVP source address configured on a specified interface. |
| 15.0(1)M | This command was modified. The **vrf** and *keywords and the *vrf-name* argument were added. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |
| 15.1(3)S1 | This command was modified. The **show ip rsvp interface** command output was enhanced to display the RSVP status configured on all the interfaces. |

## Usage Guidelines

Use the**show ip rsvp interface** command to display information about interfaces on which RSVP is enabled, including the current allocation budget and maximum available bandwidth. Enter the optional **detail**keyword for additional information, including bandwidth and signaling parameters and blockade state.

Use the **show ip rsvp interface detail** command to display information about the RSVP parameters associated with an interface. These parameters include the following:

- Total RSVP bandwidth.
- RSVP bandwidth allocated to existing flows.
- Maximum RSVP bandwidth that can be allocated to a single flow.
- The type of admission control supported (header compression methods).
- The compression methods supported by RSVP compression prediction.
- RSVP aggregation.
- The RSVP source address.

- VRFs.

## Examples

This section provides sample output from **show ip rsvp interface**commands. Depending upon the interface or platform in use and the options enabled, the output that you see may vary slightly from the examples shown below.

## Examples

The following sample output from the **show ip rsvp interface** command shows information for each interface on which RSVP is enabled:

```
Router# show ip rsvp interface
interface    rsvp       allocated  i/f max  flow max sub max  VRF
Et0/0        ena        300K       1M       1M       0
Et0/1        ena        100K       1M       1M       0
Et1/0        ena        200K       1M       1M       0
Et1/1        ena        0          1M       1M       0
Et1/2        ena        0          1M       1M       0
```

The table below describes the fields shown in the display.

***Table 127: show ip rsvp interface Field Descriptions***

| Field | Description |
|---|---|
| interface | Interface name. |
| rsvp | Status of RSVP. Indicates if enabled or disabled. |
| allocated | Current allocation budget. |
| i/f max | Maximum allocatable bandwidth. |
| flow max | Largest single flow allocatable on this interface. |
| sub max | Largest subpool value allowed on this interface. |

## Examples

The following sample output from the **show ip rsvp interfacedetail** command shows detailed RSVP information for each interface on which RSVP is enabled:

```
Router# show ip rsvp interface detail
PO0/0:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):200M bits/sec
     Max. allowed (per flow):200M bits/sec
     Max. allowed for LSP tunnels using sub-pools:0 bits/sec
     Set aside by policy (total):0 bits/sec
   Signalling:
     DSCP value used in RSVP msgs:0x3F
     Number of refresh intervals to enforce blockade state:4
     Number of missed refresh messages:4
     Refresh interval:30
 PO1/0:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):50M bits/sec
```

```
     Max. allowed (per flow):50M bits/sec
     Max. allowed for LSP tunnels using sub-pools:0 bits/sec
     Set aside by policy (total):0 bits/sec
   Signalling:
     DSCP value used in RSVP msgs:0x3F
     Number of refresh intervals to enforce blockade state:4
     Number of missed refresh messages:4
     Refresh interval:30
PO1/1:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):50M bits/sec
     Max. allowed (per flow):50M bits/sec
     Max. allowed for LSP tunnels using sub-pools:0 bits/sec
     Set aside by policy (total):0 bits/sec
   Signalling:
     DSCP value used in RSVP msgs:0x3F
     Number of refresh intervals to enforce blockade state:4
     Number of missed refresh messages:4
     Refresh interval:30
 PO1/2:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):50M bits/sec
     Max. allowed (per flow):50M bits/secMax. allowed for LSP tunnels using sub-pools:0
bits/sec
     Set aside by policy (total):0 bits/sec
   Signalling:
     DSCP value used in RSVP msgs:0x3F
     Number of refresh intervals to enforce blockade state:4
     Number of missed refresh messages:4
     Refresh interval:30
 PO1/3:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):50M bits/sec
     Max. allowed (per flow):50M bits/sec
     Max. allowed for LSP tunnels using sub-pools:0 bits/sec
     Set aside by policy (total):0 bits/sec
   Signalling:
     DSCP value used in RSVP msgs:0x3F
     Number of refresh intervals to enforce blockade state:4
     Number of missed refresh messages:4
     Refresh interval:30
 Lo0:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):200M bits/sec
     Max. allowed (per flow):200M bits/sec
     Max. allowed for LSP tunnels using sub-pools:0 bits/sec
     Set aside by policy (total):0 bits/sec
   Signalling:
     DSCP value used in RSVP msgs:0x3F
     Number of refresh intervals to enforce blockade state:4
     Number of missed refresh messages:4
     Refresh interval:30
```

The table below describes the significant fields shown in the detailed display for PO interface 0/0. The fields for the other interfaces are similar.

***Table 128: show ip rsvp interface detail Field Descriptions--Detailed RSVP Information Example***

| Field | Description |
|---|---|
| PO0/0 | Interface name. |

| Field | Description |
|---|---|
| Bandwidth | The RSVP bandwidth parameters in effect are as follows:<br>• Curr allocated--Amount of bandwidth currently allocated, in bits per second.<br>• Max. allowed (total)--Maximum amount of bandwidth allowed, in bits per second.<br>• Max. allowed (per flow)--Maximum amount of bandwidth allowed per flow, in bits per second.<br>• Max. allowed for LSP tunnels using sub-pools--Maximum amount of bandwidth allowed for label switched path (LSP) tunnels, in bits per second.<br>• Set aside by policy (total)--The amount of bandwidth set aside by the local policy, in bits per second. |
| Signalling | The RSVP signalling parameters in effect are as follows:<br>• DSCP value used in RSVP msgs--Differentiated services code point (DSCP) used in RSVP messages.<br>• Number of refresh intervals to enforce blockade state--How long, in milliseconds, before the blockade takes effect.<br>• Number of missed refresh messages--How many refresh messages until the router state expires.<br>• Refresh interval--How long, in milliseconds, until a refresh message is sent. |

## Examples

The following sample output from the **show ip rsvp interface detail** command shows the RSVP compression method prediction configuration for each interface on which RSVP is configured:

```
Router# show ip rsvp interface detail
 Et2/1:
   Bandwidth:
     Curr allocated:0 bits/sec
     Max. allowed (total):1158K bits/sec
     Max. allowed (per flow):128K bits/sec
     Max. allowed for LSP tunnels using sub-pools:0 bits/sec
     Set aside by policy (total):0 bits/sec
   Admission Control:
     Header Compression methods supported:
       rtp (36 bytes-saved), udp (20 bytes-saved)
   Neighbors:
```

```
    Using IP encap:0.  Using UDP encap:0
  Signalling:
    Refresh reduction:disabled
  Authentication:disabled
Se3/0:
  Bandwidth:
    Curr allocated:0 bits/sec
    Max. allowed (total):1158K bits/sec
    Max. allowed (per flow):128K bits/sec
    Max. allowed for LSP tunnels using sub-pools:0 bits/sec
    Set aside by policy (total):0 bits/sec
  Admission Control:
    Header Compression methods supported:
      rtp (36 bytes-saved), udp (20 bytes-saved)
  Neighbors:
    Using IP encap:1.  Using UDP encap:0
  Signalling:
    Refresh reduction:disabled
  Authentication:disabled
```

The table below describes the significant fields shown in the display for Ethernet interface 2/1. The fields for serial interface 3/0 are similar.

***Table 129: show ip rsvp interface detail Field Descriptions--RSVP Compression Method Prediction Example***

| Field | Description |
|---|---|
| Et2/1 | Interface name and number. |
| Bandwidth | The RSVP bandwidth parameters in effect are as follows:<br>• Curr allocated--Amount of bandwidth currently allocated, in bits per second.<br>• Max. allowed (total)--Maximum amount of bandwidth allowed, in bits per second.<br>• Max. allowed (per flow)--Maximum amount of bandwidth allowed per flow, in bits per second.<br>• Max. allowed for LSP tunnels using sub-pools--Maximum amount of bandwidth allowed for LSP tunnels, in bits per second.<br>• Set aside by policy (total)--The amount of bandwidth set aside by the local policy, in bits per second. |
| Admission Control | The type of admission control in effect is as follows:<br>• Header Compression methods supported:<br>• Real-Time Transport Protocol (RTP) or User Data Protocol (UDP) compression schemes and the number of bytes saved per packet. |

| Field | Description |
|---|---|
| Neighbors | The number of neighbors using IP and UDP encapsulation. |
| Signalling | The type of signaling in effect; refresh reduction is either enabled (active) or disabled (inactive). |
| Authentication | Authentication is either enabled (active) or disabled (inactive). |

## Examples

The following sample output from the **show ip rsvp interface detail**command displays detailed information, including the cryptographic authentication parameters, for all RSVP-configured interfaces on the router:

```
Router# show ip rsvp interface detail
 Et0/0:
   Bandwidth:
    Curr allocated: 0 bits/sec
    Max. allowed (total): 7500K bits/sec
    Max. allowed (per flow): 7500K bits/sec
    Max. allowed for LSP tunnels using sub-pools: 0 bits/sec
    Set aside by policy (total):0 bits/sec
   Neighbors:
    Using IP encap: 0.  Using UDP encap: 0
   Signalling:
    Refresh reduction: disabled
   Authentication: enabled
    Key:           11223344
    Type:          sha-1
    Window size:   2
    Challenge:     enabled
```

The table below describes the significant fields shown in the display.

***Table 130: show ip rsvp interface detail Field Descriptions--Cryptographic Authentication Example***

| Field | Description |
|---|---|
| Et0/0 | Interface name and number. |

| Field | Description |
|---|---|
| Bandwidth | The RSVP bandwidth parameters in effect are as follows:<br>• Curr allocated--Amount of bandwidth currently allocated, in bits per second.<br>• Max. allowed (total)--Maximum amount of bandwidth allowed, in bits per second.<br>• Max. allowed (per flow)--Maximum amount of bandwidth allowed per flow, in bits per second.<br>• Max. allowed for LSP tunnels using sub-pools--Maximum amount of bandwidth allowed for LSP tunnels, in bits per second.<br>• Set aside by policy (total)--The amount of bandwidth set aside by the local policy, in bits per second. |
| Neighbors | The number of neighbors using IP and UDP encapsulation. |
| Signalling | The type of signaling in effect; Refresh reduction is either enabled (active) or disabled (inactive). |
| Authentication | Authentication is either enabled (active) or disabled (inactive). The parameters are as follows:<br>• Key--The key (string) for the RSVP authentication algorithm displayed in clear text (for example, 11223344) or <encrypted>.<br>• Type--The algorithm to generate cryptographic signatures in RSVP messages; possible values are md5 and sha-1.<br>• Window size--Maximum number of RSVP authenticated messages that can be received out of order.<br>• Challenge--The challenge-response handshake performed with any new RSVP neighbors that are discovered on a network; possible values are enabled (active) or disabled (inactive). |

## Examples

The following sample output from the **show ip rsvp interface detail** command displays detailed information for the Ethernet 1/0 interface on which FLR is enabled:

```
Router# show ip rsvp interface detail ethernet1/0
```

```
Et1/0:
  RSVP: Enabled
  Interface State: Up
  Bandwidth:
    Curr allocated: 9K bits/sec
    Max. allowed (total): 300K bits/sec
    Max. allowed (per flow): 300K bits/sec
    Max. allowed for LSP tunnels using sub-pools (pool 1): 0 bits/sec
    Set aside by policy (total): 0 bits/sec
  Traffic Control:
    RSVP Data Packet Classification is ON via CEF callbacks
  Signalling:
    DSCP value used in RSVP msgs: 0x30
    Number of refresh intervals to enforce blockade state: 4
  FLR Wait Time (IPv4 flows):
    Repair is delayed by 500 msec.
  Authentication: disabled
    Key chain:   <none>
    Type:        md5
    Window size: 1
    Challenge:   disabled
  Hello Extension:
    State: Disabled
```

The table below describes the significant fields shown in the display.

***Table 131: show ip rsvp interface detail Field Descriptions--FLR Example***

| Field | Description |
|---|---|
| Et1/0 | Interface name and number. |
| RSVP | Enabled means active; disabled means inactive. |
| Interface State | Up means that the interface is configured; down means that the interface is not configured. |
| Bandwidth | The RSVP bandwidth parameters in effect are as follows:<br>• Curr allocated--Amount of bandwidth currently allocated, in bits per second.<br>• Max. allowed (total)--Maximum amount of bandwidth allowed, in bits per second.<br>• Max. allowed (per flow)--Maximum amount of bandwidth allowed per flow, in bits per second.<br>• Max. allowed for LSP tunnels using sub-pools--Maximum amount of bandwidth allowed for LSP tunnels, in bits per second.<br>• Set aside by policy (total)--The amount of bandwidth set aside by the local policy, in bits per second. |
| Traffic Control | RSVP Data Packet Classification is ON via CEF callbacks means that RSVP is not processing every packet; therefore, excess overhead is avoided and network performance is improved. |

| Field | Description |
|---|---|
| Signalling | The signaling parameters in effect are as follows:<br>• DSCP value used in RSVP msgs--Differentiated services code point (DSCP) value used in RSVP messages.<br>• Number of refresh intervals to enforce blockade state--How long, in milliseconds, before the blockade takes effect. |
| FLR Wait Time (IPv4 flows) | Repair is delayed by 500 msec represents the amount of time, in milliseconds, before the FLR procedure begins on the specified interface. |
| Authentication | Authentication is either enabled (active) or disabled (inactive). The parameters are as follows:<br>• Key chain--The key (string) for the RSVP authentication algorithm displayed in clear text (for example, 11223344) or <encrypted>.<br>• Type--The algorithm to generate cryptographic signatures in RSVP messages; possible values are md5 and sha-1.<br>• Window size--Maximum number of RSVP authenticated messages that can be received out of order.<br>• Challenge--The challenge-response handshake performed with any new RSVP neighbors that are discovered on a network; possible values are enabled (active) or disabled (inactive). |
| Hello Extension | Enables RSVP nodes to detect when a neighboring node is not reachable. The state is either enabled (active) or disabled (inactive). |

## Examples

The following sample output from the **show ip rsvp interface detail** command displays the aggregation parameters for each interface on which RSVP is configured:

```
Router# show ip rsvp interface detail
Se1/0:
   RSVP: Enabled
   Interface State: Up
   Bandwidth:
     Curr allocated: 300K bits/sec
     Max. allowed (total): 400K bits/sec
     Max. allowed (per flow): 400K bits/sec
     Max. allowed for LSP tunnels using sub-pools (pool 1): 0 bits/sec
     Set aside by policy (total): 0 bits/sec
```

```
Traffic Control:
  RSVP Data Packet Classification is OFF
  RSVP resource provider is: none
Signalling:
  DSCP value used in RSVP msgs: 0x3F
  Number of refresh intervals to enforce blockade state: 4
Authentication: disabled
  Key chain:   <none>
  Type:        md5
  Window size: 1
  Challenge:   disabled
FRR Extension:
  Backup Path: Not Configured
BFD Extension:
  State: Disabled
  Interval: Not Configured
RSVP Hello Extension:
  State: Disabled
RFC 3175 Aggregation: Enabled
  Role: interior
```

The table below describes the significant fields shown in the display.

***Table 132: show ip rsvp interface detail Field Descriptions--RSVP Aggregation Example***

| Field | Description |
|---|---|
| Se1/0 | Interface name and number. |
| RSVP | Enabled means active; disabled means inactive. |
| Interface State | Up means that the interface is configured; down means that the interface is not configured. |
| Bandwidth | The RSVP bandwidth parameters in effect are as follows:<br>• Curr allocated--Amount of bandwidth currently allocated, in bits per second.<br>• Max. allowed (total)--Maximum amount of bandwidth allowed, in bits per second.<br>• Max. allowed (per flow)--Maximum amount of bandwidth allowed per flow, in bits per second.<br>• Max. allowed for LSP tunnels using sub-pools--Maximum amount of bandwidth allowed for LSP tunnels, in bits per second.<br>• Set aside by policy (total)--The amount of bandwidth set aside by the local policy, in bits per second. |

| Field | Description |
|---|---|
| Traffic Control | RSVP Data Packet Classification Is OFF--Disabling data packet classification instructs RSVP not to process every packet, but to perform admission control only.<br>RSVP Resource Provider is None--Setting the resource provider to **none** instructs RSVP to not associate any resources, such as weighted fair queueing (WFQ) queues or bandwidth, with a reservation.<br>These settings are necessary because RSVP aggregation uses RSVP Scalability Enhancements for control plane aggregation only. Traffic control is performed by Class-Based Weighted Fair Queuing (CBWFQ). |
| Signalling | The signaling parameters in effect are as follows:<br>• DSCP value used in RSVP msgs--Differentiated services code point (DSCP) value used in RSVP messages IP headers.<br>• Number of refresh intervals to enforce blockade state--How long, in milliseconds, before the blockade takes effect. |
| Authentication | Authentication is either enabled (active) or disabled (inactive). The parameters are as follows:<br>• Key chain--The key (string) for the RSVP authentication algorithm displayed in clear text (for example, 11223344) or <encrypted>.<br>• Type--The algorithm to generate cryptographic signatures in RSVP messages; possible values are md5 and sha-1.<br>• Window size--Maximum number of RSVP authenticated messages that can be received out of order.<br>• Challenge--The challenge-response handshake performed with any new RSVP neighbors that are discovered on a network; possible values are enabled (active) or disabled (inactive). |
| FRR Extension | Fast Reroute backup path is configured or not configured. |

| Field | Description |
|---|---|
| BFD Extension | Bidirectional Forwarding Detection; values are the following:<br>• State--Enabled (active) or disabled (inactive).<br>• Interval--Configured with a value or Not Configured. |
| RSVP Hello Extension | Enables RSVP nodes to detect when a neighboring node is not reachable. The state is either enabled (active) or disabled (inactive). |
| RFC 3175 Aggregation | The state of aggregation as defined in RFC 3175, *AggregationofRSVPforIPv4andIPv6Reservations*; values are the following:<br>• Enabled--Active.<br>• Disabled--Inactive.<br>Role<br>• Interior--Interface is facing an aggregation region.<br>• Exterior--Interface is facing a classic RSVP region. |

## Examples

The following sample output from the **showiprsvpinterfacedetailethernet1/0** command displays the source address configured for that interface:

```
Router# show ip rsvp interface detail ethernet1/0
 Et1/0:
   RSVP: Enabled
   Interface State: Up
   Bandwidth:
     Curr allocated: 0 bits/sec
     Max. allowed (total): 7500K bits/sec
     Max. allowed (per flow): 7500K bits/sec
     Max. allowed for LSP tunnels using sub-pools (pool 1): 0 bits/sec
     Set aside by policy (total): 0 bits/sec
   Traffic Control:
     RSVP Data Packet Classification is ON via CEF callbacks
   Signalling:
     DSCP value used in RSVP msgs: 0x3F
     Number of refresh intervals to enforce blockade state: 4
     Ip address used in RSVP objects: 10.1.3.13 <----------source address for Ethernet 0/1
   Authentication: disabled
     Key chain:   <none>
     Type:        md5
     Window size: 1
     Challenge:   disabled
   Hello Extension:
     State: Disabled
```

The table below describes the significant fields shown in the display.

***Table 133: show ip rsvp interface detail Field Descriptions--RSVP Source Address Example***

| Field | Description |
|---|---|
| Et1/0 | Interface name and number. |
| RSVP | Enabled means active; disabled means inactive. |
| Interface State | Up means that the interface is configured; down means that the interface is not configured. |
| Bandwidth | The RSVP bandwidth parameters in effect are as follows:<br>• Curr allocated--Amount of bandwidth currently allocated, in bits per second.<br>• Max. allowed (total)--Maximum amount of bandwidth allowed, in bits per second.<br>• Max. allowed (per flow)--Maximum amount of bandwidth allowed per flow, in bits per second.<br>• Max. allowed for LSP tunnels using sub-pools--Maximum amount of bandwidth allowed for LSP tunnels, in bits per second.<br>• Set aside by policy (total)--The amount of bandwidth set aside by the local policy, in bits per second. |
| Traffic Control | RSVP Data Packet Classification is ON via CEF callbacks means that RSVP is not processing every packet; therefore, excess overhead is avoided and network performance is improved. |
| Signalling | The signaling parameters in effect are as follows:<br>• DSCP value used in RSVP msgs--Differentiated services code point (DSCP) value used in IP headers of RSVP messages.<br>• Number of refresh intervals to enforce blockade state--How long, in milliseconds, before the blockade takes effect.<br>• IP address used in RSVP objects--The RSVP source address for the specified interface. |

| Field | Description |
|---|---|
| Authentication | Authentication is either enabled (active) or disabled (inactive). The parameters are as follows:<br>• Key chain--The key (string) for the RSVP authentication algorithm displayed in clear text (for example, 11223344) or <encrypted>.<br>• Type--The algorithm to generate cryptographic signatures in RSVP messages; possible values are md5 and sha-1.<br>• Window size--Maximum number of RSVP authenticated messages that can be received out of order.<br>• Challenge--The challenge-response handshake performed with any new RSVP neighbors that are discovered on a network; possible values are enabled (active) or disabled (inactive). |
| Hello Extension | Enables RSVP nodes to detect when a neighboring node is not reachable. The state is either enabled (active) or disabled (inactive). |

## Examples

The following sample output from the **show ip rsvp interface vrf my vrf detail** command displays information for all the interfaces associated with the VRF named myvrf:

```
Router# show ip rsvp interface vrf myvrf detail
Se1/0:
   RSVP: Enabled
   Interface State: Up
   Bandwidth:
     Curr allocated: 300K bits/sec
     Max. allowed (total): 400K bits/sec
     Max. allowed (per flow): 400K bits/sec
     Max. allowed for LSP tunnels using sub-pools (pool 1): 0 bits/sec
     Set aside by policy (total): 0 bits/sec
   Traffic Control:
     RSVP Data Packet Classification is OFF
     RSVP resource provider is: none
   Signalling:
     DSCP value used in RSVP msgs: 0x3F
     Number of refresh intervals to enforce blockade state: 4
   Authentication: disabled
     Key chain:   <none>
     Type:        md5
     Window size: 1
     Challenge:   disabled
   FRR Extension:
     Backup Path: Not Configured
   BFD Extension:
     State: Disabled
     Interval: Not Configured
   RSVP Hello Extension:
     State: Disabled
   RFC 3175 Aggregation: Enabled
```

```
    Role: interior
VRF: myvrf
```

The table below describes the significant fields shown in the display.

***Table 134: show ip rsvp interface detail Field Descriptions--RSVP VRF Example***

| Field | Description |
|---|---|
| Se1/0 | Interface name and number. |
| RSVP | Enabled means active; disabled means inactive. |
| Interface State | Up means that the interface is configured; down means that the interface is not configured. |
| Bandwidth | The RSVP bandwidth parameters in effect are as follows:<br>• Curr allocated--Amount of bandwidth currently allocated, in bits per second.<br>• Max. allowed (total)--Maximum amount of bandwidth allowed, in bits per second.<br>• Max. allowed (per flow)--Maximum amount of bandwidth allowed per flow, in bits per second.<br>• Max. allowed for LSP tunnels using sub-pools--Maximum amount of bandwidth allowed for LSP tunnels, in bits per second.<br>• Set aside by policy (total)--The amount of bandwidth set aside by the local policy, in bits per second. |
| Traffic Control | RSVP Data Packet Classification Is OFF--Disabling data packet classification instructs RSVP not to process every packet, but to perform admission control only.<br>RSVP Resource Provider is None--Setting the resource provider to **none** instructs RSVP to not associate any resources, such as weighted fair queueing (WFQ) queues or bandwidth, with a reservation.<br>These settings are necessary because RSVP aggregation uses RSVP Scalability Enhancements for control plane aggregation only. Traffic control is performed by Class-Based Weighted Fair Queuing (CBWFQ). |

| Field | Description |
|---|---|
| Signalling | The signaling parameters in effect are as follows:<br>• DSCP value used in RSVP msgs--Differentiated services code point (DSCP) value used in RSVP messages IP headers.<br>• Number of refresh intervals to enforce blockade state--How long, in milliseconds, before the blockade takes effect. |
| Authentication | Authentication is either enabled (active) or disabled (inactive). The parameters are as follows:<br>• Key chain--The key (string) for the RSVP authentication algorithm displayed in clear text (for example, 11223344) or <encrypted>.<br>• Type--The algorithm to generate cryptographic signatures in RSVP messages; possible values are md5 and sha-1.<br>• Window size--Maximum number of RSVP authenticated messages that can be received out of order.<br>• Challenge--The challenge-response handshake performed with any new RSVP neighbors that are discovered on a network; possible values are enabled (active) or disabled (inactive). |
| FRR Extension | Fast Reroute backup path is configured or not configured. |
| BFD Extension | Bidirectional Forwarding Detection; values are the following:<br>• State--Enabled (active) or disabled (inactive).<br>• Interval--Configured with a value or Not Configured. |
| RSVP Hello Extension | Enables RSVP nodes to detect when a neighboring node is not reachable. The state is either enabled (active) or disabled (inactive). |

| Field | Description |
|---|---|
| RFC 3175 Aggregation | The state of aggregation as defined in RFC 3175, *AggregationofRSVPforIPv4andIPv6Reservations*; values are the following:<br>• Enabled--Active.<br>• Disabled--Inactive.<br>Role<br>• Interior--Interface is facing an aggregation region.<br>• Exterior--Interface is facing a classic RSVP region. |
| VRF | Name of the VRF. |

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp installed** | Displays RSVP-related installed filters and corresponding bandwidth information. |
| **show ip rsvp neighbor** | Displays current RSVP neighbors. |

# show ip rsvp interface detail

To display the hello configuration for all interface types, use the **show ip rsvp interface detail**command in user EXEC or privileged EXEC mode.

**show ip rsvp interface detail** [*type number*]

## Syntax Description

| | |
|---|---|
| *type number* | (Optional) The type and number of the interface for which you want to display the hello configuration. |

## Command Default

The hello configuration for all interfaces is displayed.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(22)S | This command was introduced. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |
| 12.2(33)SRE | This command was modified. The output was updated to display the source address used in the PHOP address field. |
| 15.1(2)T | This command was modified. The output was updated to display the overhead percent. |
| 15.1(1)S | This command was integrated into Cisco IOS Release 15.1(1)S. |
| 15.2(2)SNG | This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |

## Usage Guidelines

To display the hello configuration for a specific interface, use the **show ip rsvp interface detail** command with the *type* and *number* arguments.

## Examples

The following is sample output from the **show ip rsvp interface detail** command:

```
Router# show ip rsvp interface detail GigabitEthernet 9/47
Tu0:
   RSVP: Enabled
   Interface State: Up
   Bandwidth:
     Curr allocated: 10K bits/sec
     Max. allowed (total): 75K bits/sec
     Max. allowed (per flow): 75K bits/sec
     Max. allowed for LSP tunnels using sub-pools: 0 bits/sec
     Set aside by policy (total): 0 bits/sec
   Admission Control:
     Header Compression methods supported:
       rtp (36 bytes-saved), udp (20 bytes-saved)
     Tunnel IP Overhead percent:
       4
     Tunnel Bandwidth considered:
       Yes
   Traffic Control:
     RSVP Data Packet Classification is ON via CEF callbacks
   Signalling:
     DSCP value used in RSVP msgs: 0x3F
     Number of refresh intervals to enforce blockade state: 4
   Authentication: disabled
     Key chain:   <none>
     Type:        md5
     Window size: 1
     Challenge:   disabled
   Hello Extension:
     State: Disabled
```

The table below describes the significant fields shown in the display.

***Table 135: show ip rsvp interface detail Field Descriptions***

| Field | Description |
|---|---|
| RSVP | Status of the Resource Reservation Protocol (RSVP) (Enabled or Disabled). |
| Interface State | Status of the interface (Up or Down). |
| Curr allocated | Amount of bandwidth (in bits per second [b/s]) currently allocated. |
| Max. allowed (total) | Total maximum amount of bandwidth (in b/s) allowed. |
| Max. allowed (per flow) | Maximum amount of bandwidth (in b/s) allowed per flow. |
| Max. allowed for LSP tunnels using sub-pools | Maximum amount of bandwidth permitted for the label switched path (LSP) tunnels that obtain their bandwidth from subpools. |

| Field | Description |
|---|---|
| Tunnel IP Overhead percent | Overhead percent to override the RSVP bandwidth manually. |
| Tunnel Bandwidth considered | Indicates if the tunnel bandwidth is considered. |
| DSCP value used in RSVP msgs | Differentiated services code point (DSCP) value in the RSVP messages. |

# show ip rsvp listeners

To display the Resource Reservation Protocol (RSVP) listeners for a specified port or protocol, use the **showiprsvplisteners** command in user EXEC or privileged EXEC mode.

**show ip rsvp listeners** [*ip-address*| **any**| **vrf** {*****| *vrf-name*}] [**udp**| **tcp**| **any**| *protocol*] [*dst-port*| **any**]

## Syntax Description

| | |
|---|---|
| *ip-address* | (Optional) A particular IP address for an RSVP message. |
| **any** | (Optional) Any IP address destination for an RSVP message. |
| vrf * | (Optional) Displays all the configured virtual routing and forwarding (VRF) instances. |
| **vrf** *vrf-name* | (Optional) Displays information about a specified VRF. |
| **udp** | (Optional) User Datagram Protocol (UDP) to be used on the receiving interface and the UDP source port number. |
| **tcp** | (Optional) TCP to be used on the receiving interface and the TCP source port number. |
| **any** | (Optional) Any protocol to be used on the receiving interface and the UDP or TCP source port number. |
| *protocol* | (Optional) The protocol to be used on the receiving interface and the UDP or TCP source port number.<br>**Note** If you select the *protocol* argument, the range is from 0 to 255 and the protocol used is IP. |
| *dst-port* | (Optional) A particular destination port from 0 to 65535 for an RSVP message. |
| **any** | (Optional) Any destination for an RSVP message. |

## Command Default

If you enter the **showiprsvplisteners**command without a keyword or an argument, the command displays all the listeners that were sent and received for each interface on which RSVP is configured.

## Command Modes

User EXEC (<) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 15.0(1)M | This command was modified. The **vrf**and*keywords and the *vrf-name* argument were added. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelin

**Note** The syntax of the command depends on your platform and release. The **vrf**and * keywords and *vrf-name*argument are not supported on ASR 1000 Series Aggregation Services Routers.

Use the **showiprsvplisteners**command to display the number of listeners that were sent and received for each interface on which RSVP is configured.

## Examples

The following example shows the listeners for the VRF named myvrf1:

```
Router# show ip rsvp listeners vrf myvrf1
VRF : myvrf1
```

To Protocol DPort Description Action OutIf

10.0.2.1 any any RSVP Proxy reply

The table below describes the significant fields shown in the display.

***Table 136: show ip rsvp listeners Command Field Descriptions***

| Field | Description |
|---|---|
| VRF | Name of the VRF for which the listeners are displayed. |
| To | IP address of the receiving interface. |
| Protocol | Protocol used. |
| DPort | Destination port on the receiving router. |
| Description | Cisco IOS component that requested RSVP to do the listening; for example, RSVP proxy and label switched path (LSP) tunnel signaling. |

| Field | Description |
|---|---|
| Action | Action taken when a flow arrives at its destination. The values are:<br>• announce--The arrival of the flow is announced.<br>• reply--After the flow arrives at its destination, the sender receives a reply. |
| OutIf | Outbound interface on the receiving router.<br>**Note** If this field is blank, it means that the listener was configured in global configuration mode and is not attached to any particular interface. If an interface name appears, then the listener was configured in interface configuration mode and is attached to that interface. |

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp listener outbound** | Configures an RSVP router to listen for PATH messages sent through a specific interface. |

# show ip rsvp neighbor

To display current Resource Reservation Protocol (RSVP) neighbors, use the **showiprsvpneighbor**command in user EXEC or privileged EXEC mode.

**show ip rsvp neighbor** [**detail**| **inactive [detail]**| **vrf** {*****| *vrf-name*}]

## Syntax Description

| | |
|---|---|
| **detail** | (Optional) Displays additional information about RSVP neighbors. |
| inactive | (Optional) Displays RSVP neighbors that have had no activity for more than an hour. |
| **detail** | (Optional) Displays additional information about the inactive RSVP neighbors. |
| vrf * | (Optional) Displays all the configured virtual routing and forwarding (VRF) instances. |
| **vrf** *vrf-name* | (Optional) Name of a specified VRF. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.2(13)T | The *interface-typeinterface-number* arguments were deleted. The detail keyword was added to the command, and rate-limiting and refresh-reduction information was added to the output. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.0(1)M | This command was modified. The **vrf**and*****keywords and the *vrf-name* argument were added. |

## Usage Guidelines

Use the **showiprsvpneighbor** command to show the IP addresses for the current RSVP neighbors. Enter the **detail**keyword to display rate-limiting, refresh-reduction, and VRF information for the RSVP neighbors.

## Examples

## Examples

The following command shows the current RSVP neighbors:

```
Router# show ip rsvp neighbor
 10.0.0.1        RSVP
 10.0.0.2        RSVP
```

The table below describes the fields shown in the display.

***Table 137: show ip rsvp neighbor Field Descriptions***

| Field | Description |
|---|---|
| 10.0.0.1 | IP address of neighboring router. |
| RSVP | Type of encapsulation being used. |

## Examples

The following command shows the rate-limiting and refresh-reduction parameters for the current RSVP neighbors:

```
Router# show ip rsvp neighbor detail
Neighbor:10.0.0.1
    Encapsulation:RSVP
    Rate-Limiting:
      Dropped messages:0
Refresh Reduction:
      Remote epoch:0x1BFEA5
      Out of order messages:0
      Retransmitted messages:0
      Highest rcvd message id:1059
      Last rcvd message:00:00:04
Neighbor:10.0.0.2
    Encapsulation:RSVP
    Rate-Limiting:
      Dropped messages:0
    Refresh Reduction:
      Remote epoch:0xB26B1
      Out of order messages:0
      Retransmitted messages:0
      Highest rcvd message id:945
      Last rcvd message:00:00:05
```

The table below describes the fields shown in the display.

***Table 138: show ip rsvp neighbor detail Field Descriptions***

| Field | Description |
|---|---|
| Neighbor | IP address of the neighboring router. |

| Field | Description |
|---|---|
| Encapsulation | Type of encapsulation being used.<br>**Note** Unknown displays if an RSVP message has been sent to an IP address, but no RSVP message has been received from that IP address. This is not an error condition; it simply means that the router does not yet know what RSVP encapsulation (IP or User Data Protocol (UDP)) is preferred and should be used to send RSVP messages. |
| Rate-Limiting | The rate-limiting parameters in effect are as follows:<br>• Dropped messages = number of messages dropped by the neighbor. |
| Refresh Reduction | The refresh-reduction parameters in effect are as follows:<br>• Remote epoch = the RSVP message number space identifier (ID); randomly generated whenever the node reboots or the RSVP process restarts.<br>• Out of order messages = messages that were dropped because they are out of sequential order.<br>• Retransmitted messages = number of messages retransmitted to the neighbor.<br>• Highest rcvd message id = highest message ID number sent by the neighbor.<br>• Last rcvd message= time delta in hours, minutes, and seconds when last message was received by the neighbor. |

## Examples

The following command shows the VRF named myvrf:

```
Router# show ip rsvp neighbor vrf myvrf
VRF: myvrf
Neighbor        Encapsulation  Time since msg rcvd/sent
10.10.15.3         Raw IP         00:00:14   00:00:06
10.10.16.2         Raw IP         00:00:29   00:00:15
```

The table below describes the fields shown in the display.

*Table 139: show ip rsvp neighbor vrf Field Descriptions*

| Field | Description |
|---|---|
| VRF | Name of the VRF. |
| Neighbor | IP address of neighboring router. |
| Encapsulation | Type of encapsulation being used. |
| Time since msg rcvd/sent | Time in hh:mm:ss since a message has been received by or sent to the neighbor. |

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp interface** | Displays RSVP-related interface information. |

# show ip rsvp p2mp counters

To display any errors associated with the configuration and operation of Multiprotocol Label Switching (MPLS) traffic engineering (TE) point-to-multipoint (P2MP) sublabel switched paths (sub-LSPs), use the **showiprsvpp2mpcounters**command in in user EXEC or privileged EXEC mode.

**show ip rsvp p2mp counters**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRE | This command was introduced. |

## Examples

The following example shows the error counters for MPLS TE P2MP sub-LSPs:

```
Router# show ip rsvp p2mp counters
RSVP P2MP Error counters
Missing S2L_SUB_LSP object: 1
Multiple S2L_SUB_LSP objects: 1
Session's required bits are not zero: 1
Signalling attributes inconsistent: 1
IP header's destination is different from S2L_SUB_LSP destination: 1
Failed to enqueue S2L_SUB_LSP object into tmb: 1
Illegal Resv style: 1
```

The table below describes the significant fields shown in the display.

***Table 140: show ip rsvp p2mp counters Field Descriptions***

| Field | Description |
|---|---|
| Missing S2L_SUB_LSP object | The S2L_SUB_LSP object includes the sub-LSP destination. If the S2L_SUB_LSP object is not available, it causes an error, which is counted in this field. |
| Multiple S2L_SUB_LSP objects | The S2L_SUB_LSP object includes the sub-LSP destination. If there are multiple S2L_SUB_LSP objects, it causes an error, which is counted in this field. |
| Session's required bits are not zero | Session object protocol field should be zero. If it is not, it causes an error, which is counted in this field. |

| Field | Description |
|---|---|
| Signalling attributes inconsistent | When a router signals a P2MP LSP, all sub-LSPs should signal the same attributes. If they do not, it causes an error, which is counted in this field. |
| IP header's destination is different from S2L_SUB_LSP destination | When a path has an IP header destination address that is different from the S2L_SUB_LSP object address, the destination address in the IP header is ignored, and the destination address in the S2L_SUB_LSP object is used. If the destination address in the path is one of its own addresses, Resource Reservation Protocol (RSVP) terminates the path. The event is counted in this field. |
| Failed to enqueue S2L_SUB_LSP object into tmb | If the sub-LSP is not sent to the Timer Management block (TMB), it causes an error, which is counted in this field. |
| Illegal Resv style | The reservation style in all P2MP Resv messages is shared explicit (SE). If a different reservation is used, it causes an error, which is counted in this field. |

## Related Commands

| Command | Description |
|---|---|
| **show mpls traffic-eng forwarding statistics** | Displays informtion about MPLS TE P2MP paths and sub-LSPs. |

# show ip rsvp policy

To display the policies currently configured, use the **showiprsvppolicy** command in user EXEC or privileged mode.

**show ip rsvp policy** [**cops**| **local** [ *acl* ]]

## Syntax Description

| | |
|---|---|
| **cops** \| **local** | (Optional) Displays either the configured Common Open Policy Service (COPS) servers or the local policies. |
| *acl* | (Optional) Displays the access control lists (ACLs) whose sessions are governed by COPS servers or the local policies. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.1(1)T | This command was introduced as **showiprsvppolicycops**. |
| 12.2(13)T | This command was modified to include the **localkeyword**. This command replaces the **showiprsvppolicycops** command. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **showiprsvppolicy**command to display current local policies, configured COPS servers, default policies, and the preemption parameter (disabled or enabled).

## Examples

The following is sample output from the **showiprsvppolicy**command :

```
Router# show ip rsvp policy
Local policy:
    A=Accept    F=Forward
    Path:-- Resv:-- PathErr:-- ResvErr:-- ACL:104
    Path:-- Resv:-- PathErr:-- ResvErr:-- ACL:None [Default policy]
COPS:
Generic policy settings:
    Default policy: Accept all
    Preemption:     Disabled
```

The table below describes the fields shown in the display.

*Table 141: show ip rsvp policy Command Field Descriptions*

| Field | Description |
|---|---|
| Local policy | The local policy currently configured.<br>A = Accept the message.<br>F = Forward the message.<br>Blank (--) means messages of the specified type are neither accepted or forwarded. |
| COPS | The COPS servers currently in effect. |
| Generic policy settings | Policy settings that are not specific to COPS or the local policy.<br>Default policy: Accept all means all RSVP messages are accepted and forwarded. Reject all means all RSVP messages are rejected.<br>Preemption: Disabled means that RSVP should not implement any preemption decisions required by a particular local or remote policy. Enabled means that RSVP should implement any preemption decisions required by a particular local or remote policy. |

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling initial-retransmit-delay** | Creates a local procedure that determines the use of RSVP resources in a network. |

# show ip rsvp policy cops

The **showiprsvppolicycops** command is replaced by the **showiprsvppolicy**command. See the **showiprsvppolicy** command for more information.

# show ip rsvp policy identity

To display selected Resource Reservation Protocol (RSVP) identities in a router configuration, use the **showiprsvppolicyidentity**command in user EXEC or privileged EXEC mode.

**show ip rsvp policy identity** [ *regular-expression* ]

## Syntax Description

| | |
|---|---|
| *regular-expression* | (Optional) String of text that allows pattern matching on the alias strings of the RSVP identities to be displayed. |

## Command Default

All configured RSVP identities are displayed.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(6)T | This command was introduced. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

Use the**showiprsvppolicyidentity** command with the optional *regular-expression* argument to perform pattern matching on the alias strings of the RSVP identities to be displayed. Use this filtering capability to search for a small subset of RSVP identities in a configuration with a large number of identities.

Omit the *regular-expression* argument to display all the configured identities.

## Examples

The following sample output from the **showiprsvppolicyidentity** command displays all the configured identities:

```
Router# show ip rsvp policy identity
Alias: voice1
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=1.0
Alias: voice10
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=10.0
Alias: voice100
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=100.0
Alias: voice1000
```

```
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=1000.0
```

The table below describes the significant fields shown in the display.

***Table 142: show ip rsvp policy identity Field Descriptions***

| Field | Description |
|---|---|
| Alias | Name of the alias string. The string can have as many as 64 printable characters (in the range 0x20 to 0x7E).<br>The string has no maximum length and must contain printable characters (in the range 0x20 to 0x7E).<br>**Note** If you use the " " or ? character as part of the string itself, you must type the CTRL-V key sequence before entering the embedded " " or ? character. The alias is never transmitted to other routers. |
| Type | Types of identities. RSVP defines two types: application IDs (Application) and user IDs (User). Cisco IOS software and Cisco IOS XE software support application IDs only. |
| Locator | Information used by a router to find the correct policy to apply to RSVP messages that contain application IDs. |

The following sample output from the **showiprsvppolicyidentity**command displays all the identities whose aliases contain voice100:

```
Router# show ip rsvp policy identity voice100
Alias: voice100
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=100.0
Alias: voice1000
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=1000.0
```

The following sample output from the **showiprsvppolicyidentity**command displays all the identities whose aliases contain an exact match on voice100:

```
Router# show ip rsvp policy identity ^voice100$
Alias: voice100
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=100.0
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp listener** | Configures an RSVP router to listen for PATH messages. |
| **ip rsvp policy identity** | Defines RSVP application IDs. |

| Command | Description |
|---|---|
| **ip rsvp policy local** | Determines how to perform authorization on RSVP requests. |
| **ip rsvp reservation** | Enables a router to simulate receiving RSVP RESV messages. |
| **ip rsvp sender** | Enables a router to simulate receiving RSVP PATH messages. |

# show ip rsvp policy local

To display the local policies that are currently configured, use the **showiprsvppolicylocal** command in user EXEC or privileged EXEC mode.

**show ip rsvp policy local [detail]** [**interface** *type number*] [**acl** *acl-number*| **dscp-ip** *value*| **default**| **identity** *alias*| **origin-as** *as*]

## Syntax Description

| | |
|---|---|
| **detail** | (Optional) Displays additional information about the configured local policies including preempt-priority and local-override. |
| interface *typenumber* | (Optional) Specifies an interface. |
| **acl** *acl-number* | (Optional) Specifies an Access Control List (ACL). Range is from 1 to 199. |
| **dscp-ip** *value* | (Optional) Specifies a differentiated services code point (DSCP) for aggregate reservations. Values can be the following:<br>• 0 to 63--Numerical DSCP values. The default value is 0.<br>• af11 to af43--Assured forwarding (AF) DSCP values.<br>• cs1 to cs7--Type of service (ToS) precedence values.<br>• default--Default DSCP value.<br>• ef--Expedited forwarding (EF) DSCP values. |
| **default** | (Optional) Displays information about the default policy. |
| **identity** *alias* | (Optional) Specifies an application identity (ID) alias. |
| origin-as *as* | (Optional) Specifies an autonomous system. Values are 1 to 65535. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.0(29)S | This command was modified. The **origin-as***as* keyword and argument combination was added, and the *acl-number*argument became optional. |
| 12.4(6)T | This command was modified. The **identity***alias*and the **interface***typenumber*keyword and argument combinations were added, and the output was modified to include application ID information. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.2(33)SRC | This command was modified. The **dscp-ip***value*keyword and argument combination was added, and the output was modified to include RSVP aggregation information. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

Use the **showiprsvppolicylocal** command to display information about the selected local policies that are currently configured. You can use the **default** keyword or the **interface***typenumber* keyword and argument combination with one or more of the match criteria.

If you omit **acl***acl-number,*the**origin-as***as,*the**identity***alias,orthe***dscp-ip***value*keyword and argument combinations, all local policies currently configured appear.

You can specify only one of the ACL, the autonomous system, the application ID, or the DSCP options as a match criterion. However, that parameter can be any ACL, autonomous system, application ID, or DSCP of any local policy that you have created. If you have multiple local policies with a common match criterion, using that parameter displays all local policies that meet the match criterion. If you have created local policies each with multiple ACLs, autonomous systems, application IDs, or DSCPs as the match criteria, you cannot use that parameter to show only a specific policy. You must omit the match criteria and show all the local policies.

## Examples

## Examples

The following sample output from the **showiprsvppolicylocal**command**displays**global and per-interface local policies based on RSVP identities (application IDs) that have been configured :

```
Router# show ip rsvp policy local
  A=Accept    F=Forward
  Global:
    Path:AF Resv:AF PathErr:AF ResvErr:AF ACL(s):101
    Path:AF Resv:AF PathErr:AF ResvErr:AF AS(es):3
    Path:AF Resv:AF PathErr:AF ResvErr:AF ID:voice
```

```
    Path:AF Resv:AF PathErr:AF ResvErr:AF ID:video

  Serial2/0/0:
    Path:AF Resv:AF PathErr:AF ResvErr:AF ID:voice
    Path:AF Resv:AF PathErr:AF ResvErr:AF ID:video
  Serial2/0/1:
    Path:AF Resv:AF PathErr:AF ResvErr:AF ID:conference
    Path:AF Resv:AF PathErr:AF ResvErr:AF ID:iptv
    Path:-- Resv:-- PathErr:-- ResvErr:-- Default

Generic policy settings:
    Default policy: Accept all
    Preemption:     Disabled
```

The table below describes the significant fields shown in the display.

***Table 143: show ip rsvp policy local Field Descriptions***

| Field | Description |
|---|---|
| A=Accept<br>F=Forward | State of RSVP messages.<br>• Accept--Messages being accepted.<br>• Forward--Messages being forwarded. |
| Global | Location of the local policy. Global--Local policy configured for the entire router. |
| Path, Resv, PathErr, ResvErr, ACL(s), AS(es), ID, Default | Types of RSVP messages being accepted and forwarded and the match criteria for the local policies configured. Blank (--) means that messages of the specified type are neither accepted nor forwarded. |
| Serial2/0/0 Serial2/0/1 | Local policy configured for a specific interface on the router. |
| Path, Resv, PathErr, ResvErr, ACL(s), AS(es), ID | Types of RSVP messages being accepted and forwarded and the types of local policies configured. Blank (--) means that messages of the specified type are neither accepted nor forwarded. |
| Generic policy settings | Policy settings that are not specific to any local or remote policy.<br>• Default policy: 'Accept all' means that all RSVP messages are accepted and forwarded. 'Reject all' means that all RSVP messages are rejected.<br>• Preemption: 'Disabled' means that RSVP should not implement any preemption decisions required by a particular local or remote policy. 'Enabled' means that RSVP should implement any preemption decisions required by a particular local or remote policy. |

## Examples

The following sample output from the **showiprsvppolicylocal**command**displaysa**global local policy based on a DSCP EF that has been configured :

```
Router# show ip rsvp policy local dscp-ip ef

    A=Accept    F=Forward
    Global:
      Path:AF Resv:AF PathErr:AF ResvErr:AF DSCP(s): ef
Generic policy settings:
    Default policy: Accept all
    Preemption:     Enabled
```

See the table below for a description of the fields.

## Examples

The following sample output from the **showiprsvppolicylocaldetail**command**shows**the location of the local policy (such as whether the policy is configured globally or for a specific interface) and the settings for preemption scope and maximum bandwidth. Preemption priorities and sender and receiver limits also appear even if they are set to their defaults.

```
Router# show ip rsvp policy local detail
Global:
  Policy for ID: voice
    Preemption Scope: Unrestricted.
    Local Override:   Disabled.
    Fast ReRoute:     Accept.
    Handle:           02000409.
                           Accept               Forward
    Path:                  Yes                  Yes
    Resv:                  Yes                  Yes
    PathError:             Yes                  Yes
    ResvError:             Yes                  Yes
                           Setup Priority       Hold Priority
    TE:                    N/A                  N/A
    Non-TE:                N/A                  N/A
                           Current              Limit
    Senders:               0                    40
    Receivers:             0                    N/A
    Conversations:         0                    N/A
    Group bandwidth (bps): 0                    200K
    Per-flow b/w (bps):    N/A                  10M
  Policy for ID: video
    Preemption Scope: Unrestricted.
    Local Override:   Disabled.
    Fast ReRoute:     Accept.
    Handle:           0200040A.

                           Accept               Forward
    Path:                  Yes                  Yes
    Resv:                  Yes                  Yes
    PathError:             Yes                  Yes
    ResvError:             Yes                  Yes
                           Setup Priority       Hold Priority
    TE:                    2                    2
    Non-TE:                5                    4
                           Current              Limit
    Senders:               2                    10
    Receivers:             2                    10
    Conversations:         2                    10
    Group bandwidth (bps): 100K                 200K
    Per-flow b/w (bps):    N/A                  10M
Ethernet2/1:
  Policy for ID: voice
    Preemption Scope: Unrestricted.
    Local Override:   Disabled.
    Fast ReRoute:     Accept.
```

```
    Handle:           0200040B.

                            Accept               Forward
    Path:                   Yes                  Yes
    Resv:                   Yes                  Yes
    PathError:              Yes                  Yes
    ResvError:              Yes                  Yes
                            Setup Priority       Hold Priority
    TE:                     2                    2
    Non-TE:                 5                    4
                            Current              Limit
    Senders:                2                    10
    Receivers:              2                    10
    Conversations:          2                    10
    Group bandwidth (bps): 100K                  200K
    Per-flow b/w (bps):    N/A                   10M
Generic policy settings:
    Default policy: Accept all
    Preemption:     Disabled
```

The table below describes the significant fields shown in the display.

***Table 144: show ip rsvp policy local detail Field Descriptions***

| Field | Description |
|---|---|
| Global | Location of the local policy. Global--Local policy configured for the entire router. |
| Policy for ID | A global local policy defined for an application ID alias named voice. |
| Preemption Scope | Describes which classes of RSVP quality of service (QoS) reservations can be preempted by other classes of RSVP QoS reservations on the same interface.<br>Unrestricted means that a reservation using an application ID such as voice can preempt any other class of reservation on the same interface as that reservation, even other nonvoice reservations. |
| Local Override | Overrides any remote policy by enforcing the local policy in effect.<br>• Disabled--Not active.<br>• Enabled--Active. |
| Fast ReRoute | State of Fast ReRoute for Multiprotocol Label Switching (MPLS)/traffic engineering (TE) label switched paths (LSPs).<br>• Accept--Messages being accepted.<br>• Do not accept--Messages requesting Fast Reroute service are not being accepted. |
| Handle | Internal database ID assigned to the security association by RSVP for bookkeeping purposes. |

| Field | Description |
|---|---|
| Accept, Forward | State of RSVP messages. |
| Path, Resv, PathError, ResvError | Types of RSVP messages being accepted and forwarded.<br>• Yes--Messages are being accepted and forwarded.<br>• No--Messages are not being accepted or forwarded. |
| Setup Priority, Hold Priority | Preemption priorities. Setup Priority indicates the priority of a reservation when it is initially installed. Hold Priority indicates the priority of a reservation after it has been installed.<br>N/A means preemption priorities are not configured. |
| TE | The preemption priority of TE reservations. Values for Setup Priority and Hold Priority range from 0 to 7 where 0 is considered the highest priority. |
| Non-TE | The preemption priority of non-TE reservations. Values for Setup Priority and Hold Priority range from 0 to 65535 where 65535 is considered the highest priority. |
| Current, Limit | The present number and the highest number of these parameters allowed. |
| Senders | The number of current PATH states accepted and/or approved by this policy. |
| Receivers | The number of current RESV states accepted by this policy. |
| Conversations | The number of active bandwidth requests approved by the local policy. |
| Group bandwidth (bps) | Amount of bandwidth configured for a class of reservations in bits per second (bps). |
| Per-flow b/w (bps) | Amount of bandwidth configured for each reservation in bits per second (bps). |
| Ethernet2/1 | Local policy configured for a specific interface on the router. |

| Field | Description |
|---|---|
| Generic policy settings | Policy settings that are not specific to the local policy.<br>• Default policy: 'Accept all' means that all RSVP messages are accepted and forwarded. 'Reject all' means that all RSVP messages are rejected.<br>• Preemption: 'Disabled' means that RSVP should not implement any preemption decisions required by a particular local or remote policy. 'Enabled' means that RSVP should implement any preemption decisions required by a particular local or remote policy. |

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp policy local** | Determines how to perform authorization on RSVP requests. |

# show ip rsvp policy vrf

To display information for a Resource Reservation Protocol (RSVP) policy configured with a virtual routing and forwarding (VRF) instance, use the **showiprsvppolicyvrf**command in user EXEC or privileged EXEC mode.

{**show ip rsvp policy vrf** {*****| *vrf-name*} [**identity** [ *alias* ]]| **local** [**acl** *acl*| **default**| **detail** [**acl** *acl*| **default**| **identity** *alias*| **interface** *interface-type*| **origin-as** *as-number*]]}

## Syntax Description

| | |
|---|---|
| * | Displays all VRFs. |
| *vrf-name* | Name of a specified VRF. |
| identity | (Optional) Unique information that is conveyed in the POLICY-DATA object for RSVP messages. |
| *alias* | (Optional) Specifies a string used within the router to reference the identity in RSVP configuration commands and show displays. The string can have as many as 64 printable characters including quotes and regular expressions (in the range 0x20 to 0x7E).<br>**Note** If you use the “ ” or ? characters as part of the alias or locator string itself, you must type the CTRL/V key sequence before entering the embedded “ ” or ? characters. The alias is never transmitted to other routers. |
| local | (Optional) A local policy. |
| acl | (Optional) Access control list (ACL) for the local policy. |
| *acl* | (Optional) Specifies an ACL. Values for each ACL are 1 to 199. |
| default | (Optional) A default policy. |
| detail | (Optional) Detailed information for the VRF. |
| acl | (Optional) Access control list (ACL) for the local policy. |
| *acl* | (Optional) Specifies an ACL. Values for each ACL are 1 to 199. |
| default | (Optional) A default policy. |

| | |
|---|---|
| identity | (Optional) An application ID. |
| *alias* | (Optional) Specifies a string used within the router to reference the identity in RSVP configuration commands and show displays. The string can have as many as 64 printable characters including quotes and regular expressions (in the range 0x20 to 0x7E).<br>**Note** If you use the " " or ? characters as part of the alias or locator string itself, you must type the CTRL/V key sequence before entering the embedded " " or ? characters. The alias is never transmitted to other routers. |
| interface | (Optional) An interface for the VRF. |
| *interface-type* | (Optional) An interface name for the VRF. |
| origin-as | (Optional) An autonomous system (AS) for the VRF. |
| *as-number* | (Optional) An AS. Values for each autonomous system are 1 to 65535. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced. |

## Usage Guidelines

Use the **showiprsvppolicyvrf** command to display the policies configured for VRFs.

## Examples

The following example shows an ACL local policy that is configured for a specified VRF:

```
Router# show ip rsvp policy vrf myVrf1 local acl 101
    A=Accept    F=Forward
VRF: myVrf1
    Global:
      Path:AF Resv:AF PathErr:AF ResvErr:AF ACL(s): 101
    Ethernet0/0:
      Path:AF Resv:AF PathErr:AF ResvErr:AF ACL(s): 101
Generic policy settings:
    Default policy: Accept all
    Preemption:     Disabled
```

The table below describes the significant fields shown in the display.

*Table 145: show ip rsvp policy vrf Field Descriptions*

| Field | Description |
|---|---|
| A=Accept | Accept the message. |
| F=Forward | Forward the message. |
| VRF | Name of the VRF.<br>Global: Global policies configured for the VRF.<br>Path: AF--Accept and forward these messages.<br>Resv: AF--Accept and forward these messages.<br>PathErr--Accept and forward these messages.<br>ResvErr--Accept and forward these messages.<br>ACL(s)--Access control list number.<br>Ethernet0/0--The interface configured for the VRF. |
| Generic policy settings | Policy settings that are not specific to COPS or the local policy.<br>Default policy: Accept all means all RSVP messages are accepted and forwarded. Reject all means all RSVP messages are rejected.<br>Preemption: Disabled means that RSVP should not implement any preemption decisions required by a particular local or remote policy. Enabled means that RSVP should implement any preemption decisions required by a particular local or remote policy. |

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp policy vrf** | Configures an RSVP policy for a VRF. |

# show ip rsvp precedence

To display IP precedence information about Resource Reservation Protocol (RSVP) interfaces, use the **showiprsvpprecedence**command in user EXEC or privileged EXEC mode.

**show ip rsvp precedence** [**type number**]

## Syntax Description

| | |
|---|---|
| **type** | (Optional) Type of interface. |
| number | (Optional) Number of the interface. |

## Command Modes

User EXEC(>) Privileged EXEC(#)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced. |

## Usage Guidelines

To obtain IP precedence information about a specific interface configured to use RSVP, specify the interface name with the show ip rsvp precedence command. To obtain IP precedence information about all interfaces enabled for RSVP on the router, use the show ip rsvp precedence command without specifying an interface name.

## Examples

The following example shows the IP precedence information for the interaces on which RSVP is enabled:

```
Router# show ip rsvp precedence ethernet 0/1
Interface name   Precedence  Precedence   TOS          TOS
                   conform    exceed     conform     exceed
Ethernet0/0          -           -          -           -
Ethernet0/1          -           -          -           -
Ethernet1/1          -           -          4           -
Ethernet1/2          3           -          -           -
```

The table below describes the fields shown in the display.

***Table 146: show ip rsvp precedence Field Descriptions***

| Field | Description |
|---|---|
| Interface name | Displays the interface details. |

| Field | Description |
|---|---|
| Precedence conform | Displays the IP precedence conform information for an interface.<br>**Note** The Precedence conform value specifies an IP precedence value in the range from 0 to 7 for traffic that conforms to the RSVP flowspec. |
| Precedence exceed | Displays the IP precedence exceed information for an interface.<br>**Note** The Precedence exceed value specifies an IP Precedence value in the range from 0 to 7 for traffic that exceeds the RSVP flowspec. |
| TOS conform | Displays the IP type of service (ToS) conform information for an interface.<br>**Note** The TOS conform value specifies a ToS value in the range from 0 to 31 for traffic that conforms to the RSVP flowspec. |
| TOS exceed | Displays the IP type of service (ToS) exceed information for an interface.<br>**Note** The TOS exceed value specifies a ToS value in the range from 0 to 31 for traffic that exceeds the RSVP flowspec. |

## Related Commands

| Command | Description |
|---|---|
| show ip rsvp | Displays RSVP-related information. |
| **show ip rsvp interface** | Displays RSVP-related interface information. |
| **show ip rsvp tos** | Displays IP TOS information for RSVP enabled interfaces. |

# show ip rsvp request

To display Resource Reservation Protocol (RSVP)-related request information currently in the database, use the **showiprsvprequest**command in user EXEC or privileged EXEC mode.

### Syntax for T, 12.2S, 12.2SB, 12.2(33)SRD, and Earlier Releases

**show ip rsvp request [detail]** [**filter** [**destination** *ip-address*| *hostname*] [**dst-port** *port-number*] [**source** *ip-address*| *hostname*] [**src-port** *port-number*]] [**vrf** {*| *vrf-name*}]

### Syntax for 12.2(33)SRE with Filtering Session Type all

**show ip rsvp request [detail]** [**filter** [**session-type all**]]

### Syntax for 12.2(33)SRE with Filtering Session Type 1

**show ip rsvp request [detail]** [**filter** [**session-type** *session-type-number*]] [**destination** *ip-address*| *hostname*] [**dst-port** *port-number*] [**source** *ip-address*| *hostname*] [**src-port** *port-number*]

### Syntax for 12.2(33)SRE with Filtering Session Type 7 or 13

**show ip rsvp request [detail]** [**filter** [**session-type** *session-type-number*]] [**destination** *ip-address*| *hostname*] [**lsp-id** *lsp-id*] [**sender** *ip-address*| *hostname*] [**tunnel-id** *tunnel-id*]

## Syntax Description

| | |
|---|---|
| **detail** | (Optional) Specifies additional receiver information. |
| **filter** | (Optional) Specifies a subset of the receivers to display . |
| **session-type** *session-type-number* | (Optional) Specifies the type of RSVP sessions to display. Valid values are:<br>• **1** for IPv4 sessions<br>• **7** for IPv4 point-to-point (P2P) traffic engineering (TE) label switched path (LSP) tunnel sessions<br>• **13** for IPv4 point-to-multipoint (P2MP) TE LSP tunnel sessions. |
| **all** | (Optional) Specifies all types of RSVP sessions. |
| **destination** *ip-address* | (Optional) Specifies the destination IP address. |
| *hostname* | (Optional) Hostname of the destination. |
| **dst-port** *port-number* | (Optional) Specifies the destination port number. Valid destination port numbers can be in the range of 0 to 65535. |

| | |
|---|---|
| **lsp-id** *lsp-id* | (Optional) Specifies the label switched path ID. Valid numbers can be in the range of 0 to 65535. |
| **sender** *ip-address* | (Optional) Specifies the IP address of the tunnel head. |
| *hostname* | (Optional) Hostname of the tunnel head. |
| **source** *ip-address* | (Optional) Specifies the source IP address of the source. |
| *hostname* | (Optional) Hostname of the source. |
| **src-port** *port-number* | (Optional) Specifies the source port number. Valid source port numbers can be in the range of 0 to 65535. |
| **tunnel-id** *tunnel-id* | (Optional) Specifies the tunnel ID number. Valid numbers can be in the range of 0 to 65535. |
| **vrf** * | (Optional) Displays all the configured virtual routing and forwarding (VRF) instances. |
| **vrf** *vrf-name* | (Optional) Name of a specified VRF. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.2 | This command was integrated into Cisco IOS Release 12.2. The **detail** keyword was added to display additional request information. |
| 12.0(22)S | This command was integrated into Cisco IOS Release 12.0(22)S. This command was enhanced to show Fast Reroute information when a link-state packet (LSP) is actively using a backup tunnel that terminates at this node (that is, when a node is the merge point.) The command is supported on the Cisco 10000 series Edge Services Router (ESR). |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SRC | The command output was modified to display RSVP aggregation information. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

| Release | Modification |
|---|---|
| 15.0(1)M | This command was modified. The **vrf**and*****keywords and the *vrf-name* argument were added. |
| 12.2(33)SRE | This command was modified. The**session-type** keyword was added to display specific types of tunnels. The output was modified to display Multiprotocol (MPLS) TE P2MP information. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

Use the **showiprsvprequest** command to display the RSVP reservations currently being requested upstream for a specified interface or all interfaces. The received reservations may differ from requests because of aggregated or refused reservations. If desired, information for only a single tunnel or a subset of tunnels can be displayed.

### Limiting the Display

When hundreds or thousands of tunnels exist and you are interested in only a few, you can display the output for only a single tunnel or a subset of tunnels. To request a limited display, enter the **showiprsvprequest** command with the appropriate keyword (called an output filter): **destination**, **dst-port**, **source**, and **src-port**. You can enter any or all of the output filters, and you can enter them whether or not you specify the **detail** keyword.

You can also limit the display to a particular VRF by using the **showiprsvprequestvrf***vrf-name*command.

## Examples

## Examples

The following is sample output from the **showiprsvprequest** command when RSVP aggregation is configured:

```
Router# show ip rsvp request
To              From            Pro DPort Sport Next Hop      I/F      Fi Serv BPS
192.168.5.1     192.168.2.1     TCP 222   222   192.168.40.1  Se1/0    FF RATE 80K
192.168.50.1    192.168.40.1    0   46    0     10.10.10.4    Se1/0    FF LOAD 300K
```

The table below describes the significant fields shown in the display.

***Table 147: show ip rsvp request Field Descriptions***

| Field | Description |
|---|---|
| To | IP address of the end-to-end (E2E) receiver or deaggregator. |
| From | IP address of the E2E sender or aggregator. |
| Pro | Protocol code.<br>• TCP indicates Transmission Control Protocol.<br>• Code 0 indicates an aggregate reservation. |

| Field | Description |
|---|---|
| DPort | Destination port number.<br>• DSCP for aggregate reservations. |
| Sport | Source port number.<br>• 0 for aggregate reservations. |
| Next Hop | IP address of the next hop.<br>• Aggregator for E2E reservations mapped onto aggregates.<br>• Next hop RSVP node for aggregate or E2E reservations onto an interface. |
| I/F | Interface of the next hop. |
| Fi | Filter (Wildcard Filter, Shared Explicit, or Fixed Filter). |
| Serv | Service (value can be **rate** or **load**). |
| BPS | The rate, in bits per second, in the RSVP reservation request for a reservation.<br>**Note** In the example, the top one is the E2E reservation signaled at 80 bps and the corresponding aggregate request at 300 bps. |

## Examples

The following is sample output from the **showiprsvprequestdetail** command when RSVP aggregation is configured:

```
Router# show ip rsvp request detail

RSVP Reservation. Destination is 192.168.5.1, Source is 192.168.2.1,
  Protocol is TCP, Destination port is 222, Source port is 222
  Prev Hop: 192.168.40.1 on Serial1/0
  Reservation Style is Fixed-Filter, QoS Service is Guaranteed-Rate
  Average Bitrate is 80K bits/sec, Maximum Burst is 5K bytes
  Request ID handle: 0100040E.
  Policy: Forwarding. Policy source(s): Default
    Priorities - preempt: 0, defend: 0
  PSB Handle List [1 elements]: [0x19000407]
  RSB Handle List [1 elements]: [0x17000409]
  3175 Aggregation: RSVP 3175 AggResv 192.168.40.1->192.168.50.1_ef(46)
RSVP Reservation. Destination is 192.168.50.1, Source is 192.168.40.1,
  Protocol is 0  , Destination port is 46, Source port is 0
  Prev Hop: 10.10.10.4 on Serial1/0
  Reservation Style is Fixed-Filter, QoS Service is Controlled-Load
  Average Bitrate is 300K bits/sec, Maximum Burst is 300K bytes
  Request ID handle: 0100040B.
  Policy: Forwarding. Policy source(s): Default
    Priorities - preempt: 0, defend: 0
```

```
  PSB Handle List [1 elements]: [0x9000408]
  RSB Handle List [1 elements]: [0x100040A]
```

The table below describes the significant fields shown in the display.

***Table 148: show ip rsvp request detail--RSVP Aggregation Field Descriptions***

| Field | Description |
|---|---|
| RSVP Reservation | Destination--Receiver's IP address of the E2E RESV message.<br>Source--Sender's IP address of the E2E RESV message. |
| Protocol | Protocol--IP protocol used; TCP--Transmission Control Protocol.<br>• 0 for aggregate reservations. |
| Destination port | Receiver's port number.<br>• DSCP for aggregate reservations. |
| Source port | Sender's port number.<br>• 0 for aggregate reservations. |
| Previous Hop | IP address of the previous hop on the specified interface.<br>**Note** This is the aggregator's IP address in the case of an E2E reservation mapped onto an aggregate as seen at the deaggregator. |
| Reservation Style | Multi-reservations sharing of bandwidth; values include Fixed-Filter, Shared-Explicit, and Wildcard-Filter. |
| QoS Service | Type of quality of service (QoS) configured; values include Guaranteed-Rate and Controlled-Load. |
| Average Bitrate | Average rate requested, in bits per second, for the data. |
| Maximum Burst | Largest amount of data allowed in kilobytes. |
| Request ID handle | Internal database ID assigned to the request by RSVP for bookkeeping purposes. |
| Policy | Policy status: Forwarding--RSVP RESV messages are being accepted and forwarded. |

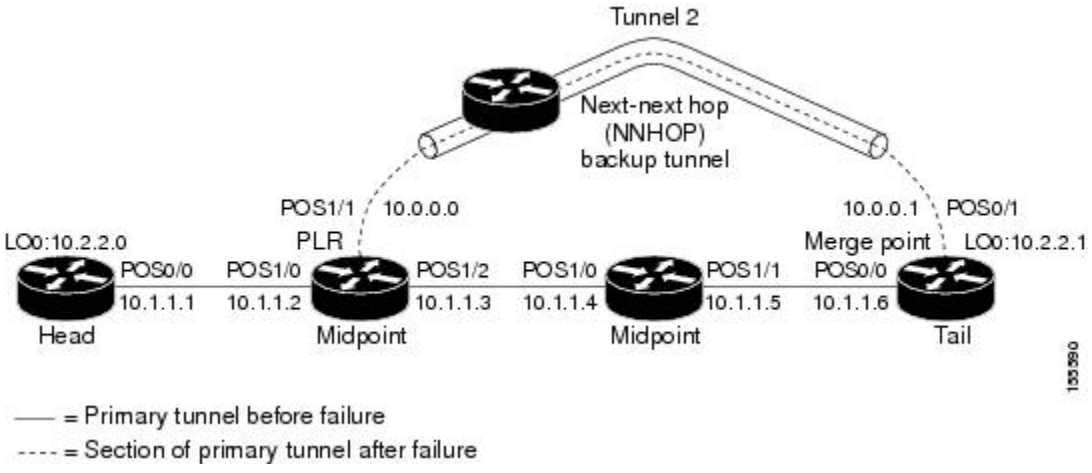
| Field | Description |
|---|---|
| Policy source(s) | Type of local policy in effect; values include Default, Local, and MPLS/TE. |
| Priorities | RSVP preemption and hold priorities of the reservation; default is 0. |
| PSB Handle List | Path state block (PSB) internal database identifier assigned by RSVP for bookkeeping purposes. |
| RSB Handle List | Reservation state block (RSB) internal database identifier assigned by RSVP for bookkeeping purposes. |
| 3175 Aggregation | RSVP aggregation as defined in RFC 3175, *Aggregation of RSVP for IPv4 and IPv6 Reservations* .<br>**Note** This E2E reservation is mapped onto an RSVP aggregate reservation with an aggregator (source) IP address of 192.168.40.1, a destination (deaggregator) IP address of 192.168.50.1, and a DSCP value of expedited forwarding (EF). |

## Examples

The following is sample output from the **showiprsvprequestdetail** command when the command is entered on the merge point before and after a failure.

This figure illustrates the network topology for the RSVP configuration example.

***Figure 56: Network Topology for the RSVP Configuration Example***



## Examples

```
Router# show ip rsvp request detail

RSVP Reservation. Tun Dest: 10.2.2.1 Tun Sender: 10.2.2.0,
   Tun ID: 1 LSP ID: 126
   Next Hop is 10.1.1.5 on POS0/1
   Label is 0
   Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
   Average Bitrate is 0G bits/sec, Maximum Burst is 1K bytes
   RRO:
    Empty
```

## Examples

```
Router# show ip rsvp request detail

RSVP Reservation. Tun Dest: 10.2.2.1 Tun Sender: 10.2.2.0,
   Tun ID: 1 LSP ID: 126
   Next Hop is 10.1.1.5 on POS0/1
   Label is 0
   Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
   Average Bitrate is 0G bits/sec, Maximum Burst is 1K bytes
   RRO:
     Empty
   FRR is in progress (we are Merge Point)
 RSVP Reservation. Tun Dest: 10.2.2.1 Tun Sender: 10.2.2.0,
   Tun ID: 1 LSP ID: 126
   Next Hop is 10.0.0.0 on POS0/1
   Label is 0
   Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
   Average Bitrate is 0G bits/sec, Maximum Burst is 1K bytes
   RRO:
     Empty
   FRR is in progress (we are Merge Point)
```

Notice that after the failure, there are two entries for the rerouted LSP.

The first entry continues to show the prefailure information (that is, RESV messages are being sent to 10.1.1.5 on POS0/1). This state is for the RESV being sent upstream before the failure, in response to path messages sent before the failure. This state may time out quickly, or it may continue to be refreshed for a few minutes if, for example, an upstream node is unaware of the failure.

The second entry shows the post-failure information (that is, RESV messages are being sent to 10.0.0.0 on POS0/1). This state is for the RESV messages being sent upstream after the failure (to the point of local repair [PLR]), and will remain and be refreshed as long as the LSP is rerouted.

In example 2, the merge point is also the tail of the LSP. There is no record route object (RRO) information because there are no nodes downstream.

## Examples

The following is sample output from the **showiprsvprequestdetail** command, which shows MPLS TE P2MP information:

```
Router# show ip rsvp request detail
Request:
  P2MP ID: 22  Tun ID: 22  Ext Tun ID: 10.1.1.201
  Tun Sender: 10.1.1.201  LSP ID: 1  SubGroup Orig: 10.1.1.201
  SubGroup ID: 1
  S2L Destination : 10.1.1.203
  Prev Hop:10.1.1.205 on Ethernet1/1
  Label: 17 (incoming)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Average Bitrate is 500K bits/sec, Maximum Burst is 1K bytes
  Request ID handle: 0100042C.
  Policy: Forwarding. Policy source(s): MPLS/TE
```

```
  PSB Handle List [1 elements]: [0x1000427]
  RSB Handle List [1 elements]: [0x100042B]
```

The table below describes the significant fields shown in the display.

***Table 149: show ip rsvp request--MPLS TE P2MP Field Descriptions***

| Field | Description |
|---|---|
| P2MP ID | A 32-bit number that identifies the set of destinations of the P2MP tunnel. |
| Tun ID | Tunnel identification number. |
| Ext Tun ID | Extended tunnel identification number. |
| Tun Sender | IP address of the sender. |
| LSP ID | Label switched path identification number. |
| SubGroup Orig | LSP headend router ID address. |
| SubGroup ID | An incremental number assigned to each sub-LSP signaled from the headend router. |
| S2L Destination | LSP tailend router ID address. |

The following is sample output from the **showiprsvprequestfiltersession-type13**command, which shows RSVP RESV requests for point-to-multipoint traffic:

```
Router# show ip rsvp request filter session-type 13

Destination   Tun Sender    TunID LSPID P2MP-ID SubID Next Hop      I/F     BPS
192.168.5.1   10.1.1.201    22    1     22      1     192.168.40.1  Se1/0   80K
```

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp reservation** | Displays RSVP PATH-related receiver information currently in the database. |
| **show ip rsvp sender** | Displays RSVP RESV-related receiver information currently in the database. |

# show ip rsvp reservation

To display Resource Reservation Protocol (RSVP)-related receiver information currently in the database, use the **showiprsvpreservation**command in user EXEC or privileged EXEC mode.

### Syntax for Cisco IOS Release T, 12.2S, 12.2SB, 12.2(33)SRD, Cisco IOS XE Release 2.6, and Earlier Releases

**show ip rsvp reservation [detail]** [**filter** [**destination** *address*] [**dst-port** *port-number*] [**source** *address*] [**src-port** *port-number*]] [**vrf** {*****| *vrf-nam* **e**}]

### Syntax for Cisco IOS Release 12.2(33)SRE with Filtering Session Type all

**show ip rsvp reservation [detail]** [**filter** [**session-type all**]]

### Syntax for Cisco IOS Release 12.2(33)SRE with Filtering Session Type 1

**show ip rsvp reservation [detail]** [**filter** [**session-type** *session-type-number*]] [**destination** *address*] [**dst-port** *port-number*] [**source** *address*] [**src-port** *port-number*]

### Syntax for Cisco IOS Release 12.2(33)SRE with Filtering Session Type 7 or 13

**show ip rsvp reservation [detail]** [**filter** [**session-type** *session-type-number*]] [**destination** *address*] [**lsp-id** *lsp-id*] [**sender** *address*] [**tunnel-id** *tunnel-id*]

## Syntax Description

| | |
|---|---|
| **detail** | (Optional) Specifies additional receiver information. |
| **filter** | (Optional) Specifies a subset of the receivers to display . |
| **destination** *address* | (Optional) Specifies the destination hostname or IP address of the receiver. |
| **dst-port** *port-number* | (Optional) Specifies the destination port number. The destination port number range is from 0 to 65535. |
| **source** *address* | (Optional) Specifies the source hostname or IP address of the receiver. |
| **src-port** *port-number* | (Optional) Specifies the source port number. The source port number range is from 0 to 65535. |
| **vrf** ***** | (Optional) Displays all the configured virtual routing and forwarding (VRF) instances. |
| *vrf-name* | (Optional) Name of a specified VRF. |

| | |
|---|---|
| **session-type** *session-type-number* | (Optional) Specifies the type of RSVP sessions to display. Valid values are:<br>• **1** for IPv4 sessions<br>• **7** for IPv4 point-to-point (P2P) traffic engineering (TE) label switched path (LSP) tunnel sessions<br>• **13** for IPv4 point-to-multipoint (P2MP) TE LSP tunnel sessions. |
| **all** | (Optional) Specifies all types of RSVP sessions. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.2 | This command was integrated into Cisco IOS Release 12.2. The **detail** keyword was added to display additional reservation information. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.4(4)T | This command was integrated into Cisco IOS Release 12.4(4)T, and its output was modified to display application ID information. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SRC | This command was modified. The command output was modified to display tunnel-based admission control (TBAC) and RSVP aggregation information. |
| 15.0(1)M | This command was modified. The **vrf**and*keywords and the *vrf-name* argument were added. |
| 12.2(33)SRE | This command was modified. The **session-type** keyword was added to display specific types of tunnels. The output was modified to display MPLS TE P2MP information. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelin

**Note** The syntax of the command depends on your platform and release. The **vrf**and * keywords and *vrf-name*argument are not supported on ASR 1000 Series Aggregation Services Routers.

Use the **showiprsvpreservation** command to display the current receiver (RESV) information in the database for a specified interface or all interfaces. This information includes reservations aggregated and forwarded from other RSVP routers.

### Limiting the Display

When hundreds or thousands of tunnels exist and you are interested in only a few, you can display the output for only a single tunnel or a subset of tunnels. To request a limited display, enter the **showiprsvpreservation** command with the appropriate keyword (called an output filter): **destination**, **dst-port**, **source**, and **src-port**. You can enter any or all of the output filters, and you can enter them whether or not you specify the **detail** keyword.

You can also limit the display to a particular VRF by using the **showiprsvpreservationvrf***vrf-name*command.

## Examples

## Examples

The following is sample output from the **showiprsvpreservation**command:

```
Router# show ip rsvp reservation
To              From            Pro DPort Sport Next Hop      I/F   Fi Serv
172.16.1.49     172.16.4.53     1   0     0     172.16.1.49     Se1   FF LOAD
```

The table below describes the significant fields shown in the display.

***Table 150: show ip rsvp reservation Field Descriptions***

| Field | Descriptions |
|---|---|
| To | IP address of the receiver. |
| From | IP address of the sender. |
| Pro | Protocol code. |
| DPort | Destination port number. |
| Sport | Source port number. |
| Next Hop | IP address of the next hop. |
| I/F | Interface of the next hop. |
| Fi | Filter (Wildcard Filter, Shared-Explicit, or Fixed-Filter). |
| Serv | Service (value can be RATE or LOAD). |

## Examples

The following is sample output from the **showiprsvpreservationdetail**command with application ID information:

```
Router# show ip rsvp reservation detail

RSVP Reservation. Destination is 192.168.104.3, Source is 192.168.104.1,
  Protocol is UDP, Destination port is 4444, Source port is 4444
  Next Hop is 192.168.106.2, Interface is ATM1/0.1
  Reservation Style is Fixed-Filter, QoS Service is Guaranteed-Rate
  Resv ID handle: 0A00040B.
  Created: 12:18:32 UTC Sat Dec 4 2004
  Average Bitrate is 5K bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  Status:
  Policy: Forwarding. Policy source(s): Default
    Priorities - preempt: 5, defend: 2
    Application ID: 'GUID=www.cisco.com, VER=10.1.1.2, APP=voice, SAPP=h323'
                    '/usr/local/bin/CallManager'
```

The table below describes the significant fields shown in the display.

***Table 151: show ip rsvp reservation detail--Application ID Field Descriptions***

| Field | Descriptions |
|---|---|
| RSVP Reservation | • Destination--Receiver's IP address of the RESV message.<br>• Source--Sender's IP address of the RESV message. |
| Protocol | Protocol--IP protocol used; UDP--User Data Protocol. |
| Destination port | Receiver's port number. |
| Source port | Sender's port number. |
| Next Hop | IP address of the next hop. |
| Interface | Interface type of the next hop. |
| Reservation Style | Multireservations sharing of bandwidth; values are Fixed-Filter, Shared-Explicit, and Wildcard-Filter. |
| QoS Service | Type of qulaity of service (QoS) configured; values are Guaranteed-Rate and Controlled Load. |
| Resv ID handle | Internal database ID assigned to the RESV message by RSVP for bookkeeping purposes. |
| Created | Time and date when the reservation was created. |
| Average Bitrate | Average rate, in bits per second, for the data. |

| Field | Descriptions |
|---|---|
| Maximum Burst | Largest amount of data allowed, in kilobytes. |
| Min Policed Unit | Size of the smallest packet generated by the application, in bytes, including the application data and all protocol headers at or above the IP level. |
| Max Pkt Size | Largest packet allowed in bytes. |
| Status | Status of the local policy; values are Proxied and Proxy-terminated.<br>**Note** A blank status field means you issued the command on a midpoint for that reservation. |
| Policy | Policy status: Forwarding--RSVP RESV messages are being accepted and forwarded. |
| Policy source(s) | Type of local policy in effect; values are Default, Local, and MPLS/TE. |
| Priorities | Preemption priorities in effect.<br>• preempt: the startup priority; values are 0 to 7 for traffic engineering (TE) reservations with 0 being the highest. Values are 0 to 65535 for non-TE reservations, with 0 being the lowest.<br>• defend: the hold priority; values are the same as preempt. |
| Application ID | A quotable string that identifies the sender application and can be used to match on local policies. The string includes the policy locator in the X.500 Distinguished Name format and the application or filename of the sender application. |

## Examples

The following is sample output from the **showiprsvpreservationdetail**command**whenTBACisconfigured:**

```
Router# show ip rsvp reservation detail

RSVP Reservation. Destination is 10.4.0.1, Source is 10.1.0.1,
  Protocol is UDP, Destination port is 100, Source port is 100
  Next Hop: 10.4.0.1 on Tunnel1, out of band
  Reservation Style is Fixed-Filter, QoS Service is Guaranteed-Rate
  Resv ID handle: 0100040D.
  Created: 11:59:53 IST Tue Mar 20 2007
  Average Bitrate is 10K bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  Status:
  Policy: Forwarding. Policy source(s): Default
```

The table below describes the significant fields shown in the display.

*Table 152: show ip rsvp reservation detail--TBAC Field Descriptions*

| Field | Descriptions |
|---|---|
| RSVP Reservation | • Destination--Receiver's IP address of the RESV message.<br>• Source--Sender's IP address of the RESV message. |
| Protocol | Protocol--IP protocol used; UDP--User Data Protocol. |
| Destination port | Receiver's port number. |
| Source port | Sender's port number. |
| Next Hop | IP address of the next hop on tunnel interface *with out-of-band signaling* . |
| Reservation Style | Multireservations sharing of bandwidth; values are Fixed-Filter, Shared-Explicit, and Wildcard-Filter. |
| QoS Service | Type of QoS configured; values are Guaranteed-Rate and Controlled Load. |
| Resv ID handle | Internal database ID assigned to the RESV message by RSVP for bookkeeping purposes. |
| Created | Time and date when the reservation was created. |
| Average Bitrate | Average rate, in bits per second, for the data. |
| Maximum Burst | Largest amount of data allowed, in kilobytes. |
| Min Policed Unit | Size of the smallest packet generated by the application, in bytes, including the application data and all protocol headers at or above the IP level. |
| Max Pkt Size | Largest packet allowed in bytes. |
| Status | Status of the local policy; values are Proxied and Proxy-terminated.<br>**Note** A blank status field means you issued the command on a midpoint for that reservation. |
| Policy | Policy status: Forwarding--RSVP RESV messages are being accepted and forwarded. |
| Policy source(s) | Type of local policy in effect; values are Default, Local, and MPLS/TE. |

## Examples

The following is sample output from the **showiprsvpreservationdetail**command**whenRSVPaggregationisconfigured:**

```
Router# show ip rsvp reservation detail

RSVP Reservation. Destination is 192.168.5.1, Source is 192.168.2.1,
  Protocol is TCP, Destination port is 222, Source port is 222
  Next Hop: 192.168.50.1 on Serial1/0
  Reservation Style is Fixed-Filter, QoS Service is Guaranteed-Rate
  Resv ID handle: 0600040A.
  Created: 20:27:58 EST Thu Nov 29 2007
  Average Bitrate is 80K bits/sec, Maximum Burst is 5K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  DiffServ Integration:  DSCPs: 46
  Status:
  Policy: Forwarding. Policy source(s): Default
  3175 Aggregation: RSVP 3175 AggResv 192.168.40.1->192.168.50.1_ef(46)
RSVP Reservation. Destination is 192.168.50.1, Source is 192.168.40.1,
  Protocol is 0  , Destination port is 46, Source port is 0
  Next Hop: 10.30.1.1 on Serial1/0
  Reservation Style is Fixed-Filter, QoS Service is Controlled-Load
  Resv ID handle: 03000408.
  Created: 20:27:50 EST Thu Nov 29 2007
  Average Bitrate is 300K bits/sec, Maximum Burst is 300K bytes
  Min Policed Unit: 20 bytes, Max Pkt Size: 0 bytes
  Status:
  Policy: Forwarding. Policy source(s): Default
```

The table below describes the significant fields shown in the display.

***Table 153: show ip rsvp reservation detail--RSVP Aggregation Field Descriptions***

| Field | Descriptions |
|---|---|
| RSVP Reservation | • Destination--Receiver's IP address of the RESV message.<br>• Deaggregator for aggregate reservations.<br>• Source--Sender's IP address of the RESV message.<br>• Aggregator for aggregate reservations. |
| Protocol | Protocol--IP protocol used; TCP--Transmission Control Protocol.<br>• 0 for aggregate reservations. |
| Destination port | Receiver's port number.<br>• Differentiated Services Code Point (DSCP) for aggregate reservations. |

| Field | Descriptions |
|---|---|
| Source port | Sender's port number.<br>• 0 for aggregate reservations. |
| Next Hop | IP address of the next hop on a specified interface.<br>• Deaggregator IP address for E2E reservations mapped onto an aggregate as seen at the aggregator.<br>• None for aggregate reservations as seen at the deaggregator. |
| Reservation Style | Multireservations sharing of bandwidth; values are Fixed-Filter, Shared-Explicit, and Wildcard-Filter. |
| QoS Service | Type of QoS Service configured; values are Guaranteed-Rate and Controlled Load. |
| Resv ID handle | Internal database ID assigned to the RESV message by RSVP for bookkeeping purposes. |
| Created | Time and date when the reservation was created. |
| Average Bitrate | Average rate requested, in bits per second, for the data. |
| Maximum Burst | Largest amount of data allowed, in kilobytes. |
| Min Policed Unit | Size of the smallest packet generated by the application, in bytes, including the application data and all protocol headers at or above the IP level.<br>• Always 0 or 20 on a node configured for RSVP aggregation. |
| Max Pkt Size | Largest packet allowed in bytes.<br>• Always 0 on a node configured for RSVP aggregation. |
| Status | Status of the local policy; policy source and preemption values.<br>**Note** A blank status field means you issued the command on a midpoint for that reservation.<br>**Note** Preemption values are shown only if RSVP preemption is enabled on the router. |

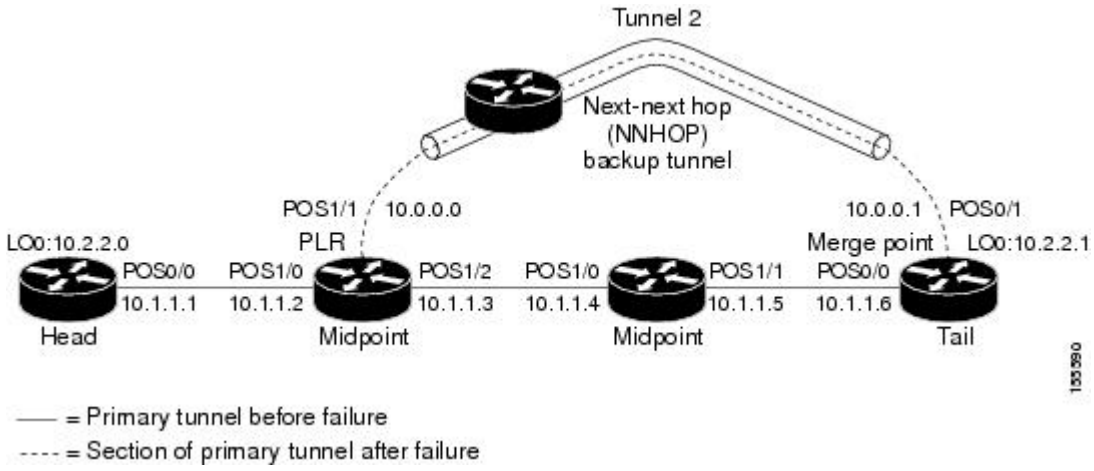
| Field | Descriptions |
|---|---|
| Policy | Policy status: Forwarding--RSVP RESV messages are being accepted and forwarded. |
| Policy source(s) | Type of local policy in effect; values are default, local, and Multiprotocol Label Switching (MPLS)/traffic engineering (TE). |
| 3175 Aggregation | Aggregated reservation on which this E2E reservation is mapped with source (aggregator) and destination (deaggregator) endpoints, IP addresses, and aggregate reservation DSCP. |

## Examples

The following is sample output from the **showiprsvpreservationdetail**command when the command is entered on the PLR before and after a failure.

This figure illustrates the network topology for the RSVP configuration example.

***Figure 61: Network Topology for the RSVP Configuration Example***




## Examples

```
Router# show ip rsvp reservation detail
RSVP Reservation. Tun Dest: 10.2.2.1 Tun Sender: 10.2.2.0,
   Tun ID: 1 LSP ID: 126
   Next Hop is 10.1.1.4 on POS1/2
   Label is 18
   Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
   Average Bitrate is 0G bits/sec, Maximum Burst is 1K bytes
   RRO:
     10.1.1.5/32, Flags:0x0 (No Local Protection)
       Label record: Flags 0x1, ctype 1, incoming label 18
     10.1.1.6/32, Flags:0x0 (No Local Protection)
       Label record: Flags 0x1, ctype 1, incoming label 0
```

## Examples

```
Router# show ip rsvp reservation detail
RSVP Reservation. Tun Dest: 10.2.2.1 Tun Sender: 10.2.2.0,
   Tun ID: 1 LSP ID: 126
   FRR is in progress: (we are PLR)
    Bkup Next Hop is  10.0.0.1 on POS1/1
        Label     is  0
    Orig Next Hop was 10.1.1.4 on POS1/2
        Label     was 18
   Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
   Average Bitrate is 0G bits/sec, Maximum Burst is 1K bytes
  RRO:
    10.2.2.1/32, Flags:0x0 (No Local Protection)
      Label record: Flags 0x1, ctype 1, incoming label 0
```

Notice the following (see italicized text) in Examples 1 and 2:

- At the PLR, you see "Fast Reroute (FRR) is in progress (we are PLR)" when an LSP has been rerouted (that is, it is actively using a backup tunnel).
- RESV messages arrive on a different interface and from a different next hop after a failure. The prefailure display shows the original NHOP and arriving interface; the post-failure display shows both the original and the new (Bkup) NHOP and arriving interface. The label is also shown.
- The Record Route Object (RRO) in arriving RESV messages changes after the failure, given that the RESV messages will avoid the failure (that is, it will traverse different links or hops).

## Examples

The following is sample output from the **showiprsvpreservationdetail**command showing point-to-multipoint information:

```
Router# show ip rsvp reservation detail

Reservation:
  P2MP ID: 22  Tun ID: 22  Ext Tun ID: 10.1.1.201
  Tun Sender: 10.1.1.201  LSP ID: 1  SubGroup Orig: 10.1.1.201
  SubGroup ID: 1
  S2L Destination : 10.1.1.203
  Next Hop: 10.0.0.205 on Ethernet0/0
  Label: 20 (outgoing)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
  Resv ID handle: 0100042A.
  Created: 09:13:16 EST Tue Jun 30 2009
  Average Bitrate is 500K bits/sec, Maximum Burst is 1K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 1500 bytes
  RRO:
    10.1.1.205/32, Flags:0x20 (No Local Protection, Node-id)
      Label subobject: Flags 0x1, C-Type 1, Label 20
    10.1.1.202/32, Flags:0x20 (No Local Protection, Node-id)
      Label subobject: Flags 0x1, C-Type 1, Label 17
    10.1.1.203/32, Flags:0x20 (No Local Protection, Node-id)
      Label subobject: Flags 0x1, C-Type 1, Label 16
  Status:
  Policy: Accepted. Policy source(s): MPLS/TE
```

The table below describes the significant fields shown in the display.

***Table 154: show ip rsvp reservation detail--MPLS TE P2MP Field Descriptions***

| Field | Description |
|---|---|
| P2MP ID | A 32-bit number that identifies the set of destinations of the P2MP tunnel. |

| Field | Description |
|---|---|
| Tun ID | Tunnel identification number. |
| Ext Tun ID | Extended tunnel identification number. |
| Tun Sender | IP address of the sender. |
| LSP ID | Label switched path identification number. |
| SubGroup Orig | LSP headend router ID address. |
| SubGroup ID | An incremental number assigned to each sub-LSP signaled from the headend router. |
| S2L Destination | LSP tailend router ID address. |

The following is sample output from the **showiprsvpreserverationfiltersession-type13**command, which shows RSVP RESV messages for point-to-multipoint traffic:

```
Router# show ip rsvp reservation filter session-type 13

Destination   Tun Sender    TunID LSPID P2MP-ID SubID Next Hop      I/F     BPS
10.1.1.203     10.1.1.201     22    1     22      1     10.0.0.205    Et0/0   500K
10.1.1.206     10.1.1.201     22    1     22      2     10.0.0.205    Et0/0   500K
10.1.1.213     10.1.1.201     22    1     22      3     10.0.0.205    Et0/0   500K
10.1.1.214     10.1.1.201     22    1     22      4     10.0.1.202    Et0/1   500K
10.1.1.216     10.1.1.201     22    1     22      5     10.0.1.202    Et0/1   500K
10.1.1.217     10.1.1.201     22    1     22      6     10.0.1.202    Et0/1   500K
```

## Related Commands

| Command | Description |
|---|---|
| **clear ip rsvp hello instance counters** | Clears (refreshes) the values for Hello instance counters. |
| **ip rsvp reservation** | Enables a router to simulate RSVP RESV message reception from the sender. |
| **show ip rsvp sender** | Displays RSVP RESV-related receiver information currently in the database. |

# show ip rsvp sbm

To display information about a Subnetwork Bandwidth Manager (SBM) configured for a specific Resource Reservation Protocol (RSVP)-enabled interface or for all RSVP-enabled interfaces on the router, use the **showiprsvpsbm**command in EXEC mode.

**show ip rsvp sbm [detail]** [*interface-type interface-number*]

## Syntax Description

| | |
|---|---|
| **detail** | (Optional) Detailed SBM configuration information, including values for the NonResvSendLimit object. |
| *interface-type interface-number* | (Optional) Interface name and interface type for which you want to display SBM configuration information. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.1(1)T | The **detail** keyword was added. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

To obtain SBM configuration information about a specific interface configured to use RSVP, specify the interface name with the **showiprsvpsbm** command. To obtain information about all interfaces enabled for RSVP on the router, use the **showiprsvpsbm** command without specifying an interface name.

To view the values for the NonResvSendLimit object, use the **detail** keyword.

## Examples

The following example displays information for the RSVP-enabled Ethernet interfaces 1 and 2 on router1:

```
Router# show ip rsvp sbm
Interface DSBM Addr      DSBM Priority    DSBM Candidate   My Priority
Et1       10.0.0.0       70               yes              70
Et2       10.2.2.150     100              yes              100
```

The following example displays information about the RSVP-enabled Ethernet interface e2 on router1:

```
Router# show ip rsvp sbm e2
Interface DSBM Addr       DSBM Priority    DSBM candidate   My Priority
e2        10.2.2.150      100              yes              100
```

The table below describes the significant fields shown in the display.

***Table 155: show ip rsvp sbm Field Descriptions***

| Field | Description |
|---|---|
| Interface | Name of the Designated Subnetwork Bandwidth Manager (DSBM) candidate interface on the router. |
| DSBM Addr | IP address of the DSBM. |
| DSBM Priority | Priority of the DSBM. |
| DSBM Candidate | Yes if the **iprsvpdsbmcandidate** command was issued for this SBM to configure it as a DSBM candidate. No if it was not so configured. |
| My Priority | Priority configured for this interface. |

The following example displays information about the RSVP-enabled Ethernet interface 2 on router1. In the left column, the local SBM configuration is shown; in the right column, the corresponding information for the current DSBM is shown. In this example, the information is the same because the DSBM won election.

```
Router# show ip rsvp sbm detailInterface:Ethernet2
Local Configuration              Current DSBM
  IP Address:10.2.2.150          IP Address:10.2.2.150
  DSBM candidate:yes              I Am DSBM:yes
  Priority:100                    Priority:100
  Non Resv Send Limit              Non Resv Send Limit
    Rate:500 Kbytes/sec              Rate:500 Kbytes/sec
    Burst:1000 Kbytes                Burst:1000 Kbytes
    Peak:500 Kbytes/sec              Peak:500 Kbytes/sec
    Min Unit:unlimited               Min Unit:unlimited
    Max Unit:unlimited               Max Unit:unlimited
```

The table below describes the significant fields shown in the display.

***Table 156: show ip rsvp sbm detail Field Descriptions***

| Field | Description |
|---|---|
| Local Configuration | The local DSBM candidate configuration. |
| Current DSBM | The current DSBM configuration. |
| Interface | Name of the DSBM candidate interface on the router. |
| IP Address | IP address of the local DSBM candidate or the current DSBM. |
| DSBM candidate | Yes if the **iprsvpdsbmcandidate** command was issued for this SBM to configure it as a DSBM candidate. No if it was not so configured. |

| Field | Description |
|---|---|
| I am DSBM | Yes if the local candidate is the DSBM. No if the local candidate is not the DSBM. |
| Priority | Priority configured for the local DSBM candidate or the current SBM. |
| Rate | The average rate, in kbps, for the DSBM candidate. |
| Burst | The maximum burst size, in KB, for the DSBM candidate. |
| Peak | The peak rate, in kbps, for the DSBM candidate. |
| Min Unit | The minimum policed unit, in bytes, for the DSBM candidate. |
| Max Unit | The maximum packet size, in bytes, for the DSBM candidate. |

## Related Commands

| Command | Description |
|---|---|
| **debug ip rsvp** | Displays information about SBM message processing, the DSBM election process, and standard RSVP enabled message processing information. |
| **debug ip rsvp detail** | Displays detailed information about RSVP and SBM. |
| **debug ip rsvp detail sbm** | Displays detailed information about SBM messages only, and SBM and DSBM state transitions. |
| **ip rsvp dsbm candidate** | Configures an interface as a DSBM candidate. |
| **ip rsvp dsbm non-resv-send-limit** | Configures the NonResvSendLimit object parameters. |

# show ip rsvp sender

To display Resource Reservation Protocol (RSVP) PATH-related sender information currently in the database, use the **showiprsvpsender**command in user EXEC or privileged EXEC mode.

### Syntax for Cisco IOS Release T, 12.2S, 12.2SB, 12.2(33)SRD, Cisco IOS XE Release 2.6 and, Earlier Releases

**show ip rsvp sender [detail]** [**filter** [**destination** *address*] [**dst-port** *port-number*] [**source** *address*] [**src-port** *port-number*]] [**vrf** {*****| *vrf-name*}]

### Syntax for Cisco IOS Release 12.2(33)SRE with Filtering Session Type all

**show ip rsvp sender [detail]** [**filter** [**session-type all**]]

### Syntax for Cisco IOS Release 12.2(33)SRE with Filtering Session Type 1

**show ip rsvp sender [detail]** [**filter** [**session-type** *session-type-number*]] [**destination** *address*] [**dst-port** *port-number*] [**source** *address*] [**src-port** *port-number*]

### Syntax for Cisco IOS Release 12.2(33)SRE with Filtering Session Type 7 or 13

**show ip rsvp sender [detail]** [**filter** [**session-type** *session-type-number*]] [**destination** *address*] [**lsp-id** *lsp-id*] [**sender** *address*] [**tunnel-id** *tunnel-id*]

## Syntax Description

| | |
|---|---|
| **detail** | (Optional) Specifies additional sender information. |
| **filter** | (Optional) Specifies a subset of the senders to display . |
| **destination** *address* | (Optional) Specifies the hostname of IP address of the destination of the sender. |
| **dst-port** *port-number* | (Optional) Specifies the destination port number. The range is from 0 to 65535. |
| **source** *address* | (Optional) Specifies the hostname or the IP address of the source of the sender. |
| **src-port** *port-number* | (Optional) Specifies the source port number. The range is from 0 to 65535. |
| **vrf** ***** | (Optional) Displays all the configured virtual routing and forwarding (VRF) instances. |
| *vrf-name* | (Optional) Name of a specified VRF. |

| | |
|---|---|
| **session-type** *session-type-number* | (Optional) Specifies the type of RSVP sessions to display. Valid values are:<br>• **1** for IPv4 sessions.<br>• **7** for IPv4 point-to-point (P2P) traffic engineering (TE) label switched path (LSP) tunnel sessions.<br>• **13** for IPv4 point-to-multipoint (P2MP) TE LSP tunnel sessions. |
| **all** | (Optional) Specifies all types of RSVP sessions. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.0(22)S | The command output was modified to display Fast Reroute information, and support was introduced for the Cisco 10000 series Edge Services Router (ESR). |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.4(4)T | The command output was modified to display application ID information. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2(33)SRB | The command output was modified to display fast local repair (FLR) information. |
| 12.2(33)SRC | The command output was modified to display tunnel-based admission control (TBAC) and RSVP aggregation information. |
| 15.0(1)M | This command was modified. The **vrf**and*****keywords and the *vrf-name* argument were added. |
| 12.2(33)SRE | This command was modified. The **session-type** keyword was added to display specific types of tunnels. The output was modified to display MPLS TE P2MP information. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelin

**Note** The syntax of the command depends on your platform and release. The **vrf**and * keywords and *vrf-name*argument are not supported on ASR 1000 Series Aggregaton Services Routers.

Use the **showiprsvpsender** command to display the RSVP sender (PATH) information currently in the database for a specified interface or for all interfaces.

The **showiprsvpsender**commandis useful for determining the state of RSVP signaling both before and after a label switched path (LSP) has been fast rerouted. The **showiprsvpsender**command is especially useful when used at the point of local repair (PLR) or at the merge point (MP).

### Limiting the Display

When hundreds or thousands of tunnels exist and you are interested in only a few, you can display the output for only a single tunnel or a subset of tunnels. To request a limited display, enter the **showiprsvpsender** command with the appropriate keyword (called an output filter): **destination**, **dst-port**, **source**, and **src-port**. You can enter any or all of the output filters, and you can enter them whether or not you specify the **detail** keyword.

### FLR Statistics

Use the **showiprsvpsenderdetail** command to display FLR statistics before, during, and after an FLR procedure. This command shows when a path state block (PSB) was repaired and can be used to determine when the cleanup began after the FLR procedure has finished. However, this command does not display old PLR or MP segments.

## Examples

## Examples

The following is sample output from the **showiprsvpsender** command:

```
Router# show ip rsvp sender
To            From          Pro  DPort  Sport  Prev Hop      I/F    BPS
172.16.1.49   172.16.4.53   1    0      0      172.16.3.53   Et1    80K
172.16.2.51   172.16.5.54   1    0      0      172.16.3.54   Et1    80K
192.168.50.1  192.168.40.1  0    46     0      none          none   17179868160
```

The tabel below describes the significant fields shown in the display.

***Table 157: show ip rsvp sender Field Descriptions***

| Field | Description |
|---|---|
| To | IP address of the receiver. |
| From | IP address of the sender. |
| Pro | Protocol code.<br>• Code 1 indicates an IP protocol such as TCP or User Datagram Protocol (UDP).<br>• Code 0 indicates an aggregate reservation. |

| Field | Description |
|---|---|
| DPort | Destination port number.<br>• The Differentiated Services Code Point (DSCP) for an aggregate reservation. |
| Sport | Source port number.<br>• 0 for an aggregate reservation. |
| Prev Hop | IP address of the previous hop.<br>• None if the node is an aggregator for this reservation. |
| I/F | Interface of the previous hop.<br>• None if the node is an aggregator for this reservation. |
| BPS | As specified in the sender_tspec characteristics of the sender data flow--specified bit rate, in bits per second.<br>• Always 17179868160 for an aggregate reservation. |

## Examples

The following is sample output from the **showiprsvpsenderdetail**command with application IDs configured:

```
Router# show ip rsvp sender detail
PATH Session address: 192.168.104.3, port: 4444. Protocol: UDP
  Sender address: 192.168.104.1, port: 4444
     Inbound from: 192.168.104.1 on interface:
  Traffic params - Rate: 5K bits/sec, Max. burst: 1K bytes
                   Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
  Path ID handle: 09000408.
  Incoming policy: Accepted. Policy source(s): Default
    Priorities - preempt: 5, defend: 2
    Application ID: 'GUID=www.cisco.com, VER=10.1.1.2, APP=voice, SAPP=h323'
                    '/usr/local/bin/CallManager'
  Status: Proxied
  Output on ATM1/0.1. Policy status: Forwarding. Handle: 04000409
    Policy source(s): Default
```

The table below describes the significant fields shown in the display.

*Table 158: show ip rsvp sender detail Field Descriptions*

| Field | Descriptions |
|---|---|
| PATH Session address | Destination IP address of the PATH message.<br>• port--Number of the destination port.<br>• Protocol--IP protocol used. |
| Sender address | Source IP address of the PATH message.<br>• port--Number of the source port. |
| Inbound from | IP address of the sender and the interface name.<br>**Note** A blank interface field means that the PATH message originated at the router on which the **show** command is being executed (the headend router). A specified interface means that the PATH message originated at an upstream router. |
| Traffic params | Traffic parameters in effect:<br>• Rate--Speed, in kilobits per second.<br>• Max. burst--Largest amount of data allowed, in kilobytes.<br>• Min Policed Unit--Size, in bytes, of the smallest packet generated by the application, including the application data and all protocol headers at or above the IP level.<br>• Max Pkt Size--Largest packet allowed in bytes. |
| PATH ID handle | Internal database ID assigned to the PATH message by RSVP for bookkeeping purposes. |
| Incoming policy | State of the incoming policy:<br>• Accepted--RSVP PATH messages are being accepted, but not forwarded.<br>• Not Accepted--RSVP PATH messages are being rejected. |
| Policy source(s) | Type of local policy in effect; values include Default, Local, and MPLS/TE. |

| Field | Descriptions |
|---|---|
| Priorities | Preemption priorities in effect:<br>• preempt--The startup priority; values are 0 to 7 for traffic engineering (TE) reservations with 0 being the highest. Values are 0 to 65535 for non-TE reservations with 0 being the lowest.<br>• defend--The hold priority; values are the same as for preempt. |
| Application ID | A quotable string that identifies the sender application and can be used to match on local policies. The string includes the policy locator in the X.500 Distinguished Name format and the application or filename of the sender application. |
| Status | Status of the local policy:<br>• Proxied--Head.<br>• Proxy-terminated--Tail.<br>• Blockaded--Tail or midpoint and an RESVERROR message has recently been received; therefore, the PSB enters the blockaded state. |
| Output on ATM1/0/1 | Policy status (on the outbound interface):<br>• Forwarding--Inbound PATH messages are being forwarded.<br>• Not Forwarding--Outbound PATH messages are being rejected.<br>• Handle--Internal database ID assigned to the PATH message by RSVP for bookkeeping purposes. |
| Policy source(s) | Type of local policy in effect; values are Default, Local, and MPLS/TE. |

## Examples

The following is sample output from the **showiprsvpsenderdetail** command before FLR has occurred:

```
Router# show ip rsvp sender detail

PATH:
   Destination 192.168.101.21, Protocol_Id 17, Don't Police , DstPort 1
   Sender address: 10.10.10.10, port: 1
   Path refreshes:
```

```
  arriving: from PHOP 172.16.31.34 on Et0/0 every 30000 msecs
Traffic params - Rate: 9K bits/sec, Max. burst: 9K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
Path ID handle: 01000401.
Incoming policy: Accepted. Policy source(s): Default
Status:
Output on Ethernet1/0. Policy status: Forwarding. Handle: 02000400
  Policy source(s): Default
Path FLR: Never repaired
```

The table below describes the significant fields shown in the display.

***Table 159: show ip rsvp sender detail Field Descriptions--Before FLR***

| Field | Descriptions |
|---|---|
| PATH | PATH message information:<br>• Destination IP address.<br>• Protocol ID number.<br>• Policing.<br>• Destination port number. |
| Sender address | Source IP address of the PATH message.<br>• port--Number of the source port. |
| Path refreshes | Refresh information:<br>• IP address of the source (previous hop [PHOP]).<br>• Interface name and number.<br>• Frequency, in milliseconds (ms). |
| Traffic params | Traffic parameters in effect:<br>• Rate--Speed, in kilobits per second.<br>• Max. burst--Largest amount of data allowed, in kilobytes.<br>• Min Policed Unit--Size, in bytes, of the smallest packet generated by the application, including the application data and all protocol headers at or above the IP level.<br>• Max Pkt Size--Largest packet allowed, in bytes. |
| PATH ID handle | Internal database ID assigned to the PATH message by RSVP for bookkeeping purposes. |

| Field | Descriptions |
|---|---|
| Incoming policy | State of the incoming policy:<br>• Accepted--RSVP PATH messages are being accepted, but not forwarded.<br>• Not Accepted--RSVP PATH messages are being rejected. |
| Policy source(s) | Type of local policy in effect; values are Default, Local, and MPLS/TE. |
| Status | Status of the local policy:<br>• Proxied--Head.<br>• Proxy-terminated--Tail.<br>• Blockaded--Tail or midpoint and an RESVERROR message have recently been received; therefore, the path state block (PSB) enters the blockaded state.<br>**Note** A blank field means none of the above. |
| Output on *interface* | Policy status (on the outbound interface):<br>• Forwarding--Inbound PATH messages are being forwarded.<br>• Not Forwarding--Outbound PATH messages are being rejected.<br>• Handle--Internal database ID assigned to the PATH message by RSVP for bookkeeping purposes. |
| Policy source(s) | Type of local policy in effect; values are Default, Local, and MPLS/TE. |
| Path FLR | Never repaired--Indicates that the node has never been a point of local repair (PLR) and, therefore, has never repaired the PSB. |

## Examples

**Note** A node that initiates an FLR procedure is the point of local repair or PLR.

The following is sample output from the **showiprsvpsenderdetail** command at the PLR during an FLR procedure:

```
Router# show ip rsvp sender detail

PATH:
   Destination 192.168.101.21, Protocol_Id 17, Don't Police , DstPort 1
   Sender address: 10.10.10.10, port: 1
   Path refreshes:
     arriving: from PHOP 172.16.31.34 on Et0/0 every 30000 msecs
   Traffic params - Rate: 9K bits/sec, Max. burst: 9K bytes
     Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
   Path ID handle: 01000401.
   Incoming policy: Accepted. Policy source(s): Default
   Status:
   Path FLR: PSB is currently being repaired...try later
   PLR - Old Segments: 1
    Output on Ethernet1/0, nhop 172.16.36.34
    Time before expiry: 2 refreshes
    Policy status: Forwarding. Handle: 02000400
       Policy source(s): Default
```

The table below describes the significant fields shown in the display.

***Table 160: show ip rsvp sender detail Field Descriptions--at the PLR During FLR***

| Field | Descriptions |
|---|---|
| PATH | PATH message information including the following:<br>• Destination IP address.<br>• Protocol ID number.<br>• Policing.<br>• Destination port number. |
| Sender address | Source IP address of the PATH message.<br>• port--Number of the source port. |
| Path refreshes | Refresh information:<br>• IP address of the source (previous hop [PHOP]).<br>• Interface name and number.<br>• Frequency, in milliseconds (ms). |

| Field | Descriptions |
|---|---|
| Traffic params | Traffic parameters in effect:<br>• Rate--Speed, in kilobits per second.<br>• Max. burst--Largest amount of data allowed, in kilobytes.<br>• Min Policed Unit--Size, in bytes, of the smallest packet generated by the application, including the application data and all protocol headers at or above the IP level.<br>• Max Pkt Size--Largest packet allowed, in bytes. |
| PATH ID handle | Internal database ID assigned to the PATH message by RSVP for bookkeeping purposes. |
| Incoming policy | State of the incoming policy:<br>• Accepted--RSVP PATH messages are being accepted, but not forwarded.<br>• Not Accepted--RSVP PATH messages are being rejected. |
| Policy source(s) | Type of local policy in effect; values are Default, Local, and MPLS/TE. |
| Status | Status of the local policy:<br>• Proxied--Head.<br>• Proxy-terminated--Tail.<br>• Blockaded--Tail or midpoint and an RESVERROR message have recently been received; therefore, the PSB enters the blockaded state.<br>**Note** A blank field means none of the above. |
| Path FLR | PSB is currently being repaired. FLR is in process. |

| Field | Descriptions |
|---|---|
| PLR - Old Segments | The number of old segments or interfaces after the PLR initiated the FLR procedure. For each old segment, the following information displays:<br>• Output on interface--Outbound interface after the FLR and the next-hop IP address.<br>• Time before expiry--Number of PATH messages sent on a new segment before the old route (segment) expires.<br>• Policy status (on the outbound interface):<br>  • Forwarding--Inbound PATH messages are being forwarded.<br>  • Not Forwarding--Outbound PATH messages are being rejected.<br>  • Handle--Internal database ID assigned to the PATH message by RSVP for bookkeeping purposes.<br>• Policy source(s)--Type of local policy in effect; values are Default, Local, and MPLS/TE. |

## Examples

**Note** The node where the old and new paths (also called segments or interfaces) meet is the merge point (MP).

The following is sample output from the **showiprsvpsenderdetail** command at the MP during an FLR procedure:

```
Router# show ip rsvp sender detail

PATH:
   Destination 192.168.101.21, Protocol_Id 17, Don't Police , DstPort 1
   Sender address: 10.10.10.10, port: 1
   Path refreshes:
     arriving: from PHOP 172.16.37.35 on Et1/0 every 30000 msecs
Traffic params - Rate: 9K bits/sec, Max. burst: 9K bytes
     Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
   Path ID handle: 09000406.
   Incoming policy: Accepted. Policy source(s): Default
   Status: Proxy-terminated
   Path FLR: Never repaired
   MP - Old Segments: 1
    Input on Serial2/0, phop 172.16.36.35
    Time before expiry: 9 refreshes
```

The table below describes the significant fields shown in the display.

*Table 161: show ip rsvp sender detail Field Descriptions--at the MP During FLR*

| Field | Descriptions |
|---|---|
| PATH | PATH message information:<br>• Destination IP address.<br>• Protocol ID number.<br>• Policing.<br>• Destination port number. |
| Sender address | Source IP address of the PATH message.<br>• port--Number of the source port. |
| Path refreshes | Refresh information:<br>• IP address of the source (previous hop [PHOP]).<br>• Interface name and number.<br>• Frequency, in milliseconds (ms). |
| Traffic params | Traffic parameters in effect:<br>• Rate--Speed, in kilobits per second.<br>• Max. burst--Largest amount of data allowed, in kilobytes.<br>• Min Policed Unit--Size, in bytes, of the smallest packet generated by the application, including the application data and all protocol headers at or above the IP level.<br>• Max Pkt Size--Largest packet allowed, in bytes. |
| PATH ID handle | Internal database ID assigned to the PATH message by RSVP for bookkeeping purposes. |
| Incoming policy | State of the incoming policy:<br>• Accepted--RSVP PATH messages are being accepted, but not forwarded.<br>• Not Accepted--RSVP PATH messages are being rejected. |
| Policy source(s) | Type of local policy in effect; values are Default, Local, and MPLS/TE. |

| Field | Descriptions |
|---|---|
| Status | Status of the local policy:<br>• Proxied--Head.<br>• Proxy-terminated--Tail.<br>• Blockaded--Tail or midpoint and an RESVERROR message have recently been received; therefore, the PSB enters the blockaded state.<br>**Note** A blank field means none of the above. |
| *Path FLR* | Never repaired--Indicates that the node has never been a PLR and, therefore, has never repaired the PSB. |
| MP - Old Segments | The number of old segments or interfaces on the MP before the PLR initiated the FLR procedure. For each old segment,the following information displays:<br>• Input on *interface*--Inbound interface and the previous-hop IP address.<br>• Time before expiry--Number of PATH messages to be received on other segments before this segment expires. |

## Examples

The following is sample output from the **showiprsvpsenderdetail** command at the PLR after an FLR procedure:

```
Router# show ip rsvp sender detail

PATH:
   Destination 192.168.101.21, Protocol_Id 17, Don't Police , DstPort 1
   Sender address: 10.10.10.10, port: 1
   Path refreshes:
     arriving: from PHOP 172.16.31.34 on Et0/0 every 30000 msecs
   Traffic params - Rate: 9K bits/sec, Max. burst: 9K bytes
     Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
   Path ID handle: 05000401.
   Incoming policy: Accepted. Policy source(s): Default
   Status:
   Output on Serial3/0. Policy status: Forwarding. Handle: 3B000406
     Policy source(s): Default
   Path FLR: Started 12:56:16 EST Thu Nov 16 2006, PSB repaired 532(ms) after.
           Resv/Perr: Received 992(ms) after.
```

The table below describes the significant fields shown in the display.

*Table 162: show ip rsvp sender detail Field Descriptions--At the PLR After FLR*

| Field | Descriptions |
|---|---|
| PATH | PATH message information including the following:<br>• Destination IP address.<br>• Protocol ID number.<br>• Policing.<br>• Destination port number. |
| Sender address | Source IP address of the PATH message.<br>• port--Number of the source port. |
| Path refreshes | Refresh information including the following:<br>• IP address of the source (previous hop [PHOP]).<br>• Interface name and number.<br>• Frequency, in milliseconds (ms). |
| Traffic params | Traffic parameters in effect:<br>• Rate--Speed, in kilobits per second.<br>• Max. burst--Largest amount of data allowed, in kilobytes.<br>• Min Policed Unit--Size, in bytes, of the smallest packet generated by the application, including the application data and all protocol headers at or above the IP level.<br>• Max Pkt Size--Largest packet allowed, in bytes. |
| Path ID handle | Internal database ID assigned to the PATH message by RSVP for bookkeeping purposes. |
| Incoming policy | State of the incoming policy:<br>• Accepted--RSVP PATH messages are being accepted, but not forwarded.<br>• Not Accepted--RSVP PATH messages are being rejected. |
| Policy source(s) | Type of local policy in effect; values are Default, Local, and MPLS/TE. |

| Field | Descriptions |
|---|---|
| Status | Status of the local policy:<br>• Proxied--Head.<br>• Proxy-terminated--Tail.<br>• Blockaded--Tail or midpoint and an RESVERROR message have recently been received; therefore, the PSB enters the blockaded state.<br>**Note** A blank field means none of the above. |
| Output on Serial3/0 | Policy status (on the outbound interface):<br>• Forwarding--Inbound PATH messages are being forwarded.<br>• Not Forwarding--Outbound PATH messages are being rejected.<br>• Handle--Internal database ID assigned to the PATH message by RSVP for bookkeeping purposes. |
| Policy source(s) | Type of local policy in effect; values are Default, Local, and MPLS/TE. |
| *Path FLR* | FLR statistics that show when RSVP received the notification from RIB and how long thereafter the PATH message was sent. This delay can result when the interface on which the PATH message was sent had a wait time configured or when other PSBs were processed before this one or a combination of both. The statistics also show when an associated RESV or PATHERROR message was received.<br>**Note** This delay tells you the time when Quality of Service (QoS) was not honored for the specified flow. |

## Examples

The following is sample output from the **showiprsvpsenderdetail** command when TBAC is configured:

```
Router# show ip rsvp sender detail

PATH:
  Destination 10.0.0.3, Protocol_Id 17, Don't Police , DstPort 2
  Sender address: 10.0.0.1, port: 2
  Path refreshes:
    arriving: from PHOP 10.1.1.1 on Et0/0 every 30000 msecs. Timeout in 189 sec
  Traffic params - Rate: 10K bits/sec, Max. burst: 10K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
```

```
Path ID handle: 02000412.
Incoming policy: Accepted. Policy source(s): Default
Status:
Output on Tunnel1, out of band. Policy status: Forwarding. Handle: 0800040E
  Policy source(s): Default
Path FLR: Never repaired
```

The table below describes the significant fields shown in the display.

***Table 163: show ip rsvp sender detail Field Descriptions--With TBAC***

| Field | Descriptions |
|---|---|
| PATH | PATH message information:<br>• Destination IP address.<br>• Protocol ID number.<br>• Policing.<br>• Destination port number. |
| Sender address | Source IP address of the PATH message.<br>• port--Number of the source port. |
| Path refreshes | Refresh information:<br>• IP address of the source (previous hop [PHOP]).<br>• Interface name and number.<br>• Frequency, in milliseconds (ms).<br>**Note** A blank field means no refreshes have occurred. |
| Traffic params | Traffic parameters in effect:<br>• Rate--Speed, in kilobits per second.<br>• Max. burst--Largest amount of data allowed, in kilobytes.<br>• Min Policed Unit--Size, in bytes, of the smallest packet generated by the application, including the application data and all protocol headers at or above the IP level.<br>• Max Pkt Size--Largest packet allowed, in bytes. |
| PATH ID handle | Internal database ID assigned to the PATH message by RSVP for bookkeeping purposes. |

| Field | Descriptions |
|---|---|
| Incoming policy | State of the incoming policy:<br>• Accepted--RSVP PATH messages are being accepted, but not forwarded.<br>• Not Accepted--RSVP PATH messages are being rejected. |
| Policy source(s) | Type of local policy in effect; values are Default, Local, and MPLS/TE. |
| Status | Status of the local policy:<br>• Proxied--Head.<br>• Proxy-terminated--Tail.<br>• Blockaded--Tail or midpoint and an RESVERROR message have recently been received; therefore, the PSB enters the blockaded state.<br>**Note** A blank field means none of the above. |
| Output on Tunnel1 | Policy status (on the outbound tunnel with out-of-band signaling):<br>• Forwarding--Inbound PATH messages are being forwarded.<br>• Not Forwarding--Outbound PATH messages are being rejected.<br>• Handle--Internal database ID assigned to the PATH message by RSVP for bookkeeping purposes. |
| Policy source(s) | Type of local policy in effect; values are Default, Local, and MPLS/TE. |
| Path FLR | Never repaired--Indicates that the node has never been a point of local repair (PLR) and, therefore, has never repaired the PSB. |

## Examples

The following is sample output from the **showiprsvpsenderdetail** command when RSVP aggregation is configured:

```
Router# show ip rsvp sender detail
```

```
PATH:
  Destination 10.10.10.21, Protocol_Id 17, Don't Police , DstPort 1
  Sender address: 10.10.10.11, port: 1
  Path refreshes:
    arriving: from PHOP 10.10.10.34 on Et1/0 every 30000 msecs
  Traffic params - Rate: 10K bits/sec, Max. burst: 10K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
  Path ID handle: 0F000406.
  Incoming policy: Accepted. Policy source(s): Default
  Status:
  3175 Aggregation: agg_info : AggResv 10.10.10.34->10.10.10.2_46
  Output on Serial2/0. Policy status: Forwarding. Handle: 09000405
    Policy source(s): Default
  Path FLR: Never repaired
PATH:
  Deaggregator 10.10.10.2, DSCP 46, Don't Police
  Aggregator address: 10.10.10.34
  Path refreshes:
    arriving: from PHOP 192.168.34.36 on Et1/0 every 30000 msecs
  Traffic params - Rate: 17179868160 bits/sec, Max. burst: 536870784 bytes
    Min Policed Unit: 1 bytes, Max Pkt Size 2147483647 bytes
  Path ID handle: 1500040A.
  Incoming policy: Accepted. Policy source(s): Default
  Status: Proxy-terminated
  Path FLR: Never repaired
```

The table below describes the significant fields shown in the display.

***Table 164: show ip rsvp sender detail Field Descriptions--With RSVP Aggregation***

| Field | Descriptions |
|---|---|
| PATH | PATH message information for E2E reservations:<br>• Destination IP address.<br>• Protocol ID number.<br>• Policing.<br>  • Always Don't Police.<br>• Destination port number. |
| Sender address | Source IP address of the PATH message.<br>• port--Number of the source port. |
| Path refreshes | Refresh information:<br>• IP address of the source (previous hop [PHOP]).<br>• Interface name and number.<br>• Frequency, in milliseconds (ms).<br>**Note** A blank field means no refreshes have occurred. |

| Field | Descriptions |
|---|---|
| Traffic params | Traffic parameters in effect:<br>• Rate--Speed, in kilobits per second.<br>  • Always MAX rate possible for aggregate reservations.<br>• Max. burst--Largest amount of data allowed, in kilobytes.<br>  • Always MAX burst possible for aggregate reservations.<br>• Min Policed Unit--Size, in bytes, of the smallest packet generated by the application, including the application data and all protocol headers at or above the IP level.<br>• Max Pkt Size--Largest packet allowed, in bytes. |
| PATH ID handle | Internal database ID assigned to the PATH message by RSVP for bookkeeping purposes. |
| Incoming policy | State of the incoming policy:<br>• Accepted--RSVP PATH messages are being accepted, but not forwarded.<br>• Not Accepted--RSVP PATH messages are being rejected. |
| Policy source(s) | Type of local policy in effect; values are Default, Local, and MPLS/TE. |
| Status | Status of the local policy:<br>• Proxied--Head.<br>• Proxy-terminated--Tail.<br>• Blockaded--Tail or midpoint and an RESVERROR message have recently been received; therefore, the PSB enters the blockaded state.<br>**Note** A blank field means none of the above. |
| 3175 Aggregation: agg_info | IP address of the aggregated reservation on which this E2E reservation is mapped with specified source (aggregator) and destination (deaggregator) endpoints and DSCP. |

| Field | Descriptions |
|---|---|
| Output on Serial2/0 | Policy status (on the outbound interface):<br>• Forwarding--Inbound PATH messages are being forwarded.<br>• Not Forwarding--Outbound PATH messages are being rejected.<br>• Handle--Internal database ID assigned to the PATH message by RSVP for bookkeeping purposes. |
| Policy source(s) | Type of local policy in effect; values are Default, Local, and MPLS/TE. |
| Path FLR | Never repaired--Indicates that the node has never been a point of local repair (PLR) and, therefore, has never repaired the PSB. |
| PATH | PATH message information for aggregate reservations:<br>• Deaggregator IP address.<br>• Differentiated Services Code Point (DSCP) value.<br>• Policing.<br>• Always Don't Police.<br>• Aggregator IP address.<br>**Note** Remaining parameters are defined in the preceding fields. |

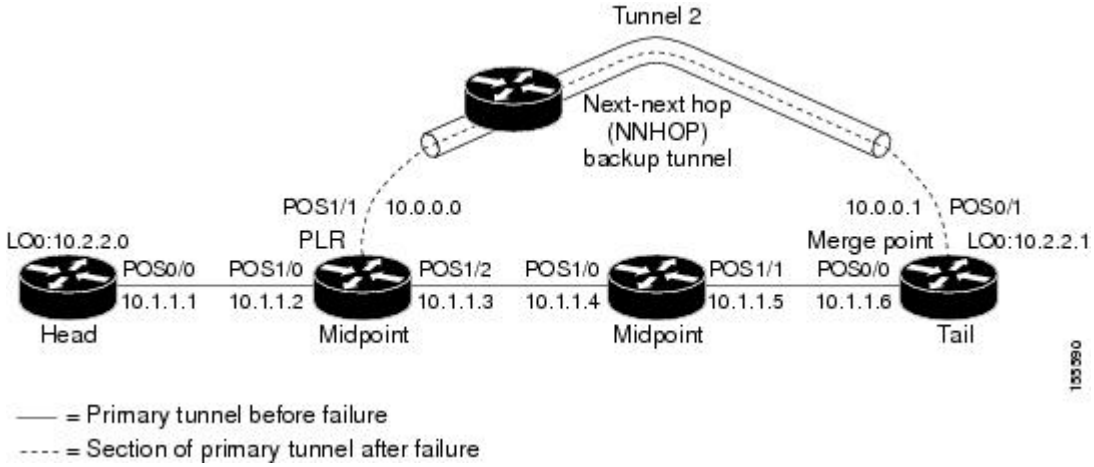
## Examples

The following is sample output from the **showiprsvpsenderdetail** command under these circumstances:

- The command is entered at the PLR before a failure (Example 1).
- The command is entered at the PLR after a failure (Example 2).
- The command is entered at the MP before a failure (Example 3).
- The command is entered at the MP after a failure (Example 4).
- The command output shows all senders (Example 5).
- The command output shows only senders who have a specific destination (Example 6).
- The command output shows more detail about a sender who has a specific destination (Example 7).

This figure illustrates the network topology for the RSVP configuration example.

***Figure 66: Network Topology for the RSVP Configuration Example***




## Examples

The following is sample output from the **showiprsvpsenderdetail** command when it is entered at the PLR before a failure:

```
Router# show ip rsvp sender detail
PATH:
   Tun Dest: 10.2.2.1 Tun ID: 1 Ext Tun ID: 10.2.2.0
   Tun Sender: 10.2.2.0, LSP ID: 126
   Path refreshes arriving on POS1/0 from PHOP 10.1.1.1
   Path refreshes being sent to NHOP 10.1.1.4 on POS1/1
   Session Attr::
     Setup Prio: 0, Holding Prio: 0
     Flags: Local Prot desired, Label Recording, SE Style
     Session Name:tagsw4500-23_t1
   ERO:
     10.1.1.4 (Strict IPv4 Prefix, 8 bytes, /32)
     10.1.1.5 (Strict IPv4 Prefix, 8 bytes, /32)
     10.1.1.6 (Strict IPv4 Prefix, 8 bytes, /32)
     10.2.2.1 (Strict IPv4 Prefix, 8 bytes, /32)
   Traffic params - Rate: 0G bits/sec, Max. burst: 1K bytes
   Fast-Reroute Backup info:
     Inbound  FRR: Not active
     Outbound FRR: Ready -- backup tunnel selected
       Backup Tunnel: Tu2          (label 0)
       Bkup Sender Template:
         Tun Sender: 10.0.0.0, LSP ID: 126
       Bkup FilerSpec:
         Tun Sender: 10.0.0.0, LSP ID 126
```

The table below describes the significant fields shown in the display.

**Note** The Flags field is important for Fast Reroute. For information about flags that must be set, see the Flags field description in the table.

*Table 165: show ip rsvp sender detail Field Descriptions--On PLR Before Failure*

| Field | Description |
|---|---|
| **The first five fields provide information that uniquely identifies the LSP.**<br>**The first three fields identify the LSP's session (that is, the contents of the SESSION object in arriving PATH messages).** | |
| Tun Dest | IP address of the destination of the tunnel. |
| Tun ID | Tunnel identification number. |
| Ext Tun ID | Extended tunnel identification number. |
| **The next two fields identify the LSP's sender (SENDER_TEMPLATE object of arriving PATH messages).** | |
| Tun Sender | Tunnel sender. |
| LSP ID | LSP identification number. |
| **The remaining fields indented under PATH provide additional information about this LSP.** | |
| **Session Attr** --Session attributes. Refers to information included in the SESSION_ATTRIBUTE object of arriving PATH messages, such as the Setup and Holding Priorities, Flags, and the Session Name. | |
| Setup Prio | Setup priority. |
| Holding Prio | Holding priority. |
| Flags | An LSP must have the "Local protection desired" flag of the SESSION_ATTRIBUTE object set for the LSP to use a backup tunnel (that is, in order to receive local protection). If this flag is not set, you have not enabled Fast Reroute for this tunnel at its headend (by entering the **tunnelmplstraffic-engfast-reroute** command). Next-next hop (NNHOP) backup tunnels rely on label recording, so LSPs should have the "label recording desired" flag set too. This flag is set if the tunnel was configured for Fast Reroute. |

| Field | Description |
|---|---|
| **ERO** --Refers to the EXPLICIT_ROUTE Object (ERO) of the PATH messages. This field displays the contents of the ERO at this node. As a PATH message travels from the sender (headend) to the receiver (tailend), each node removes its own IP address from the ERO. The displayed value reflects the remainder of hops between this node and the tail. | |
| **Fast-Reroute Backup info** --Information that is relevant to Fast Reroute for this LSP. | |
| Inbound FRR | If this node is downstream from a rerouted LSP (for example, at a merge point for this LSP), the state is Active. |
| Outbound FRR | If this node is a PLR for an LSP, there are three possible states:<br>• Active--This LSP is actively using its backup tunnel, presumably because there has been a downstream failure.<br>• No Backup--This LSP does not have local (Fast Reroute) protection. No backup tunnel has been selected for it to use in case of a failure.<br>• Ready--This LSP is ready to use a backup tunnel in case of a downstream link or node failure. A backup tunnel has been selected for it to use. |
| Backup Tunnel | If the Outbound FRR state is Ready or Active, this field indicates the following:<br>• Which backup tunnel has been selected for this LSP to use in case of a failure.<br>• The inbound label that will be prepended to the LSP's data packets for acceptance at the backup tunnel tail (the merge point). |

| Field | Description |
|---|---|
| Bkup Sender Template | If the Outbound FRR state is Ready or Active, SENDER_TEMPLATE and FILTERSPEC objects are shown. These objects will be used in RSVP messages sent by the backup tunnel if the LSP starts actively using the backup tunnel. They differ from the original (prefailure) objects only in that the node (the PLR) substitutes its own IP address for that of the original sender. For example, PATH and PATHTEAR messages will contain the new SENDER_TEMPLATE. RESV and RESVTEAR messages will contain the new FILTERSPEC object. If this LSP begins actively using the backup tunnel, the display changes. |
| Bkup FilerSpec | If the Outbound FRR state is Ready or Active, SENDER_TEMPLATE and FILTERSPEC objects are shown. These objects will be used in RSVP messages sent by the backup tunnel if the LSP starts actively using the backup tunnel. They differ from the original (prefailure) objects only in that the node (the PLR) substitutes its own IP address for that of the original sender. For example, PATH and PATHTEAR messages will contain the new SENDER_TEMPLATE. RESV and RESVTEAR messages will contain the new FILTERSPEC object. If this LSP begins actively using the backup tunnel, the display changes as shown in Example 2. |

## Examples

If the LSP begins actively using the backup tunnel and the command is entered at the PLR after a failure, the display changes as shown in the following output.

```
Router# show ip rsvp sender detail
PATH:
   Tun Dest: 10.2.2.1 Tun ID: 1 Ext Tun ID: 10.2.2.0
   Tun Sender: 10.2.2.0, LSP ID: 126
   Path refreshes arriving on POS1/0 from PHOP 10.1.1.1
   Path refreshes being sent to NHOP 10.2.2.1 on Tunnel2
   Session Attr::
     Setup Prio: 0, Holding Prio: 0
     Flags: Local Prot desired, Label Recording, SE Style
     Session Name:tagsw4500-23_t1
   ERO:
     10.2.2.1 (Strict IPv4 Prefix, 8 bytes, /32)
     10.2.2.1 (Strict IPv4 Prefix, 8 bytes, /32)
   Traffic params - Rate: 0G bits/sec, Max. burst: 1K bytes
   Fast-Reroute Backup info:
     Inbound  FRR: Not active
     Outbound FRR: Active -- using backup tunnel
       Backup Tunnel: Tu2        (label 0)
       Bkup Sender Template:
         Tun Sender: 10.0.0.0, LSP ID: 126
       Bkup FilerSpec:
         Tun Sender: 10.0.0.0, LSP ID 126
```

```
      Orig Output I/F: Et2
      Orig Output ERO:
        10.1.1.4 (Strict IPv4 Prefix, 8 bytes, /32)
        10.1.1.5 (Strict IPv4 Prefix, 8 bytes, /32)
        10.1.1.6 (Strict IPv4 Prefix, 8 bytes, /32)
        10.2.2.1 (Strict IPv4 Prefix, 8 bytes, /32)
```

Once an LSP is actively using a backup tunnel, the following changes occur:

- PATH refreshes are no longer sent to the original NHOP out the original interface. They are sent through the backup tunnel to the node that is the tail of the backup tunnel (NHOP or NNHOP).
- The ERO is modified so that it will be acceptable upon arrival at the NHOP or NNHOP.
- The display shows both the original ERO and the new one that is now being used.
- The display shows the original output interface (that is, the interface from which PATH messages were sent for this LSP before the failure).

## Examples

If the same **showiprsvpsender** command is entered at the merge point (the backup tunnel tail), the display changes from before to after the failure. The following is sample output before a failure:

```
Router# show ip rsvp sender detail
PATH:
   Tun Dest: 10.2.2.1 Tun ID: 1 Ext Tun ID: 10.2.2.0
   Tun Sender: 10.2.2.0, LSP ID: 126
   Path refreshes arriving on POS0/0 from PHOP 10.1.1.5
   Session Attr::
     Setup Prio: 0, Holding Prio: 0
     Flags: Local Prot desired, Label Recording, SE Style
     Session Name:tagsw4500-23_t1
   Traffic params - Rate: 0G bits/sec, Max. burst: 1K bytes
   Fast-Reroute Backup info:
     Inbound  FRR: Not active
     Outbound FRR: No backup tunnel selected
```

## Examples

After a failure, the following changes occur:

- The interface and previous hop (PHOP) from which PATH messages are received will change.
- The inbound FRR becomes Active.
- The original PHOP and the original input interface are displayed as shown in the following output.

The following is sample output after a failure:

```
Router# show ip rsvp sender detail
PATH:
   Tun Dest: 10.2.2.1 Tun ID: 1 Ext Tun ID: 10.2.2.0
   Tun Sender: 10.2.2.0, LSP ID: 126
   Path refreshes arriving on POS0/1 from PHOP 10.0.0.0 on Loopback0
   Session Attr::
     Setup Prio: 0, Holding Prio: 0
     Flags: Local Prot desired, Label Recording, SE Style
     Session Name:tagsw4500-23_t1
   Traffic params - Rate: 0G bits/sec, Max. burst: 1K bytes
   Fast-Reroute Backup info:
     Inbound  FRR: Active
       Orig Input I/F: POS0/0
       Orig PHOP: 10.1.1.5
       Now using Bkup Filterspec w/ sender: 10.0.0.0 LSP ID: 126
     Outbound FRR: No backup tunnel selected
```

Notice the following changes:

- After a failure, PATH refreshes arrive on a different interface and from a different PHOP.
- The original PHOP and input interface are shown under Fast-Reroute Backup information, along with the FILTERSPEC object that will now be used when sending messages (such as RESV and RESVTEAR).

## Examples

In the following example, information about all senders is displayed:

```
Router# show ip rsvp sender
To              From              Pro DPort Sport Prev Hop        I/F  BPS  Bytes
10.2.2.1        10.2.2.0          1   1     59    10.1.1.1        Et1   0G     1K
10.2.2.1        172.31.255.255    1   2     9                           0G     1K
10.2.2.1        10.2.2.0          1   3     12    10.1.1.1        Et1   0G     1K
10.2.2.1        172.31.255.255    1   3     20                          0G     1K
172.16.0.0      172.31.255.255    1   0     23                          0G     1K
172.16.0.0      172.31.255.255    1   1     22                          0G     1K
172.16.0.0      172.31.255.255    1   1000  22                          0G     1K
```

The table below describes the significant fields shown in the display.

***Table 166: show ip rsvp sender Field Descriptions***

| Field | Description |
|---|---|
| To | IP address of the receiver. |
| From | IP address of the sender. |
| Pro | Protocol code. Code 1 indicates Internet Control Message Protocol (ICMP). |
| DPort | Destination port number. |
| Sport | Source port number. |
| Prev Hop | IP address of the previous hop. |
| I/F | Interface of the previous hop. |
| BPS | Reservation rate, in bits per second, that the application is advertising it might achieve. |
| Bytes | Bytes of burst size that the application is advertising it might achieve. |

## Examples

To show only information about senders having a specific destination, specify the destination filter as shown in the following output. In this example, the destination is 172.16.0.0.

```
Router# show ip rsvp sender filter destination 172.16.0.0
To          From         Pro DPort Sport Prev Hop    I/F  BPS  Bytes
172.16.0.0  172.31.255   1   0     23                    0G     1K
172.16.0.0  172.31.255   1   1     22                    0G     1K
172.16.0.0  172.31.255   1   1000  22                    0G     1K
```

**Examples**

To show more detail about the sender whose destination port is 1000 (as shown in Example 6), specify the command with the destination port filter:

```
Router# show ip rsvp sender filter detail dst-port 1000
PATH:
  Tun Dest 172.16.0.0 Tun ID 1000 Ext Tun ID 172.31.255.255
  Tun Sender: 172.31.255.255, LSP ID: 22
  Path refreshes being sent to NHOP 10.1.1.4 on Ethernet2
  Session Attr::
    Setup Prio: 7, Holding Prio: 7
    Flags: SE Style
    Session Name:tagsw4500-25_t1000
  ERO:
    10.1.1.4 (Strict IPv4 Prefix, 8 bytes, /32)
    172.16.0.0 (Strict IPv4 Prefix, 8 bytes, /32)
  Traffic params - Rate: 0G bits/sec, Max. burst: 1K bytes
  Fast-Reroute Backup info:
    Inbound  FRR: Not active
    Outbound FRR: No backup tunnel selected
```

**Examples**

The following is sample output from the **showiprsvpsendervrfmyvrfdetail** command showing all the senders associated with the VRF named myvrf:

```
Router# show ip rsvp sender detail vrf myvrf
PATH:
  Destination 10.10.10.21, Protocol_Id 17, Don't Police , DstPort 1
  Sender address: 10.10.10.11, port: 1
  Path refreshes:
Traffic params - Rate: 10K bits/sec, Max. burst: 10K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
  Path ID handle: 0F000406.
  Incoming policy: Accepted. Policy source(s): Default
  Status: Proxied
Output on Serial2/0. Policy status: Forwarding. Handle: 09000405
    Policy source(s): Default
  Path FLR: Never repaired
  VRF: myvrf
```

The table below describes the significant fields shown in the display.

***Table 167: show ip rsvp sender detail Field Descriptions--With VRF***

| Field | Descriptions |
|---|---|
| PATH | PATH message information for E2E reservations:<br>• Destination IP address.<br>• Protocol ID number.<br>• Policing.<br>  • Always Don't Police.<br>• Destination port number. |
| Sender address | Source IP address of the PATH message.<br>• port--Number of the source port. |

| Field | Descriptions |
|---|---|
| Path refreshes | Refresh information:<br>• IP address of the source (previous hop [PHOP]).<br>• Interface name and number.<br>• Frequency, in milliseconds (ms).<br>**Note** A blank field means no refreshes have occurred. |
| Traffic params | Traffic parameters in effect:<br>• Rate--Speed, in kilobits per second.<br>  • Always MAX rate possible for aggregate reservations.<br>• Max. burst--Largest amount of data allowed, in kilobytes.<br>  • Always MAX burst possible for aggregate reservations.<br>• Min Policed Unit--Size, in bytes, of the smallest packet generated by the application, including the application data and all protocol headers at or above the IP level.<br>• Max Pkt Size--Largest packet allowed, in bytes. |
| PATH ID handle | Internal database ID assigned to the PATH message by RSVP for bookkeeping purposes. |
| Incoming policy | State of the incoming policy:<br>• Accepted--RSVP PATH messages are being accepted, but not forwarded.<br>• Not Accepted--RSVP PATH messages are being rejected. |
| Policy source(s) | Type of local policy in effect; values are Default, Local, and MPLS/TE. |

| Field | Descriptions |
|---|---|
| Status | Status of the local policy:<br>• Proxied--Head.<br>• Proxy-terminated--Tail.<br>• Blockaded--Tail or midpoint and an RESVERROR message have recently been received; therefore, the PSB enters the blockaded state.<br>**Note** A blank field means none of the above. |
| Output on Serial2/0 | Policy status (on the outbound interface):<br>• Forwarding--Inbound PATH messages are being forwarded.<br>• Not Forwarding--Outbound PATH messages are being rejected.<br>• Handle--Internal database ID assigned to the PATH message by RSVP for bookkeeping purposes. |
| Policy source(s) | Type of local policy in effect; values are Default, Local, and MPLS/TE. |
| Path FLR | Never repaired--Indicates that the node has never been a point of local repair (PLR) and, therefore, has never repaired the PSB. |
| VRF | Name of the VRF for which senders are displayed. |

## Examples

The following is sample output from the **showiprsvpsenderdetail**command showing point-to-multipoint information:

```
Router# show ip rsvp sender detail

P2MP ID: 22  Tun ID: 22  Ext Tun ID: 10.1.1.201
  Tun Sender: 10.1.1.201  LSP ID: 1  SubGroup Orig: 10.1.1.201
  SubGroup ID: 1
  S2L Destination : 10.1.1.203
  Path refreshes:
    sent:     to   NHOP 10.0.0.205 on Ethernet0/0
  Session Attr:
    Setup Prio: 7, Holding Prio: 7
    Flags: (0xF) Local Prot desired, Label Recording, SE Style, Bandwidth Prot desired
    Session Name: R201_t22
  ERO: (incoming)
    10.1.1.201 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.0.201 (Strict IPv4 Prefix, 8 bytes, /32)
    10.0.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
```

```
    10.1.1.205 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.1.202 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.0.202 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.0.203 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.1.203 (Strict IPv4 Prefix, 8 bytes, /32)
  ERO: (outgoing)
    10.0.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.1.205 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.1.202 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.0.202 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.0.203 (Strict IPv4 Prefix, 8 bytes, /32)
    10.1.1.203 (Strict IPv4 Prefix, 8 bytes, /32)
  Traffic params - Rate: 500K bits/sec, Max. burst: 1K bytes
    Min Policed Unit: 1 bytes, Max Pkt Size 2147483647 bytes
  Fast-Reroute Backup info:
    Inbound  FRR: Not active
    Outbound FRR: Ready -- backup tunnel selected
      Backup Tunnel: Tu666      (label 20)
      Bkup Sender Template:
        Tun Sender: 10.0.2.201  LSP ID: 1  SubGroup Orig: 10.1.1.201
        SubGroup ID: 1
      Bkup FilerSpec:
        Tun Sender: 10.0.2.201, LSP ID: 1, SubGroup Orig: 10.1.1.201
        SubGroup ID: 1
  Path ID handle: 01000414.
  Incoming policy: Accepted. Policy source(s): MPLS/TE
  Status: Proxied
  Output on Ethernet0/0. Policy status: Forwarding. Handle: 02000413
    Policy source(s): MPLS/TE
```

The table below describes the significant fields shown in the display.

***Table 168: show ip rsvp sender--MPLS TE P2MP Field Descriptions***

| Field | Description |
|---|---|
| P2MP ID | A 32-bit number that identifies the set of destinations of the P2MP tunnel. |
| Tun ID | Tunnel identification number. |
| Ext Tun ID | Extended tunnel identification number. |
| Tun Sender | IP address of the sender. |
| LSP ID | Label switched path identification number. |
| SubGroup Orig | LSP headend router ID address. |
| SubGroup ID | An incremental number assigned to each sub-LSP signaled from the headend router. |
| S2L Destination | LSP tailend router ID address. |

The following is sample output from the **showiprsvpsenderfiltersession-type13**command, which shows RSVP RESV requests for point-to-multipoint traffic:

```
Router# show ip rsvp sender filter session-type 13

Session Type 13 (te-p2mp-lsp)
```

```
Destination     Tun Sender      TunID LSPID P2MP-ID    SubID I/F      BPS
10.1.1.203       10.1.1.201       22    1     22          1     none     500K
10.1.1.206       10.1.1.201       22    1     22          2     none     500K
10.1.1.213       10.1.1.201       22    1     22          3     none     500K
10.1.1.214       10.1.1.201       22    1     22          4     none     500K
10.1.1.216       10.1.1.201       22    1     22          5     none     500K
10.1.1.217       10.1.1.201       22    1     22          6     none     500K
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp sender** | Enables a router to simulate RSVP PATH message reception from the sender. |
| **show ip rsvp reservation** | Displays RSVP PATH-related receiver information currently in the database. |

# show ip rsvp signalling

To display Resource Reservation Protocol (RSVP) signaling information that optionally includes rate-limiting and refresh-reduction parameters for RSVP messages, use the **showiprsvpsignalling**command in EXEC mode.

**show ip rsvp signalling** [**rate-limit**| **refresh reduction**]

## Syntax Description

| | |
|---|---|
| **rate-limit** | (Optional) Rate-limiting parameters for signalling messages. |
| **refresh reduction** | (Optional) Refresh-reduction parameters and settings. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |

## Usage Guidelines

Use the **showiprsvpsignalling**command witheitherthe**rate-limit**or the**refreshreduction** keyword to display rate-limiting parameters or refresh-reduction parameters, respectively.

## Examples

The following command shows rate-limiting parameters:

```
Router# show ip rsvp signalling rate-limit
Rate Limiting:enabled
  Max msgs per interval:4
  Interval length (msec):20
  Max queue size:500
  Max msgs per second:200
  Max msgs allowed to be sent:37
```

The table below describes the fields shown in the display.

*Table 169: show ip rsvp signalling rate-limit Command Field Descriptions*

| Field | Description |
|---|---|
| Rate Limiting: enabled (active) or disabled (not active) | The RSVP rate-limiting parameters in effect including the following:<br>• Max msgs per interval = number of messages allowed to be sent per interval (timeframe).<br>• Interval length (msecs) = interval (timeframe) length in milliseconds.<br>• Max queue size = maximum size of the message queue in bytes.<br>• Max msgs per second = maximum number of messages allowed to be sent per second. |

The following command shows refresh-reduction parameters:

```
Router# show ip rsvp signalling refresh reduction
Refresh Reduction:enabled
  ACK delay (msec):250
  Initial retransmit delay (msec):1000
  Local epoch:0x74D040
  Message IDs:in use 600, total allocated 3732, total freed 3132
```

The table below describes the fields shown in the display.

*Table 170: show ip rsvp signalling refresh reduction Command Field Descriptions*

| Field | Description |
|---|---|
| Refresh Reduction: enabled (active) or disabled (not active) | The RSVP refresh-reduction parameters in effect including the following:<br>• ACK delay (msec) = how long in milliseconds before the receiving router sends an acknowledgment (ACK).<br>• Initial retransmit delay (msec) = how long in milliseconds before the sending router retransmits a message.<br>• Local epoch = the RSVP process identifier that defines a local router for refresh reduction and reliable messaging; randomly generated each time a node reboots or the RSVP process restarts.<br>• Message IDs = the number of message identifiers (IDs) in use, the total number allocated, and the total number available (freed). |

## Related Commands

| Command | Description |
|---|---|
| **clear ip rsvp signalling rate-limit** | Clears the counters recording dropped messages. |
| **clear ip rsvp signalling refresh reduction** | Clears the counters recording retransmissions and out-of-order messages. |
| **debug ip rsvp rate-limit** | Displays debug messages for RSVP rate-limiting events. |
| **ip rsvp signalling rate-limit** | Controls the transmission rate for RSVP messages sent to a neighboring router during a specified amount of time. |
| **ip rsvp signalling refresh reduction** | Enables refresh reduction. |

# show ip rsvp signalling blockade

To display the Resource Reservation Protocol (RSVP) sessions that are currently blockaded, use the **showiprsvpsignallingblockade**command in EXEC mode.

**show ip rsvp signalling blockade [detail]** [*name*| *address*]

## Syntax Description

| | |
|---|---|
| **detail** | (Optional) Additional blockade information. |
| *name* | (Optional) Name of the router being blockaded. |
| *address* | (Optional) IP address of the destination of a reservation. |

## Command Default

If you enter the **showiprsvpsignallingblockade**command without a keyword or an argument, the command displays all the blockaded sessions on the router.

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |

## Usage Guidelines

Use the show ip rsvp signalling blockade command to display the RSVP sessions that are currently blockaded.

An RSVP sender becomes blockaded when the corresponding receiver sends a Resv message that fails admission control on a router that has RSVP configured. A ResvError message with an admission control error is sent in reply to the Resv message, causing all routers downstream of the failure to mark the associated sender as blockaded. As a result, those routers do not include that contribution to subsequent Resv refreshes for that session until the blockade state times out.

Blockading solves a denial-of-service problem on shared reservations where one receiver can request so much bandwidth as to cause an admission control failure for all the receivers sharing that reservation, even though the other receivers are making requests that are within the limit.

## Examples

The following example shows all the sessions currently blockaded:

```
Router# show ip rsvp signalling blockade
To              From            Pro DPort Sport Time Left Rate
192.168.101.2   192.168.101.1   UDP 1000  1000  27        5K
192.168.101.2   192.168.101.1   UDP 1001  1001  79        5K
192.168.101.2   192.168.101.1   UDP 1002  1002  17        5K
225.1.1.1       192.168.104.1   UDP 2222  2222  48        5K
```

The table below describes the fields shown in the display.

***Table 171: show ip rsvp signalling blockade Command Field Descriptions***

| Field | Description |
|---|---|
| To | IP address of the receiver. |
| From | IP address of the sender. |
| Pro | Protocol used. |
| DPort | Destination port number. |
| Sport | Source port number. |
| Time Left | Amount of time, in seconds, before the blockade expires. |
| Rate | The average rate, in bits per second, for the data. |

The following example shows more detail about the sessions currently blockaded:

```
Router# show ip rsvp signalling blockade detail
Session address: 192.168.101.2, port: 1000. Protocol: UDP
Sender address:  192.168.101.1, port: 1000
  Admission control error location: 192.168.101.1
  Flowspec that caused blockade:
    Average bitrate:      5K bits/second
    Maximum burst:        5K bytes
    Peak bitrate:         5K bits/second
    Minimum policed unit: 0 bytes
    Maximum packet size:  0 bytes
    Requested bitrate:    5K bits/second
    Slack:                0 milliseconds
  Blockade ends in:       99 seconds
Session address: 192.168.101.2, port: 1001. Protocol: UDP
Sender address:  192.168.101.1, port: 1001
  Admission control error location: 192.168.101.1
  Flowspec that caused blockade:
    Average bitrate:      5K bits/second
    Maximum burst:        5K bytes
    Peak bitrate:         5K bits/second
    Minimum policed unit: 0 bytes
    Maximum packet size:  0 bytes
    Requested bitrate:    5K bits/second
    Slack:                0 milliseconds
  Blockade ends in:       16 seconds
Session address: 192.168.101.2, port: 1002. Protocol: UDP
Sender address:  192.168.101.1, port: 1002
  Admission control error location: 192.168.101.1
  Flowspec that caused blockade:
    Average bitrate:      5K bits/second
    Maximum burst:        5K bytes
    Peak bitrate:         5K bits/second
    Minimum policed unit: 0 bytes
    Maximum packet size:  0 bytes
    Requested bitrate:    5K bits/second
    Slack:                0 milliseconds
  Blockade ends in:       47 seconds
Session address: 225.1.1.1, port: 2222. Protocol: UDP
```

```
Sender address:  192.168.104.1, port: 2222
  Admission control error location: 192.168.101.1
  Flowspec that caused blockade:
    Average bitrate:      5K bits/second
    Maximum burst:        5K bytes
    Peak bitrate:         5K bits/second
    Minimum policed unit: 0 bytes
    Maximum packet size:  0 bytes
    Requested bitrate:    5K bits/second
    Slack:                0 milliseconds
  Blockade ends in:       124 seconds
```

The table below describes the fields shown in the display.

***Table 172: show ip rsvp signalling blockade detail Command Field Descriptions***

| Field | Description |
|---|---|
| Session address | Destination IP address of the reservation affected by the blockade. |
| port | Destination port number of the reservation affected by the blockade. |
| Protocol | Protocol used by the reservation affected by the blockade; choices include User Datagram Protocol (UDP) and TCP. |
| Sender address | Source IP address of the reservation affected by the blockade. |
| port | Source port number of the reservation affected by the blockade. |
| Admission control error location | IP address of the router where the admission control error occurred. |
| Flowspec that caused blockade | Parameters for the flowspec that caused the blockade. |
| Average bitrate | The average rate, in bits per second, for the flowspec. |
| Maximum burst | The maximum burst size, in bytes, for the flowspec. |
| Peak bitrate | The peak rate, in bps, for the flowspec. |
| Minimum policed unit | The minimum policed unit, in bytes, for the flowspec. |
| Maximum packet size | The maximum packet size, in bytes, for the flowspec. |
| Requested bitrate | The requested rate, in bits per second, for the flowspec. |
| Slack | Time, in milliseconds, allocated to a router for scheduling delivery of packets. |

| Field | Description |
|---|---|
| Blockade ends in | Time, in seconds, until the blockade expires. |

# show ip rsvp signalling fast-local-repair

To display fast-local-repair (FLR)-specific information maintained by Resource Reservation Protocol (RSVP), use the **showiprsvpsignallingfast-local-repair** command in user EXEC or privileged EXEC mode.

**show ip rsvp signalling fast-local-repair** [**statistics [detail]**]

## Syntax Description

| | |
|---|---|
| **statistics** | (Optional) Displays information about FLR procedures. |
| detail | (Optional) Displays additional information about FLR procedures. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRB | This command was introduced. |
| 15.0(1)M | This command was modified. The output was changed to display the virtual routing and forwarding (VRF) name for which the FLR was triggered on the point of local repair (PLR). |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

Use the **showiprsvpsignallingfast-local-repair** command to display the FLR and RSVP message pacing rates that are configured.

Use the **showiprsvpsignallingfast-local-repairstatistics**command to display the FLR procedures and related information including the following:

- The process number
- The state
- The start time
- The number of path state blocks (PSBs) repaired
- The repair rate
- The Routing Information Base (RIB) notification process time
- The repair time of the last PSB

Use the **showiprsvpsignallingfast-local-repairstatisticsdetail**command to display detailed information about FLR procedures including the following:

- The time of the routing notification
- The elapsed time for processing all notifications in the queue
- The rate and pacing unit (the refresh spacing in ms) used
- The number of PSBs repaired
- The number of times RSVP has suspended

For each run, the following information appears:

- The time that the run started relative to the start of the procedure
- The time that RSVP suspended again
- The number of notifications processed in this run

For each neighbor, the following information appears:

- The delay of the first PATH message sent to this neighbor
- The delay of the last PATH message sent to this neighbor

## Examples

## Examples

The following example displays information about the FLR rate:

```
Router# show ip rsvp signalling fast-local-repair
Fast Local Repair: enabled
   Max repair rate (paths/sec): 400
   Max processed   (paths/run): 1000
```

The table below describes the significant fields shown in the display.

***Table 173: show ip rsvp signalling fast-local-repair Field Descriptions***

| Field | Description |
|---|---|
| Fast Local Repair | FLR state. Values are the following:<br>• enabled--FLR is configured.<br>• disabled--FLR is not configured. |
| Max repair rate (paths/sec) | Maximum repair rate, in paths per second. |
| Max processed (paths/run) | Maximum notification elements processed, in paths per run. |

## Examples

The following example displays information about FLR procedures:

```
Router# show ip rsvp signalling fast-local-repair statistics
Fast Local Repair: enabled
   Max repair rate (paths/sec): 1000
   Max processed   (paths/run): 1000
FLR Statistics:
  FLR   State    Start                          #PSB   Repair RIB Proc Last
  Proc.          Time                           Repair Rate   Time      PSB
  1     DONE     15:16:32 MET Wed Oct 25 2006   2496   1000   91(ms)    3111(ms)
```

The table below describes the significant fields shown in the display.

***Table 174: show ip rsvp signalling fast-local-repair statistics Field Descriptions***

| Field | Description |
|---|---|
| Fast Local Repair | FLR state. Values are the following:<br>• enabled--FLR is configured.<br>• disabled--FLR is not configured. |
| Max repair rate (paths/sec) | Maximum repair rate, in paths per second. |
| Max processed (paths/run) | Maximum notification elements processed, in paths per run. |
| FLR Statistics | FLR-related information. |
| FLR Proc. | FLR procedure number. The last 32 procedures are listed from the most recent to the oldest; they are numbered from 1 to 32. |
| State | Current state of the FLR procedure. Values are the following:<br>• DONE--The FLR procedure is complete.<br>• IN PROGRESS--The FLR procedure is incomplete. |
| Start Time | Time when RSVP received the routing notification. |
| #PSB Repair | Number of PSBs repaired. |
| Repair Rate | Repair rate used, in paths per second. |

| Field | Description |
|---|---|
| RIB Proc Time | Time that RSVP spent to process all RIB notifications and schedule the path refreshes, in microseconds (us), milliseconds (msec or ms), or seconds (sec).<br>**Note** The value is converted to fit the column width; however, seconds are rarely used because RSVP RIB notification processing is very fast. |
| Last PSB | Elapsed time, in microseconds (us), milliseconds (msec or ms), or seconds (sec), between the start of an FLR procedure and when RSVP sent the last PATH message.<br>**Note** The value is converted to fit the column width; however, seconds are rarely used because RSVP RIB notification processing is very fast. |

## Examples

The following example displays detailed information about FLR procedures:

```
Router# show ip rsvp signalling fast-local-repair statistics detail
Fast Local Repair: enabled
   Max repair rate (paths/sec): 1000
   Max processed   (paths/run): 1000
FLR Statistics:
   FLR 1: DONE
     Start Time: 15:16:32 MET Wed Oct 25 2006
     Number of PSBs repaired:          2496
     Used Repair Rate (msgs/sec):      1000
     RIB notification processing time: 91(ms)
     Time of last PSB refresh:         3111(ms)
     Time of last Resv received:       4355(ms)
     Time of last Perr received:       0(us)
     Suspend count: 2
       Run  Number   Started              Duration
       ID   of ntf.  (time from Start)
       2    498      81(ms)               10(ms)
       1    998      49(ms)               21(ms)
       0    1000     0(us)                22(ms)
     FLR Pacing Unit: 1 msec
     Affected neighbors:
       Nbr Address     Interface    Relative Delay Values (msec) VRF
       10.1.2.12       Et0/3        [500  ,..., 5000  ]          vrf1
       10.1.2.12       Et1/3        [500  ,..., 5000  ]          vrf2
```

The table below describes the significant fields shown in the display.

***Table 175: show ip rsvp signalling fast-local-repair statistics detail Field Descriptions***

| Field | Description |
|---|---|
| Fast Local Repair | FLR state. Values are the following:<br>• enabled--FLR is configured.<br>• disabled--FLR is not configured. |

| Field | Description |
|---|---|
| Max repair rate (paths/sec) | Maximum repair rate, in paths per second. |
| Max processed (paths/run) | Maximum notification elements processed, in paths per run. |
| FLR Statistics | FLR-related information. |
| FLR 1 | FLR procedure number and current state. The last 32 procedures are listed from the most recent to the oldest; they are numbered from 1 to 32. Values for the state are the following:<br>• DONE--The FLR procedure is complete.<br>• IN PROGRESS--The FLR procedure is incomplete. |
| Start Time | Time when RSVP received the routing notification. |
| Number of PSBs repaired | Total PSBs repaired. |
| Used Repair Rate (msgs/sec) | Repair rate used, in messages per second. |
| RIB notification processing time | Time, in milliseconds (ms), that RSVP spent to process all RIB notifications. |
| Time of last PSB refresh | Elapsed time, in milliseconds (ms), between the start of an FLR procedure and when RSVP sent the last PATH refresh message. |
| Time of last Resv received | Elapsed time, in milliseconds (ms), between the start of an FLR procedure and when RSVP received the last RESV message. |
| Time of last Perr received | Elapsed time, in microseconds (us), between the start of an FLR procedure and when RSVP received the last PATHERROR message. |
| Suspend count | Number of times that RSVP has suspended during a specific procedure.<br>**Note** If this value is nonzero, details for each run are shown. |
| Run ID | Identifier (number) for each time that RSVP has run. |
| Number of ntf. | Number of notifications (PSBs) processed in a run. |
| Started (time from Start) | Time, in milliseconds (ms), that the run began relative to the start of the FLR procedure. |

| Field | Description |
|---|---|
| Duration | Length of time, in milliseconds (ms), for the run. |
| FLR Pacing Unit | Frequency, in milliseconds (msec), for RSVP message pacing; that is, how often a PATH message is sent. The value is rounded down. |
| Affected neighbors | Neighbors involved in the FLR procedure. |
| Nbr Address | IP address for each neighbor involved in a procedure. |
| Interface | Interface for the neighbor. |
| Relative Delay Values | Times, in milliseconds (msec), when the PSB refreshes were sent.<br>**Note** In the sample display, there is a 1-msec pacing unit; therefore, PSBs to 10.1.2.12 have been sent with delays of 1 msec from 500, 501, 502, 503, ... 2995. If a 5-msec pacing unit were used, the delays would be 500, 505, 510,... 2990, 2995. |
| VRF | VRF name for which the FLR was triggered on the PLR. |

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp signalling fast-local-repair notifications** | Configures the number of notifications that are processed before RSVP suspends. |
| **ip rsvp signalling fast-local-repair rate** | Configures the repair rate that RSVP uses for an FLR procedure. |
| **ip rsvp signalling fast-local-repair wait** | Configures the delay used to start an FLR procedure. |
| **ip rsvp signalling rate-limit** | Controls the transmission rate for RSVP messages sent to a neighboring router during a specified amount of time. |

# show ip rsvp signalling rate-limit

To display the Resource Reservation Protocol (RSVP) rate-limiting parameters, use the **showiprsvpsignallingrate-limit** command in user EXEC or privileged EXEC mode.

**show ip rsvp signalling rate-limit**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.0(24)S | This command was integrated into Cisco IOS Release 12.0(24)S. |
| 12.0(29)S | The command output was modified to show the revised rate-limiting parameters. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. |
| 12.2(18)SXF5 | This command was integrated into Cisco IOS Release 12.2(18)SXF5. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |
| Cisco IOS XE Release 2.3 | This command was integrated into Cisco IOS XE Release 2.3. |

## Examples

The following command shows the rate-limiting parameters:

```
Router# show ip rsvp signalling rate-limit
Rate Limiting:
  Burst: 1
  Limit: 20
  Maxsize: 500
  Period <msec>: 5
  Max rate <msgs/sec>: 2
```

The table below describes the fields shown in the display.

*Table 176: show ip rsvp signalling rate-limit Field Descriptions*

| Field | Description |
|---|---|
| Rate Limiting | The RSVP rate-limiting parameters are enabled or disabled. They include the following:<br>• Burst-Number of messages sent each period from the queue.<br>• Limit-Maximum number of messages sent each period from the queue.<br>• Maxsize-Maximum size of the message queue, in bytes.<br>• Period (msec)-Interval (time frame) in milliseconds.<br>• Max rate (msgs/sec)-Maximum number of messages allowed to be sent per second. |

## Related Commands

| Command | Description |
|---|---|
| **clear ip rsvp signalling rate-limit** | Clears (sets to zero) the number of messages that were dropped because of a full queue. |
| **debug ip rsvp rate-limit** | Displays debug messages for RSVP rate-limiting events. |
| **ip rsvp signalling rate-limit** | Controls the transmission rate for RSVP messages sent to a neighboring router during a specified amount of time. |

# show ip rsvp signalling refresh

To display the Resource Reservation Protocol (RSVP) signaling refresh behavior parameters for RSVP messages, use the **showiprsvpsignallingrefresh** command in user EXEC or privileged EXEC mode.

**show ip rsvp signalling refresh** {**interval**| **misses**| **reduction**}

## Syntax Description

| | |
|---|---|
| **interval** | Specifies the time interval between steady refresh messages. |
| **misses** | Specifies the number of refreshes that are not received during the trigger state timeout. |
| **reduction** | Specifies the RSVP refresh reduction parameters and settings. |

## Command Modes

User EXEC (>)

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |
| 12.2(24)T | The**interval** and **misses** keywords were added. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |

## Usage Guidelines

Use the **showiprsvpsignallingrefresh** command to display the refresh behavior parameters.

## Examples

The following example shows the refresh interval parameters:

```
Router# show ip rsvp signalling refresh interval

Refresh interval (msec): 30000
```

The following example shows the refresh misses parameters:

```
Router# show ip rsvp signalling refresh misses
Refresh misses: 4
```

The following example shows the refresh reduction parameters:

```
Router# show ip rsvp signalling refresh reduction
Refresh Reduction: disabled
  ACK delay (msec): 250
  Initial retransmit delay (msec): 1000
  Local epoch: 0x6975F6
  Message IDs: in use 0, total allocated 0, total freed 0
```

## Related Commands

| Command | Description |
|---|---|
| **clear ip rsvp signalling rate-limit** | Clears the counters recording dropped messages. |
| **debug ip rsvp rate-limit** | Displays debug messages for RSVP rate-limiting events. |
| **ip rsvp signalling rate-limit** | Controls the transmission rate for RSVP messages sent to a neighboring router during a specified amount of time. |

# show ip rsvp snooping

To display a list of VLANs in which Resource Reservation Protocol (RSVP) snooping is enabled, use the **show ip rsvp snooping** command in privileged EXEC mode.

**show ip rsvp snooping**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(44)SE | This command was introduced. |

## Usage Guidelines

You can use the **ip rsvp snooping** command to enabled RSVP snooping on the required VLANs. The **show ip rsvp snooping** command allows you to view how many VLANs have RSVP snooping enabled in them. VLAN details are optional and are visible only on platforms that support per-VLAN snooping. If VLAN details are not specified in the **ip rsvp snooping** command, snooping will be enabled on all VLANs and the **show ip rsvp snooping** command indicates the same.

## Examples

The following sample output displays a list of VLANs in which RSVP snooping is enabled:

```
Device# show ip rsvp snooping

*May 29 09:06:27.597: %SYS-5-CONFIG_I: Configured from console by consoleoping

RSVP Snooping is enabled on this Vlans
----------------------------------------
VLan 70         VLan 71         VLan 72
VLan 73         VLan 74
----------------------------------------
```

The following sample output shows that RSVP snooping is enabled on all VLANs:

```
Device# show ip rsvp snooping

RSVP snooping is enabled globally.
```

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp snooping** | Enables RSVP snooping in a specific set of VLANs. |

# show ip rsvp tos

To display IP type of service (ToS) information about Resource Reservation Protocol (RSVP) interfaces, use the **showiprsvptos**command in user EXEC or privileged EXEC mode.

**show ip rsvp tos** [**type number**]

## Syntax Description

| | |
|---|---|
| **type** | (Optional) Type of interface. |
| number | (Optional) Number of the interface. |

## Command Modes

User EXEC(>) Privileged EXEC(#)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)M | This command was introduced. |

## Usage Guidelines

To obtain IP ToS information about a specific interface configured to use RSVP, specify the interface name with the show ip rsvp tos command. To obtain IP ToS information about all interfaces enabled for RSVP on the router, use the show ip rsvp tos command without specifying an interface name.

## Examples

The following example shows the IP ToS information for the interaces on which RSVP is enabled:

```
Router# show ip rsvp tos ethernet 0/1
Interface name   Precedence  Precedence   TOS          TOS
                   conform    exceed     conform     exceed
Ethernet0/0          -           -          -           -
Ethernet0/1          -           -          -           -
Ethernet1/1          -           -          4           -
Ethernet1/2          3           -          -           -
```

The table below describes the fields shown in the display.

***Table 177: show ip rsvp tos Field Descriptions***

| Field | Description |
|---|---|
| Interface name | Displays the interface details. |

| Field | Description |
|---|---|
| Precedence conform | Displays the IP precedence conform information for an interface.<br>**Note** The Precedence conform value specifies an IP precedence value in the range from 0 to 7 for traffic that conforms to the RSVP flowspec. |
| Precedence exceed | Displays the IP precedence exceed information for an interface.<br>**Note** The Precedence exceed value specifies an IP Precedence value in the range from 0 to 7 for traffic that exceeds the RSVP flowspec. |
| TOS conform | Displays the IP type of service (ToS) conform information for an interface.<br>**Note** The TOS conform value specifies a ToS value in the range from 0 to 31 for traffic that conforms to the RSVP flowspec. |
| TOS exceed | Displays the IP type of service (ToS) exceed information for an interface.<br>**Note** The TOS exceed value specifies a ToS value in the range from 0 to 31 for traffic that exceeds the RSVP flowspec. |

## Related Commands

| Command | Description |
|---|---|
| show ip rsvp | Displays RSVP-related information. |
| **show ip rsvp interface** | Displays RSVP-related interface information. |
| **show ip rsvp precedence** | Displays IP precedence information for RSVP enabled interfaces. |

# show ip rsvp transport

To display information about Resource Reservation Protocol (RSVP) transport protocol (TP) sessions, use the **showiprsvptransport** command in user EXEC or privileged EXEC mode.

**show ip rsvp transport** {**clients**| **statistics**}

## Syntax Description

| | |
|---|---|
| **clients** | Displays information about RSVP clients that initiated the TP sessions. |
| **statistics** | Displays statistics for RSVP TP sessions. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.1(3)T | This command was introduced. |
| 15.1(1)S | This command was integrated into Cisco IOS Release 15.1(1)S. |

## Examples

The following is sample output from the **showiprsvptransportstatistics** command:

```
Router# show ip rsvp transport statistics
RSVP Transport Statistics:
 Transport Statistics: 2
  Start Time: 05:57:42 IST Thu Nov 5 2009
  Destination: 10.1.1.2, Protocol_Id: 6, DstPort: 22
  Client_id: 1, Initiator_Id: 10.1.1.1
  Source: 10.1.1.1, SrcPort: 11, Instance_Id: 9999
 Outgoing interface: Ethernet1/0
  Event type: RSVP_TP_EVENT_SESSION_DOWN
 Transport Statistics: 1
  Start Time: 05:57:16 IST Thu Nov 5 2009
  Destination: 10.1.1.2, Protocol_Id: 6, DstPort: 22
  Client_id: 1, Initiator_Id: 10.1.1.1
  Source: 10.1.1.1, SrcPort: 11, Instance_Id: 9999
  Incoming interface: Ethernet0/0
  TP data: example1
  Event type: RSVP_TP_EVENT_MSG_RCVD
  Received message type: Path
```

The table below describes the significant fields shown in the display.

*Table 178: show ip rsvp transport statistics Field Descriptions*

| Field | Description |
|---|---|
| Transport Statistics | Displays the buffer size, in megabye (MB), which is used to store information about the RSVP TP statistics. |
| Start Time | Displays the time from when the router started recording RSVP statistics. |
| Destination | Destination address to where the PATH message is sent. |
| Protocol_Id | Identifier that is used to configure RSVP as transport protocol. |
| DstPort | Destination port to which the PATH message is sent. |
| Client_id | Identification number of the client that initiates RSVP as a transport protocol. |
| Initiator_Id | Hostname or IP address that identifies the node initiating the transport service request. |
| Source | Source address from where the PATH message is sent. |
| SrcPort | Source port from which the PATH message is sent. |
| Instance_Id | Instance ID that identifies the transport service request from a particular client application and from a particular initiator. |
| Incoming interface | Interface type and number from which the PATH messages are sent. |
| TP data | Transport protocol data. |
| Event type | Type of event that has occurred. |
| Received message type | Type of messages being sent. |

The following example shows how to display the RSVP client ID and client type information:

```
Router# show ip rsvp transport clients
Client-ID  Type
1           CLI
```

## Related Commands

| Command | Description |
|---|---|
| **show ip rsvp transport sender-host** | Displays RSVP PATH state information. |

# show ip rsvp transport sender

To display Resource Reservation Protocol (RSVP) PATH state information, use the **showiprsvptransportsender** command in user EXEC or privileged EXEC mode.

**show ip rsvp transport sender** [**vrf** {*****| *vrf-name*}] **[detail]** [**filter** [**destination** *dest-address*| **dst-port** *dst-port*| **source** *source-addr*| **src-port** *src-port*]]

## Syntax Description

| | |
|---|---|
| **vrf** | (Optional) Specifies the VPN routing and forwarding (VRF) details. |
| ***** | (Optional) Displays RSVP PATH state information for all VRFs and global routing domain. |
| *vrf-name* | (Optional) VRF name. |
| **detail** | (Optional) Displays detailed description of the PATH state information. |
| **filter** | (Optional) Filters the display to limit the output. |
| **destination** | (Optional) Filters the display to show information related to the destination. |
| *dest-address* | (Optional) IP address specifying the destination. |
| **dst-port** | (Optional) Filters the display to show information related to the destination port. |
| *dst-port* | Destination port or tunnel ID. The range is from 0 to 65535. |
| **source** | (Optional) Filters the display to show information related to the source. |
| *source-addr* | (Optional) IP address specifying the source. |
| **src-port** | (Optional) Filters the display to show information related to the source port. |
| *src-port* | (Optional) Destination port or link-state packet (LSP) ID. The range is from 0 to 65535. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.1(3)T | This command was introduced. |
| 15.1(1)S | This command was integrated into Cisco IOS Release 15.1(1)S. |

## Usage Guidelines

You can use the **showiprsvptransport** command to display information related to RSVP configured as transport protocol.

## Examples

The following example shows how to display information about the PATH messages being sent from the sender to the receiver:

```
Router# show ip rsvp transport sender
To              From            Pro DPort Sport Prev Hop         I/F
10.1.1.1       10.2.2.2         TCP 101   101   none             none
```

The table below describes the significant fields shown in the display.

***Table 179: show ip rsvp transport sender Field Descriptions***

| Field | Description |
|---|---|
| To | IP address of the receiver. |
| From | IP address of the sender or the client. |
| Pro | Identifier that is used to configure RSVP as transport protocol. |
| DPort | Destination port to which the PATH message is sent. |
| Sport | Source port from which the PATH message is sent. |
| Prev Hop | The hop address used to transport the PATH message from the sender to the receiver. |

The following example shows how to display detailed information about RSVP messages:

```
Router# show ip rsvp transport sender detail
Transport PATH:
  Destination 10.1.1.1, Protocol_Id 6,  DstPort 101
  Sender address: 10.2.2.2, port: 101
  Path refreshes:
     Path ID handle: 01000402.
  Client_id: 251
   Initiator_id: 10.2.2.2
   Instance_id: 3421
```

The table below describes the significant fields shown in the display.

*Table 180: show ip rsvp transport sender detail Field Descriptions*

| Field | Description |
|---|---|
| Transport PATH: | Displays information related to the transport path taken to send the PATH messages. |
| Destination | Destination address to where the PATH message is sent. |
| Protocol_Id | Identifier that is used to configure RSVP as transport protocol. |
| DstPort | Destination port to which the PATH message is sent. |
| Sender address | Source address from where the PATH message is sent. |
| port | Source port from which the PATH message is sent. |
| Path refreshes | Displays information about the periodic refreshes of PATH and Resv messages. |
| Path ID handle | Displays the number of times the PATH and Resv messages have been refreshed. |
| Client id | Identification number of the client that initiates RSVP as a transport protocol. |
| Initiator_id | Hostname or IP address that identifies the node initiating the transport service request. |
| Instance_id | Instance ID that identifies the transport service request from a particular client application and from a particular initiator. |

## Related Commands

| Command | Description |
|---|---|
| **ip rsvp transport** | Configures RSVP as transport protocol. |
| **ip rsvp transport sender-host** | Configures static RSVP host path. |
| **show ip rsvp transport** | Displays information about RSVP TP sessions. |

# show ip rtp header-compression

To display Real-Time Transport Protocol (RTP) statistics, use the **showiprtpheader-compression** command in privileged EXEC mode.

**show ip rtp header-compression** [*interface-type interface-number*] **[detail]**

## Syntax Description

| | |
|---|---|
| *interface-type interface-number* | (Optional) The interface type and number. |
| **detail** | (Optional) Displays details of each connection. |

## Command Default

No default behavior or values

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 11.3 | This command was introduced. |
| 12.1(5)T | The command output was modified to include information related to the Distributed Compressed Real-Time Transport Protocol (dCRTP) feature. |
| 12.3(11)T | The command output was modified to include information related to the Enhanced Compressed Real-Time Transport Protocol (ECRTP) feature. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

The **detail** keyword is not available with the **showiprtpheader-compression** command on a Route Switch Processor (RSP). However, the **detail** keyword is available with the show ip rtp header-compression command on a Versatile Interface Processor (VIP). Enter the show ip rtp header-compression interface-type interface-number detail command on a VIP to retrieve detailed information regarding RTP header compression on a specific interface.

## Examples

The following example displays statistics from ECRTP on an interface:

```
Router# show ip rtp header-compression

RTP/UDP/IP header compression statistics:
  Interface Serial2/0 (compression on, IETF, ECRTP)
    Rcvd:    1473 total, 1452 compressed, 0 errors, 0 status msgs
```

```
          0 dropped, 0 buffer copies, 0 buffer failures
Sent:     1234 total, 1216 compressed, 0 status msgs, 379 not predicted
          41995 bytes saved, 24755 bytes sent
          2.69 efficiency improvement factor
Connect: 16 rx slots, 16 tx slots,
          6 misses, 0 collisions, 0 negative cache hits, 13 free contexts
          99% hit ratio, five minute miss rate 0 misses/sec, 0 max
```

The table below describes the significant fields shown in the display.

***Table 181: show ip rtp header-compression Field Descriptions***

| Field | Description |
|---|---|
| Interface | Type and number of interface. |
| Rcvd | Received statistics described in subsequent fields. |
| total | Number of packets received on the interface. |
| compressed | Number of packets received with compressed headers. |
| errors | Number of errors. |
| status msgs | Number of resynchronization messages received from the peer. |
| dropped | Number of packets dropped. |
| buffer copies | Number of buffers that were copied. |
| buffer failures | Number of failures in allocating buffers. |
| Sent | Sent statistics described in subsequent fields. |
| total | Number of packets sent on the interface. |
| compressed | Number of packets sent with compressed headers. |
| status msgs | Number of resynchronization messages sent from the peer. |
| not predicted | Number of packets taking a non-optimal path through the compressor. |
| bytes saved | Total savings in bytes due to compression. |
| bytes sent | Total bytes sent after compression. |
| efficiency improvement factor | Compression efficiency. |
| Connect | Connect statistics described in subsequent fields. |
| rx slots | Total number of receive slots. |

| Field | Description |
|---|---|
| tx slots | Total number of transmit slots. |
| misses | Total number of misses. |
| collisions | Total number of collisions. |
| negative cache hits | Total number of negative cache hits. |
| free contexts | Number of available context resources. |
| hit ratio | Percentage of received packets that have an associated context. |
| five minute miss rate | Number of new flows found per second averaged over the last five minutes. |
| max | Highest average rate of new flows reported. |

## Related Commands

| Command | Description |
|---|---|
| **ip rtp compression-connections** | Specifies the total number of RTP header compression connections supported on the interface. |
| **ip rtp header-compression** | Enables RTP header compression. |

# show ip tcp header-compression

To display TCP/IP header compression statistics, use the **show ip tcp header-compression** command in user EXEC or privileged EXEC mode.

**show ip tcp header-compression** [*interface-type interface-number*] **[detail]**

## Syntax Description

| | |
|---|---|
| *interface-type interface-number* | (Optional) The interface type and number. |
| **detail** | (Optional) Displays details of each connection. This keyword is available only in privileged EXEC mode. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 10.0 | This command was introduced. |
| 12.4 | This command was integrated into Cisco Release 12.4 and its command output was modified to include additional compression statistics. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(15)T12 | This command was modifed. Support was added for the special Van Jacobson (VJ) format of TCP header compression. |

## Examples

The following is sample output from the **show ip tcp header-compression** command:

```
Router# show ip tcp header-compression

TCP/IP header compression statistics:
  Interface Serial2/0 (compression on, IETF)
    Rcvd:    53797 total, 53796 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
    Sent:    53797 total, 53796 compressed, 0 status msgs, 0 not predicted
             1721848 bytes saved, 430032 bytes sent
             5.00 efficiency improvement factor
    Connect: 16 rx slots, 16 tx slots,
             1 misses, 0 collisions, 0 negative cache hits, 15 free contexts
             99% hit ratio, five minute miss rate 0 misses/sec, 0 max
```

The table below describes the significant fields shown in the display.

*Table 182: show ip tcp header-compression Field Descriptions*

| Field | Description |
|---|---|
| Interface Serial2/0 (compression on, IETF) | Interface type and number on which compression is enabled. |
| Rcvd: | Received statistics described in subsequent fields. |
| total | Total number of TCP packets received on the interface. |
| compressed | Total number of TCP packets compressed. |
| errors | Number of packets received with errors. |
| status msgs | Number of resynchronization messages received from the peer. |
| dropped | Number of packets dropped due to invalid compression. |
| buffer copies | Number of packets that needed to be copied into bigger buffers for decompression. |
| buffer failures | Number of packets dropped due to a lack of buffers. |
| Sent: | Sent statistics described in subsequent fields. |
| total | Total number of TCP packets sent on the interface. |
| compressed | Total number of TCP packets compressed. |
| status msgs | Number of resynchronization messages sent from the peer. |
| not predicted | Number of packets taking a nonoptimal path through the compressor. |
| bytes saved | Total savings in bytes due to compression. |
| bytes sent | Total bytes sent after compression. |
| efficiencyimprovement factor | Improvement in line efficiency because of TCP header compression, expressed as the ratio of total packet bytes to compressed packet bytes. The ratio should be greater than 1.00. |
| Connect: | Connection statistics described in subsequent fields. |
| rxslots | Total number of receive slots. |

| Field | Description |
|---|---|
| txslots | Total number of transmit slots. |
| misses | Indicates the number of times a match could not be made. If your output shows a large miss rate, then the number of allowable simultaneous compression connections may be too low. |
| collisions | Total number of collisions. |
| negative cache hits | Total number of negative cache hits.<br>**Note** This field is not relevant for TCP header compression; it is used for Real-Time Transport Protocol (RTP) header compression. |
| free contexts | Total number of free contexts.<br>**Note** Free contexts (also known as connections) are an indication of the number of resources that are available, but not currently in use, for TCP header compression. |
| hit ratio | Percentage of times the software found a match and was able to compress the header. |
| Five minute miss rate 0 misses/sec | Calculates the miss rate over the previous five minutes for a longer-term (and more accurate) look at miss rate trends. |
| max | Maximum value of the previous field. |

The following example for Cisco IOS Release 12.4(15)T12 shows that the TCP special VJ format is enabled:

```
Router# show ip tcp header-compression serial 5/0 detail

TCP/IP header compression statistics:
 DLCI 100        Link/Destination info: ip 10.72.72.2
Configured:
 Max Header 60 Bytes, Max Time 50 Secs, Max Period 32786 Packets, Feedback On, Spl-VJ On
Negotiated:
 Max Header 60 Bytes, Max Time 50 Secs, Max Period 32786 Packets, Feedback On, Spl-VJ On
TX contexts:
```

## Related Commands

| Command | Description |
|---|---|
| **ip header-compression special-vj** | Enables the special VJ format of TCP header compression. |
| **ip tcp compression-connections** | Specifies the total number of TCP header compression connections that can exist on an interface |

| Command | Description |
|---|---|
| **special-vj** | Enables the special VJ format of TCP header compression so that context IDs are included in compressed packets. |

# show ip vrf

To display the set of defined Virtual Private Network (VPN) routing and forwarding (VRF) instances and associated interfaces, use the **showipvrf** command in user EXEC or privileged EXEC mode.

**show ip vrf** [**brief**| **detail**| **interfaces**| **id**] [ *vrf-name* ]

## Syntax Description

| | |
|---|---|
| **brief** | (Optional) Displays concise information on the VRFs and associated interfaces. |
| **detail** | (Optional) Displays detailed information on the VRFs and associated interfaces. |
| **interfaces** | (Optional) Displays detailed information about all interfaces bound to a particular VRF or any VRF. |
| **id** | (Optional) Displays the VPN IDs that are configured in a PE router for different VPNs. |
| *vrf-name* | (Optional) Name assigned to a VRF. |

## Command Default

When you do not specify keywords or arguments, the command shows concise information about all configured VRFs.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.0(17)ST | This command was modified. The id keyword was added. The VPN ID information was added to the output of the show ip vrf detail command. |
| 12.2(4)B | This command was integrated into Cisco IOS Release 12.2(4)B. |
| 12.2(8)T | This command was integrated into Cisco IOS Release 12.2(8)T. |
| 12.3(6) | This command was integrated into Cisco IOS Release 12.3(6). The command shows the downstream VRF for each associated Virtual access interface (VAI). |
| 12.2(27)SBC | This command was integrated into Cisco IOS Release 12.2(27)SBC. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

| Release | Modification |
|---|---|
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use this command to display information about VRFs. Two levels of detail are available:

- The **brief**keyword (or no keyword) displays concise information.
- The **detail** keyword displays all information.

To display information about all interfaces bound to a particular VRF, or to any VRF, use the interfaces keyword. To display information about VPN IDs assigned to a PE router, use the id keyword.

When you use the **showipvrf** command, interface and subinterface names are truncated in the output. For example, GigabitEthernet3/1/0.100 is displayed as Gi3/1/0.100.

## Examples

Cisco IOS T Train, Cisco IOS SB Train, Cisco IOS B Train, and Cisco IOS SX Train

The following example displays information about all the VRFs configured on the router, including the downstream VRF for each associated VAI. The lines that are highlighted (for documentation purposes only) indicate the downstream VRF.

```
Router# show ip vrf
  Name                              Default RD          Interfaces
  v1                                20:20               Gi0/2.4294967291
                                                        Gi0/2.4294967293
                                                        Gi0/2.4294967294
                                                        Gi0/2.4294967295
  vpn152-1                          152:1               Lo1
```

The table below describes the significant fields shown in the display.

***Table 183: show ip vrf Field Descriptions***

| Field | Description |
|---|---|
| Name | Specifies the VRF name. |
| Default RD | Specifies the default route distinguisher. |
| Interfaces | Specifies the network interface. |

The following example displays detailed information about all of the VRFs configured on the router, including all of the VAIs associated with each VRF:

```
Router# show ip vrf detail vpn152-1
VRF vpn152-1; default RD 152:1; default VPNID <not set>
VRF Table ID = 2
  Interfaces:
    Lo1
  Connected addresses are not in global routing table
```

```
  Export VPN route-target communities
    RT:152:1
  Import VPN route-target communities
    RT:152:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
```

The table below describes the significant fields shown in the display.

***Table 184: show ip vrf detail Field Descriptions***

| Field | Description |
|---|---|
| default VPNID | Specifies the VPN ID that uniquely identifies every VPN in the network. |
| VRF Table ID | Uniquely identifies the VRF routing table. |
| Interfaces | Specifies the network interfaces. |
| Export VPN route-target communities | Specifies VPN route-target export communities. |
| Import VPN route-target communities | Specifies VPN route-target import communities. |
| VRF label distribution protocol | MPLS label distribution protocol in the VRF context. This is required when VRF is configured for Carrier Supporting Carrier (CSC). This could be LDP (enabled via the **mplsip** command on the VRF interface) or BGP (enabled via the **send-label** command in the router bgp VRF address-family configuration mode). |

The following example shows the interfaces bound to a particular VRF:

```
Router# show ip vrf interfaces
Interface              IP-Address      VRF                              Protocol
Gi0/2.4294967291       unassigned      v1                               down
Gi0/2.4294967293       unassigned      v1                               down
Gi0/2.4294967294       unassigned      v1                               down
Gi0/2.4294967295       unassigned      v1                               down
Lo1                    10.1.1.1        vpn152-1                         up
```

The table below describes the significant fields shown in the display.

***Table 185: show ip vrf interfaces Field Descriptions***

| Field | Description |
|---|---|
| Interface | Specifies the network interfaces for a VRF. |
| IP-Address | Specifies the IP address of a VRF interface. |
| VRF | Specifies the VRF name. |

| Field | Description |
|---|---|
| Protocol | Displays the state of the protocol (up or down) for each VRF interface. |

Cisco IOS SR Train

The following example displays output from the **showipvrf** command with the **detail** keyword. The information shown is for a VRF named vpn1.

```
Router# show ip vrf detail vpn1
VRF vpn1 (VRF Id = 1); default RD 1:1; default VPNID <not set>
 Interfaces:
 Lo1                     Lo99                    Et0/0
VRF Table ID = 1
 Export VPN route-target communities
 RT:1:1
 Import VPN route-target communities
  RT:1:1                  RT:2:1
No import route-map
No export route-map
 VRF label distribution protocol: not configured
 VRF label allocation mode: per-prefix
```

The table below describes the significant fields shown in the display.

***Table 186: show ip vrf detail Field Descriptions***

| Field | Description |
|---|---|
| VRF ID | Uniquely identifies the VRF within the router. |
| VRF label allocation mode | Indicates the type of label mode used based on the route types. |

## Related Commands

| Command | Description |
|---|---|
| **import map** | Configures an import route map for a VRF. |
| **ip vrf** | Configures a VRF routing table. |
| **ip vrf forwarding (interface configuration)** | Associates a VRF with an interface or subinterface. |
| **rd** | Creates routing and forwarding tables for a VRF. |
| **route-target** | Creates a route-target extended community for a VRF. |
| **vpn id** | Assigns a VPN ID to a VRF. |

# show lane qos database

**Note** Effective with Cisco IOS Release 15.1M, the **showlaneqosdatabase**command is not available in Cisco IOS software.

To display the contents of a specific LAN Emulation (LANE) quality of service (QoS) database, use the **showlaneqosdatabase**command in privileged EXEC mode.

**show lane qos database** *name*

## Syntax Description

| | |
|---|---|
| *name* | Specifies the QoS over LANE database to display. |

## Command Default

This command is not configured by default.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1(2)E | This command was introduced. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 15.1M | This command was removed. |

## Examples

This example shows how to display the contents of a QoS over LANE database for a Catalyst 5000 family ATM Module:

```
ATM# show lane qos database user1
QOS: user1
    configured cos values: 5-7, usage: 1
    dst nsap: 47.009181000000061705B0C01.00E0B0951A40.0A
    pcr: 500000, mcr: 100000
```

This example shows how to display the contents of a QoS over LANE database for a Cisco 4500, 7200, or 7500 series router:

```
Router# show lane qos database user2
QOS: user2
    configured cos values: 5-7, usage: 1
    dst nsap: 47.009181000000061705B0C01.00E0B0951A40.0A
    pcr: 500000, mcr: 100000
```

## Related Commands

| Command | Description |
|---|---|
| **atm-address** | Specifies the QoS parameters associated with a particular ATM address. |
| **lane client qos** | Applies a QoS over LANE database to an interface. |
| **lane qos database** | Begins the process of building a QoS over LANE database. |
| **ubr+ cos** | Maps a CoS value to a UBR+ VCC. |

# show mls qos through wrr-queue threshold


- show metadata application table, page 1510
- show metadata flow, page 1512
- show mls qos, page 1519
- show mls qos aggregate policer, page 1524
- show mls qos free-agram, page 1526
- show mls qos interface, page 1527
- show mls qos maps, page 1529
- show mls qos mpls, page 1533
- show mls qos protocol, page 1536
- show mls qos queuing interface, page 1538
- show mls qos statistics-export info, page 1542
- show platform hardware acl entry global-qos, page 1544
- show platform hardware pp active infrastructure pi npd rx policer, page 1546
- show platform hardware qfp active feature qos config global, page 1548
- show platform lowq, page 1550
- show platform qos policy-map, page 1551
- show platform software infrastructure punt statistics, page 1554
- show policy-manager events, page 1556
- show policy-manager policy, page 1558
- show policy-map, page 1560
- show policy-map class, page 1576
- show policy-map control-plane, page 1578
- show policy-map interface, page 1582
- show policy-map interface brief, page 1631

- show policy-map interface service group, page 1640
- show policy-map interface service instance, page 1642
- show policy-map mgre, page 1647
- show policy-map multipoint, page 1650
- show policy-map session, page 1652
- show policy-map target service-group, page 1660
- show policy-map type access-control, page 1662
- show policy-map type nat, page 1665
- show policy-map type port-filter, page 1667
- show protocol phdf, page 1670
- show qbm client, page 1672
- show qbm pool, page 1674
- show qdm status, page 1677
- show queue, page 1679
- show queueing, page 1685
- show queueing interface, page 1692
- show random-detect-group, page 1697
- show running-config service-group, page 1700
- show service-group, page 1702
- show service-group interface, page 1705
- show service-group state, page 1707
- show service-group stats, page 1708
- show service-group traffic-stats, page 1711
- show subscriber policy ppm-shim-db, page 1713
- show table-map, page 1714
- show tech-support nbar platform, page 1716
- show tech-support rsvp, page 1730
- show traffic-shape, page 1732
- show traffic-shape queue, page 1735
- show traffic-shape statistics, page 1740
- show vrf, page 1743
- show wrr-queue, page 1747
- subscriber accounting accuracy, page 1748

- svc-bundle, page 1749
- table-map (value mapping), page 1750
- tcp, page 1753
- tcp contexts, page 1754
- traffic-shape adaptive, page 1756
- traffic-shape fecn-adapt, page 1758
- traffic-shape group, page 1760
- traffic-shape rate, page 1763
- trust, page 1766
- tx-ring-limit, page 1768
- vbr-nrt, page 1770
- vc-hold-queue, page 1774
- wrr-queue bandwidth, page 1776
- wrr-queue cos-map, page 1778
- awrr-queue dscp-map, page 1780
- wrr-queue queue-limit, page 1782
- wrr-queue random-detect, page 1784
- wrr-queue threshold, page 1786

# show metadata application table

To display a list of metadata applications defined on a device, use the **show metadata application table** command in privileged EXEC mode.

**show metadata application table**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T | This command was introduced. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |

## Examples

The following is sample output from the **show metadata application table** command:

```
Device# show metadata application table

ID     Name                  Vendor                Vendor id
-------------------------------------------------------------------------------
113    telepresence-media    -                     -
114    telepresence-contr$   -                     -
478    telepresence-data     -                     -
414    webex-meeting         -                     -
56     citrix                -                     -
81     cisco-phone           -                     -
472    vmware-view           -                     -
473    wyze-zero-client      -                     -
61     rtp                   -                     -
64     h323                  -                     -
5060   sip                   -                     -
554    rtsp                  -                     -
496    jabber                -                     -
5222   xmpp-client           -                     -
```

The table below describes the significant fields shown in the display.

***Table 187: show metadata application table Field Descriptions***

| Field | Description |
|---|---|
| ID | Application ID. Internally maps to the application name. |
| Name | Name of the application. |

## Related Commands

| Command | Description |
|---|---|
| **metadata application-params** | Enters metadata application entry configuration mode and creates new metadata application parameters. |

# show metadata flow

To display metadata flow information, use the **show metadata flow** command in privileged EXEC mode.

**show metadata flow** {**classification table** | **local-flow-id** *flow-id* [**source** {**msp | nbar | rsvp**}] | **statistics** | **table** [[**application name** *app-name* [**ip | ipv6**]] | **filter** [**destination** {*ip-address* | *ipv6-address*}] [**source** {*ip-address* | *ipv6-address*}] | **ip | ipv6**]}

## Syntax Description

| | |
|---|---|
| **classification** | Displays metadata control plane classification information. |
| **table** | Displays metadata flow information for all flow entries. |
| **local-flow-id** *flow-id* | Displays information for the specified local flow ID, which is a unique ID for a given five-tuple metadata flow entry created locally.<br>• The local flow ID is automatically generated when the flow entry is created. |
| **source** | (Optional) Displays metadata flow information for the specified source. |
| **msp** | (Optional) Displays metadata flow information for Media-Proxy Services. |
| **nbar** | (Optional) Displays metadata flow information for Network-Based Application Recognition (NBAR). |
| **rsvp** | (Optional) Displays metadata flow information for the Resource Reservation Protocol (RSVP). |
| **statistics** | Displays metadata flow statistics. |
| **application** | (Optional) Displays metadata flow information for the specified application. |
| **name** *app-name* | (Optional) Specifies all the flows for the specified application. |
| **ip** | (Optional) Displays metadata flow information for the specified IPv4 address. |
| **ipv6** | (Optional) Displays metadata flow information for the specified IPv6 address. |

| | |
|---|---|
| **filter** | (Optional) Displays metadata flow information based on the filter criteria. |
| **destination** } | (Optional) Displays metadata flow information for the specified destination address. |
| **source** | (Optional) Displays metadata flow information for the specified source address. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 15.2(1)T | This command was introduced. |
| 15.1(1)SY | This command was integrated into Cisco IOS Release 15.1(1)SY. |
| 15.3(1)T | This command was modified. The **source**, **msp**, **nbar**, and **rsvp** keywords were added. IPv6 address information was added to the command output. |

## Examples

The following is sample output from the **show metadata flow classification table** command:

```
Device# show metadata flow classification table

Policy Type Codes:
QOS     : QOS                              PM      : Performance Monitor
PMD     : Performance Monitor Dynamic      MACE    : MACE
-------------------------------------------------------------------------------
Target          Flow ID    Dir   Policy     Filter(s)
                                 Type
--------------+----------+-----+----------+----------------------------------

Se2/0           1          OUT
Se2/0           2          OUT
Se2/0           3          OUT
Se2/0           4          OUT   QOS        application telepresence-media
Se2/0           5          OUT   QOS        application telepresence-media
Se2/0           6          OUT
Se2/0           7          OUT
Se2/0           8          OUT   QOS        application telepresence-media
Se2/0           9          OUT
```

The table below describes the significant fields shown in the display.

***Table 188: show metadata classification table Field Descriptions***

| Field | Description |
|---|---|
| Target | Interface name for which the policy map is attached. |

| Field | Description |
|---|---|
| Flow ID | Flow entry identifier. |
| Dir | Direction of the flow entry. IN indicates that the flow is entering the network element. OUT indicates that the flow is exiting the network element. CL indicates that the flow has been classified successfully. |

The following is sample output from the **show metadata flow local-flow-id** command:

```
Device# show metadata flow local-flow-id 22

To                                      From

Protocol SPort   DPort   Ingress I/F             Egress I/F
2012:33:1:2::2                          2012:33:1:2::1
UDP      49002   49003   n/a                     Serial2/0

Metadata Attributes :

Global Session Id           :   74657374-2D54-502D-3100-000000000000-00000000-00000000
Clock Frequency             :   123456
End Point Model             :   Test-TP-Model
Application Signaling Type  :   sip
Application Transport Type  :   rtp
Application Traffic Type    :   realtime
Application Device Class    :   room-conferencing
Application Category        :   voice-and-video
Application Group           :   telepresence-group
Application Media Type      :   video
Application Tag             :   218103921 (telepresence-media)
Application Name            :   telepresence-media

Matched filters :

 Direction: IN:
 Direction: OUT:
```

The table below describes the significant fields shown in the display.

***Table 189: show metadata flow local-flow-id Field Descriptions***

| Field | Description |
|---|---|
| To | Destination address of the flow entry. |
| From | Source address from where the flow entry is sent. |
| Protocol | Transport protocol, TCP or UDP, used for the flow. |
| SPort | Source port of the flow entry. Valid range is from 1 to 65535. |
| DPort | Destination port of the flow entry. Valid range is from 1 to 65535. |
| Ingress I/F | Ingress interface. Incoming interface for a given network element. |

| Field | Description |
|---|---|
| Egress I/F | Egress interface. Outgoing interface for a given network element. |
| Global Session ID | Global session ID of the application. |
| Clock Frequency | Frequency of the application clock. |
| End Point Model | Model of the application. |
| Application Signaling Type | Name of the application vendor. |
| Application Transport Type | Transport type of the metadata application. |
| Application Traffic Type | Traffic type of the metadata application. |
| Application Device Class | Classification of the metadata application. |
| Application Category | Category of the metadata application. |
| Application Group | Group of the metadata application. |
| Application Media Type | Type of media for the metadata application. |
| Application Tag | Application identifier.<br>• Every metadata application name is mapped to a unique application tag. |
| Application Name | Name of the metadata application. |
| Direction | Direction for the application. |

The following is sample output from the **show metadata flow statistics** command:

```
Device# show metadata flow statistics

Interface specific report :

Serial2/0: Classified flows : Ingress 0, Egress 0

Chunk statistics :

Type               Allocated       Returned        Failed

IP Flow             9               0               0
Flow Key            29              20              0
Source List         4               0               0
Flow Info           29              29              0
Attribute Data      29              29              0
Feature Object      2               0               0

Event Statistics:

Add Flow                : 9         Delete Flow             : 0
```

```
Received                : 30        Rejected                : 0
Transient               : 0         Posted                  : 29
Ingress Change          : 0         Egress Change           : 11
Unknown                  : 0         Source Limit Exceeded    : 0
```

The table below describes the significant fields shown in the displays.

***Table 190: show metadata flow statistics Field Descriptions***

| Field | Description |
|---|---|
| Interface specific report | Report specifying the number of egress or ingress flows per interface. |
| Ingress | Number of flows that entered the interface. |
| Egress | Number of flows that exited the interface. |
| Chunk statistics | Information specific to the chunk memory. |
| Type | Refers to the type of information or data structure usage for which memory consumption is recorded. |
| Allocated | Memory allocated for the specified type of information. |
| Returned | Memory returned to the system for the specified type of information. |
| Failed | Record of the memory allocation failures. |
| Event Statistics | Information specific to every flow event that has occurred on the device. |
| Add Flow | Number of flows added into the network element. |
| Delete Flow | Number of flows deleted from the network element. |
| Received | Number of flows received by the network element. |
| Rejected | Number of flows rejected by the network element. |
| Transient | Number of flows that are in transient state. |
| Posted | Number of change notifications received by the Resource Reservation Protocol (RSVP). |
| Ingress Change | Number of times the ingress interface changed. |
| Egress Change | Number of times the egress interface changed. |
| Unknown | Number of times an unknown event was received. |

| Field | Description |
|---|---|
| Source Limit Exceeded | Number of times the flow limit defined for the device was exceeded. |

The following is sample output from the **show metadata flow table** command:

```
Device# show metadata flow table

Total number of IPV4 metadata flows 6

Flow  To              From            Proto DPort SPort Ingress      Egress

4     10.0.0.1        10.0.0.2        UDP   49008 49007             Se2/0
6     10.0.0.3        10.0.0.4        UDP   49004 49003             Se2/0
5     10.2.0.3        10.2.0.6        UDP   49010 49009             Se2/0
2     10.2.1.6        10.2.2.6        UDP   49004 49003             Se2/0
1     10.2.2.6        10.2.3.6        UDP   49002 49001             Se2/0
3     10.2.3.6        10.2.3.7        UDP   49006 49005             Se2/0


Total number of IPV6 metadata flows 3

To                                      From
Flow  Proto DPort SPort Ingress      Egress

2001:DB8:1::1                          2001:DB8:1::2
9     UDP   49001 49000              Se2/0
2001:DB8:1::3                          2001:DB8:1::4
7     UDP   49001 49000              Se2/0
2001:DB8:1::12                         2001:DB8:1::13
8     UDP   49003 49002              Se2/0
```

**Note** The output for the IPv6 metadata flow table appears in two lines as the IPv6 addresses can be long.

The following is sample output from the **show metadata flow table application name sip ip** command:

```
Device#  show metadata flow table application name sip ip

Flow  To              From           Protocol  DPort  SPort  Ingress   Egress  SSRC

2     209.165.201.14  209.165.201.18  UDP      70    80       Eth1/1   Eth1/2  3000
```

The following is sample output from the **show metadata flow table application name sip ipv6** command:

```
Device# show metadata flow table application name sip ipv6

To                                      From
Flow  Proto DPort SPort Ingress      Egress

2001:DB8:1::3                          2001:DB8:1::4
9     UDP   49001 49000              Se2/0
2001:DB8:1::5                          2001:DB8:1::6
7     UDP   49001 49000              Se2/0
2001:DB8:1::12                         2001:DB8:1::14
8     UDP   49003 49002              Se2/0
```

The following is sample output from the **show metadata flow table filter destination** command. You can specify the source or destination IPv4 address as the filter criterion.

```
Device# show metadata flow table filter destination 209.165.201.1

Entries To: 209.165.201.1
```

```
Flow ID    From             Protocol DPort   SPort   Ingress I/F    Egress I/F
1          209.165.201.3    UDP      1000    1000    Et0/0          Et0/1
2          209.165.201.3    UDP      1001    1001    Et0/0          Et0/1
Total Flows: 2
```

The following is sample output from the **show metadata flow table ipv6** command:

```
Device# show metadata flow table ipv6

To                                    From
Flow  Proto DPort SPort Ingress      Egress

2001:DB8:1::1                          2001:DB8:1::2
9     UDP   49001 49000              Se2/0
2001:DB8:1::3                          2001:DB8:1::4
7     UDP   49001 49000              Se2/0
2001:DB8:1::12                         2001:DB8:1::13
8     UDP   49003 49002              Se2/0
```

## Related Commands

| Command | Description |
|---|---|
| **debug metadata** | Enables debugging for metadata flow. |
| **metadata application-params** | Enters metadata application entry configuration mode and creates new metadata application parameters. |
| **show metadata application table** | Displays a list of metadata applications defined on a device. |
| **metadata flow** | Enables metadata on a device. |

# show mls qos

To display multilayer switching (MLS) quality of service (QoS) information, use the **showmlsqos** command in privileged EXEC mode.

**show mls qos** [{**arp**| **ipv6**| **ip**| **ipx**| **last**| **mac**| **module** [ *module-number* ]} [*interface interface-number*| **slot** *slot*| **null 0**| **port-channel** *number*| **vlan** *vlan-id*]] **[detailed]**

## Syntax Description

| | |
|---|---|
| **arp** | (Optional) Displays Address Resolution Protocol (ARP) information. |
| **ipv6** | (Optional) Displays IPv6 information. |
| **ip** | (Optional) Displays information about the MLS IP status. |
| **ipx** | (Optional) Displays information about the MLS Internetwork Packet Exchange (IPX) status. |
| **last** | (Optional) Displays information about the last packet-policing. |
| **mac** | (Optional) Displays information about the MAC address-based QoS status. |
| **module** *module-number* | (Optional) Specifies the module (slot) number; displays the global and per-interface QoS enabled and disabled settings and the global QoS counters. |
| *interface* | (Optional) Interface type; valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **ge-wan**, **pos**, and **atm**. |
| *interface-number* | (Optional) Module and port number; see the "Usage Guidelines" section for valid values. |
| **slot** *slot* | (Optional) Specifies the slot number; displays the global and per-interface QoS enabled and disabled settings and the global QoS counters. |
| **null 0** | (Optional) Specifies the null interface; the only valid value is **0**. |
| **port-channel** *number* | (Optional) Specifies the channel interface; there is a maximum of 64 values ranging from 1 to 282. |

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) Specifies the VLAN ID; valid values are from 1 to 4094. |
| **detailed** | (Optional) Displays additional statistics. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | This command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(18)SXE | The **arp**and **ipv6** keywords were added on the Supervisor Engine 720 only. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXI | • The following information was added to the command output on the Catalyst 6500 series switch:<br>  • Display of last 30-second counters.<br>  • Display of peak 30-second counters over the last 5 minutes.<br>  • Display of 5-minute average and peak packets-per-second (pps) rates.<br>• The peak rates are monitored with 10-second resolution. Releases prior to Cisco IOS Release 12.2(33)SXI were monitored at 30-second resolution. |

## Usage Guidelines

The ge-wan, pos, and atm interfaces are not supported on systems that are configured with a Supervisor Engine 720.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **port-channel***number*values from 257 to 282 are supported on the Content Switching Module (CSM) and the Firewall Services Module (FWSM) only.

**Catalyst 6500 Series Switches**

In Cisco IOS Release 12.2(33)SXI and later releases, the following information is included in the output of the **showmlsqos** command:

- Display of last 30-second counters.

- Display of peak 30-second counters over the last 5 minutes.
- Display of 5-minute average and peak bps rates.

The peak rates are monitored with 10-second resolution. Releases prior to Cisco IOS Release 12.2(33)SXI are monitored at 30-second resolution.

## Examples

## Examples

This example shows how to display information about the last logged packet:

```
Router# show mls qos last
QoS engine last packet information:
    Packet was transmitted
    Output TOS/DSCP: 0xC0/48[unchanged]   Output COS: 0[unchanged]
    Aggregate policer index: 0(none)
    Microflow policer index: 0(none)
```

## Examples

This example shows how to display IPv6 information:

```
Router# show mls qos ipv6
QoS Summary [IPv6]:      (* - shared aggregates, Mod - switch module)
     Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                                  Id         Id
-------------------------------------------------------------------------------
      All  7   -    Default    0    0*    No  0      189115356              0
```

## Examples

This example shows how to display QoS information:

```
Router# show mls qos
QoS is enabled globally
Microflow policing is enabled globally
QoS ip packet dscp rewrite enabled globally
QoS is disabled on the following interfaces:
Fa6/3 Fa6/4
QoS DSCP-mutation map is enabled on the following interfaces:
Fa6/5
Vlan or Portchannel(Multi-Earl) policies supported: Yes
Egress policies supported: Yes
----- Module [5] -----
QoS global counters:
Total packets: 164
IP shortcut packets: 0
Packets dropped by policing: 0
IP packets with TOS changed by policing: 0
IP packets with COS changed by policing: 0
Non-IP packets with COS changed by policing: 0
MPLS packets with EXP changed by policing: 0
```

## Examples

This example shows the output if you do not enter any keywords:

```
Router# show mls qos
  QoS is enabled globally
  Microflow QoS is enabled globally
QoS global counters:
    Total packets: 217500
    IP shortcut packets: 344
    Packets dropped by policing: 344
    IP packets with TOS changed by policing 18323
```

```
    IP packets with COS changed by policing 1602
    Non-IP packets with COS changed by policing 0
```

## Examples

The **showmlsqos** command output in Cisco IOS Release 12.2(33)SXI and later releases contains more packet counter information than in previous releases.

This example shows the Cisco IOS Release 12.2(33)SXI output with the **detailed** keyword:

```
Router# show mls qos detailed
  QoS is enabled globally
  Policy marking depends on port_trust
  QoS ip packet dscp rewrite enabled globally
  Input mode for GRE Tunnel is Pipe mode
  Input mode for MPLS is Pipe mode
  Vlan or Portchannel(Multi-Earl) policies supported: Yes
  Egress policies supported: Yes
 ----- Module [5] -----
Traffic:            Total pkt's   30-s pkt's    peak pkts  5-min avg pps   peak pps
-------------------------------------------------------------------------------
Total packets:           775606           46           22               2          5
IP shortcut packets:    5465402           33           16               1          1
Packets dropped by
policing:                     0            0            0               0          0
IP packets with TOS
changed by policing:         41           10            4               0          0
IP packets with COS
changed by policing:          2            0            0               0          0
Non-IP packets with COS
changed by policing:          0            0            0               0          0
MPLS packets with EXP
changed by policing:          0            0            0               0          0
```

The table below describes the significant fields added when you enter the **detailed** keyword.

***Table 191: show mls qos detailed Field Descriptions***

| Field | Description |
|---|---|
| Total packets | The cumulative counters. |
| IP shortcut packets | Number of IP shortcut packets. |
| Packets dropped by policing | Number of police dropped packets. |
| Packets changed by policing | Number of police modified packets. |
| 30-s pkts | The total 30-second packet count over the last 5 minutes. |
| 30-s peak pkts | The peak 30-second packet count over the last 5 minutes. |
| 5-min avg pps | The average packets-per-second (pps) rate over the last 5 minutes. |
| 5-min peak pps | The peak pps rate over the last 5 minutes. |

## Related Commands

| Command | Description |
|---|---|
| **mls qos (global configuration mode)** | Enables the QoS functionality globally. |
| **mls qos (interface configuration mode)** | Enables the QoS functionality on an interface. |
| **show mls qos aggregate-policer** | Displays information about the aggregate policer. |
| **show mls qos free-agram** | Displays the number of free aggregate RAM indexes on the switch processor and the DFCs. |
| **show mls qos interface** | Displays MLS QoS information at the interface level. |
| **show mls qos maps** | Displays MLS QoS mapping information. |
| **show mls qos mpls** | Displays an interface summary for MPLS QoS classes in policy maps. |
| **show mls qos protocol** | Displays protocol pass-through information. |
| **show mls qos statistics-export** | Displays MLS statistics data-export status and configuration. |

# show mls qos aggregate policer

To display information about the aggregate policer for multilayer switching (MLS) quality of service (QoS), use the **showmlsqosaggregatepolicer** command in EXEC mode.

**show mls qos aggregate policer** [ *aggregate-name* ]

## Syntax Description

| | |
|---|---|
| *aggregate-name* | (Optional) Name of the aggregate policer. |

## Command Default

This command has no default settings.

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

Aggregate policing works independently on each Distributed Forwarding Card (DFC)-equipped switching module and independently on the Policy Feature Card 2 (PFC2), which supports any non-DFC-equipped switching modules. Aggregate policing does not combine flow statistics from different DFC-equipped switching modules. You can display aggregate-policing statistics for each DFC-equipped switching module, the PFC2, and any non-DFC-equipped switching modules that are supported by the PFC2.

## Examples

This example shows how to display information about the aggregate policer for MLS QoS:

```
Router# show mls qos aggregate-policer
ag1 (undefined)
    AgId=0 [ pol1 pol2 ]
ag2 64000 64000 conform-action set-dscp-transmit 56 exceed-action drop
    AgId=0 [ pol3 ]
ag3 32000 32000 conform-action set-dscp-transmit 34 exceed-action drop
```

In the output, the following applies:

- The **AgId** parameter displays the hardware-policer ID and is nonzero if assigned.
- The policy maps using the policer, if any, are listed in the square brackets ([]).
- If there are no policies using the policer, no **AgId** line is displayed.

- If the policer is referred to in policy maps, but has not been defined, [**undefined**] is displayed.

## Related Commands

| Command | Description |
|---|---|
| **mls qos aggregate-policer** | Defines a named aggregate policer for use in policy maps. |

# show mls qos free-agram

To display the number of free aggregate RAM indexes on the switch processor and the Distributed Forwarding Cards (DFCs), use the **showmlsqosfree-agram** command in EXEC mode.

**show mls qos free-agram**

## Syntax Description

This command has no arguments or keywords.

## Command Default

This command has no default settings.

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXD | Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2 |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Examples

This example shows how to display the number of free aggregate RAM indexes on the switch processor and the DFCs:

```
Router# show mls qos free-agram
Total Number of Available AG RAM indices : 1023
 Module [1]
 Free AGIDs : 1023
 Module [6]
 Free AGIDs : 1023
```

# show mls qos interface

To display Multilayer Switching (MLS) quality of service (QoS) information at the interface level, use the **showmlsqosinterface**command in privileged EXEC mode.

**show mls qos interface** [ *interface-id* ] **[policers]**

## Syntax Description

| | |
|---|---|
| *interface-id* | (Optional) Specifies the interface for which QoS information is to be displayed. |
| **policers** | (Optional) Displays all the policers configured on the interface, their settings, and the number of policers unassigned. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1(6)EA2 | This command was introduced. |
| 12.2(15)ZJ | This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Use the **showmlsqosinterface** command without keywords to display parameters for all interfaces.

Use the **showmlsqosinterface***interface-id* command to display the parameters for a specific interface.

On most Cisco switch platforms, the global command, "(no) mls qos", is used to toggle the MLS QoS state to be enabled or disabled. When MLS QoS is disabled globally, the CoS/IP Precidence/DSCP values for all traffic passing through the switch will not be modified. On the other hand, if MLS QoS is enabled, then by default all interfaces will be in an *untrusted* state, which means all incoming CoS/IP Prec/DSCP values will be remarked down to 0.

**Cisco_2600 and Cisco_3600 Series Switches**

Becuase the**(no)mlsqos**global command is not supported for the Cisco_2600 or Csico_3600 series switches, this presents a unique situationregarding the default trust state for the interface.

By default, when there is no "mls qos" related commands configured under an interface on the Cisco_2600 or Cisco_3600 series switches, the CoS/IP Prec/DSCP value of all incoming traffic will not be remarked as it passes through the switch. This has the same result as when MLS QoS is disabled on other Cisco switches.

## Examples

The following is sample output from the **showmlsqosinterfacefastethernet0/1**command:

```
Router# show mls qos interface fastethernet0/1
FastEthernet0/1
trust state: trust cos
COS override: dis
default COS: 0
```

The following example shows that there is no mls QoS command configured on the interface. the CoS/IP Precidence/DSCP values of incoming traffic will not be remarked as it passes through the switch.

```
Router# show mls qos interface f1/1
FastEthernet1/1
trust state: none  <<<
trust mode: none  <<<
COS override: dis
default COS: 0
pass-through: none
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos cos** | Defines the default MLS CoS value of a port or assigns the default CoS value to all incoming packets on the port. |
| **mls qos map** | Defines the MLS CoS-to-DSCP map and DSCP-to-CoS map. |
| **mls qos trust** | Configures the MLS port trust state and classifies traffic by an examination of the CoS or DSCP value. |

# show mls qos maps

To display multilayer switching (MLS) quality of service (QoS) mapping information, use the **showmlsqosmaps** command in privileged EXEC mode.

### Cisco 2600, 3660, 3700, 3845, 7200, 7400, and 7500 Series Routers

**show mls qos maps** [**cos-dscp**| **dscp-cos**]

### Cisco 7600 Series Router and Catalyst 6500 Series Switch

**show mls qos maps** [**cos-dscp**| **cos-mutation**| **dscp-cos**| **dscp-exp**| **dscp-mutation**| **exp-dscp**| **exp-mutation**| **ip-prec-dscp**| **policed-dscp**]

## Syntax Description

| | |
|---|---|
| **cos-dscp** | (Optional) Displays the class of service (CoS)-to-differentiated services code point (DSCP) map. |
| **dscp-cos** | (Optional) Displays the DSCP-to-CoS map. |
| **cos-mutation** | (Optional) Displays the CoS-mutation map. |
| **dscp-exp** | (Optional) Displays the DSCP-to-exp map. |
| **dscp-mutation** | (Optional) Displays the DSCP-mutation map. |
| **exp-dscp** | (Optional) Displays the exp-to-DSCP map. |
| **exp-mutation** | (Optional) Displays the exp-mutation map. |
| **ip-prec-dscp** | (Optional) Displays the IP-precedence-to-DSCP map. |
| **policed-dscp** | (Optional) Displays the policed-DSCP map. |

## Command Default

All MLS QoS maps are displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.1(6)EA2 | This command was introduced. |
| 12.2(14)SX | This command was implemented on the Cisco 7600 series routers. |

| Release | Modification |
|---|---|
| 12.2(15)ZJ | This command was implemented on the following platforms: Cisco 2600 series routers, Cisco 3600 series routers, and Cisco 3700 series routers. |
| 12.2(17b)SXA | This command was changed to support the **cos-mutation**, **exp-dscp**, and **exp-mutation** keywords. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers. |
| 12.2(33)SXI | Support was added for all map type keywords. |

## Usage Guidelines

Maps are used to generate an internal DSCP value, which represents the priority of the traffic. Use the **showmlsqosmaps** command without keywords to display all maps.

## Examples

The following is sample output from the **showmlsqosmapscos-dscp** command displaying the DSCP values to which each CoS value will be mapped:

```
Router# show mls qos maps cos-dscp
Cos-dscp map:
       cos:  0  1  2  3  4  5  6  7
     --------------------------------
      dscp:  8  8  8  8 24 32 56 56
```

The following is sample output from the **showmlsqosmapsdscp-cos** command displaying the CoS values to which each DSCP value will be mapped:

```
Router# show mls qos maps dscp-cos
Dscp-cos map:
       dscp:  0  8 10 16 18 24 26 32 34 40 46 48 56
     ---------------------------------------------
        cos:  0  1  1  1  2  2  3  3  4  4  5  6  7
```

This example shows how to display the QoS-map settings:

```
Router# show mls qos maps
   Policed-dscp map:
            0  1  2  3  4  5  6  7  8  9
   ---------------------------------
      00:  00 01 02 03 04 05 06 07 08 09
      10:  10 11 12 13 14 15 16 17 18 19
      20:  20 21 22 23 24 25 26 27 28 29
      30:  30 31 32 33 34 35 36 37 38 39
      40:  40 41 42 43 44 45 46 47 48 49
      50:  50 51 52 53 54 55 56 57 58 59
      60:  60 61 62 63
   Dscp-cos map:
            0  1  2  3  4  5  6  7  8  9
   ---------------------------------
      00:  00 00 00 00 00 00 00 00 01 01
      10:  01 01 01 01 01 01 02 02 02 02
      20:  02 02 02 02 03 03 03 03 03 03
      30:  03 03 04 04 04 04 04 04 04 04
      40:  05 05 05 05 05 05 05 05 06 06
```

```
      50:  06 06 06 06 06 06 07 07 07 07
      60:  07 07 07 07
   Cos-dscp map:
         cos:   0  1  2  3  4  5  6  7
       ---------------------------------
        dscp:   0  8 16 24 32 40 48 56
   IpPrecedence-dscp map:
       ipprec:   0  1  2  3  4  5  6  7
       ---------------------------------
        dscp:   0  8 16 24 32 40 48 56
Router#
```

In the policed DSCP and DSCP-CoS map displays, the new DSCP or CoS values are shown in the body of the table. The decade of the original DSCP value is shown in the left-side vertical column, and the units digit is in the top row. For example, the DSCP-CoS map indicates that if the original DSCP value is between 32 and 39, the CoS will be set to 4.

The CoS-DSCP and IP precedence-DSCP maps display the DSCP values to which each CoS or IP precedence value will be mapped. For example, the IP precedence-DSCP map indicates that if the original IP precedence value is 3, the DSCP will be set to 24.

This example shows how to verify the configuration of DSCP-mutation mapping:

```
Router# show mls qos maps | begin DSCP mutation

DSCP mutation map mutmap1:                    (dscp= d1d2)
     d1 :  d2 0  1  2  3  4  5  6  7  8  9
     ------------------------------------
      0 :    00 01 02 03 04 05 06 07 08 09
      1 :    10 11 12 13 14 15 16 17 18 19
      2 :    20 21 22 23 24 25 26 27 28 29
      3 :    08 31 32 33 34 35 36 37 38 39
      4 :    40 41 42 43 44 45 46 47 48 49
 <...Output Truncated...>
Router#
```

In the DSCP mutation map display, the marked-down DSCP values are shown in the body of the table. The first digit (d1) of the original DSCP value is in the left-side vertical column labeled d1, and the second digit (d2) is in the top row. For example, a DSCP value of 30 maps to a new DSCP value of 08.

## Related Commands

| Command | Description |
|---|---|
| **mls qos map** | Defines the CoS-to-DSCP map and DSCP-to-CoS map. |
| **mls qos map cos-dscp** | Defines the ingress CoS-to-DSCP map for trusted interfaces. |
| **mls qos map cos-mutation** | Maps a packet's CoS to a new CoS value. |
| **mls qos map dscp-cos** | Defines an egress DSCP-to-CoS map. |
| **mls qos map dscp-mutation** | Defines a named DSCP mutation map. |
| **mls qos map ip-prec-dscp** | Defines an ingress IP precedence-to-DSCP map for trusted interfaces. |
| **mls qos map policed-dscp** | Sets the mapping of policed DSCP values to marked-down DSCP values. |

# show mls qos mpls

To display an interface summary for Multiprotocol Label Switching (MPLS) quality of service (QoS) classes in policy maps, use the **showmlsqosmpls** command in user EXEC or privileged EXEC mode.

**show mls qos mpls** [**interface-type** *interface-number*| **module slot**]

## Syntax Description

| | |
|---|---|
| *interface-type interface-number* | (Optional) Interface type; valid values are the following:<br>• **fastethernet**<br>• **gigabitethernet**<br>• **tengigabitethernet** .<br>(Optional) Module and port number; see the “Usage Guidelines” section for valid values. |
| **module** slot | (Optional) Specifies the module slot number. |

## Command Modes

User EXEC Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(17a)SX | This command was introduced on the Supervisor Engine 720. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |

## Usage Guidelines

This command is supported in PFC3BXL or PFC3B mode only.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

## Examples

The following example shows an interface summary for MPLS QoS classes in policy maps:

```
Router# show mls qos mpls
QoS Summary [MPLS]: (* - shared aggregates, Mod - switch module)
Int Mod Dir Class-map DSCP Agg Trust Fl AgForward-By AgPoliced-By
Id Id
-------------------------------------------------------------------------------------------------------
```

```
Fa3/38 5 In exp2 0 1 dscp 0 378900 0
Fa3/41 5 In exp4 0 3 dscp 0 0 0
All 5 - Default 0 0* No 0 1191011240 0
```

The table below describes the significant fields shown in the display.

***Table 192: show mls qos mpls Field Descriptions***

| Field | Description |
|---|---|
| QoS Summary [MPLS]: (* - shared aggregates, Mod - switch module) | Shows if there are any shared aggregate policers, indicated by *, and the type of module. |
| Int Mod Dir Class-map DSCP Agg Trust Fl AgForward-By AgPoliced-By | Provides the column headings for the following lines in the display. These include interface name and number, module number, direction, class-map name, and DSCP value. |
| Fa3/38 5 In exp2 0 1 dscp 0 378900 0 | Provides the following information:<br>• Fa3/38--Interface name and number.<br>• 5--Module number in the chassis.<br>• In--Direction of the policy applied (In = ingress).<br>• exp2--Class map configured in the policy.<br>• 0--Differentiated Services Code Point (DSCP) value.<br>• 1--Policer ID assigned to that class map.<br>• dscp--Trust value configured on the port. In this example, the value is trusting on DSCP.<br>• 0--The flow ID if the flow policer is configured.<br>• 378900--The aggregate forwarded bytes, meaning the forwarded traffic.<br>• 0--The aggregate policed bytes, meaning this traffic has been subjected to policing. |
| All 5 - Default 0 0* No 0 1191011240 0 | The total of the preceding lines including the aggregate forwarded and aggregate policed bytes. |

## Related Commands

| Command | Description |
|---|---|
| **mls qos exp-mutation** | Attaches an egress-EXP mutation map to the interface. |
| **mls qos map exp-dscp** | Defines the ingress EXP value to the internal DSCP map. |

| Command | Description |
|---|---|
| **mls qos map exp-mutation** | Maps a packet's EXP to a new EXP value. |

# show mls qos protocol

To display protocol pass-through information, use the **showmlsqosprotocol**command in EXEC mode.

**show mls qos protocol** [**module** *number*]

## Syntax Description

| | |
|---|---|
| **module** *number* | (Optional) Specifies the module number. |

## Command Default

This command has no default settings.

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(17a)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(18)SXE | Support for this command was introduced on the Supervisor Engine 2 but does not support Address Resolution Protocol (ARP), Integrated Intermediate System-to-Intermediate System (IS-IS), or Enhanced Interior Gateway Routing Protocol (EIGRP).<br>Support for neighbor discovery protocol packets was added on the Supervisor Engine 720 only. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Examples

This example shows how to display protocol pass-through information:

```
Router# show mls qos protocol
RIP : Passthru mode
OSPF : Passthru mode
ND : Policing mode Cir = 32000 Burst = 1000
----- Module [5] -----
Routing protocol RIP is using AgId 0*
Routing protocol OSPF is using AgId 0*
Routing protocol ND is using AgId 1
----- Module [6] -----
Routing protocol RIP is using AgId 0*
Routing protocol OSPF is using AgId 0*
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos protocol** | Defines the routing-protocol packet policing . |

# show mls qos queuing interface

To display the queueing statistics of an interface, use the **showmlsqosqueuinginterface**command in user EXEC mode.

**show mls qos queuing interface** {*type*| **vlan**}

## Syntax Description

| | |
|---|---|
| *type* | Interface type.<br>For Cisco 7600 series routers, the valid interface types are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**. |
| **vlan** | Specifies the VLAN identification number; valid values are from 1 to 4094. |

## Command Modes

User EXEC (>)

## Command History

| Release | Modification |
|---|---|
| 15.0(1)S | This command was introduced on LAN cards on Cisco 7600 Series Routers. |

## Usage Guidelines

### Cisco 7600 Series Routers

The pos, atm, and ge-wan interfaces are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

The *typenumber*argument used with the **interface** keyword designates the module and port number. Valid values depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Use the **showqm-spport-data**command to verify the values that are programmed in the hardware.

## Examples

The following example shows sample output from the **showmlsqosqueuinginterfacegigabitethernet5/1**command on the Endor (RSP720-10G) card.

```
Router# show mls qos queuing interface gig5/1
Weighted Round-Robin
  Port QoS is enabled
  Port is untrusted
  Extend trust state: not trusted [COS = 0]
  Default COS is 0
```

```
    Queueing Mode In Tx direction: mode-cos
    Transmit queues [type = 1p3q8t]:
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       01         WRR                 08
       02         WRR                 08
       03         WRR                 08
       04         Priority            01
WRR bandwidth ratios:  100[queue 1] 150[queue 2] 200[queue 3]
    queue-limit ratios:     50[queue 1]  20[queue 2]  15[queue 3]  15[Pri Queue]
    queue tail-drop-thresholds
    --------------------------
    1     70[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    2     70[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    3     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    queue random-detect-min-thresholds
    ----------------------------------
      1    40[1] 70[2] 70[3] 70[4] 70[5] 70[6] 70[7] 70[8]
      2    40[1] 70[2] 70[3] 70[4] 70[5] 70[6] 70[7] 70[8]
      3    70[1] 70[2] 70[3] 70[4] 70[5] 70[6] 70[7] 70[8]
    queue random-detect-max-thresholds
    ----------------------------------
      1    70[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      2    70[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      3    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    WRED disabled queues:
    queue thresh cos-map
    ---------------------------------------
    1     1      0
    1     2      1
    1     3
    1     4
    1     5
    1     6
    1     7
    1     8
    2     1      2
    2     2      3 4
    2     3
    2     4
    2     5
    2     6
    2     7
    2     8
    3     1      6 7
    3     2
    3     3
    3     4
    3     5
    3     6
    3     7
    3     8
    4     1      5
    Queueing Mode In Rx direction: mode-cos
    Receive queues [type = 2q8t]:
    Queue Id    Scheduling  Num of thresholds
    -----------------------------------------
       01         WRR                 08
       02         WRR                 08
    WRR bandwidth ratios:  100[queue 1]   0[queue 2]
    queue-limit ratios:    100[queue 1]   0[queue 2]
    queue tail-drop-thresholds
    --------------------------
    1     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    2     100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    queue random-detect-min-thresholds
    ----------------------------------
      1    40[1] 40[2] 50[3] 50[4] 50[5] 50[6] 50[7] 50[8]
      2    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
    queue random-detect-max-thresholds
    ----------------------------------
      1    70[1] 80[2] 90[3] 100[4] 100[5] 100[6] 100[7] 100[8]
      2    100[1] 100[2] 100[3] 100[4] 100[5] 100[6] 100[7] 100[8]
```

```
    queue thresh cos-map
    ---------------------------------------
    1     1      0 1 2 3 4 5 6 7
    1     2
    1     3
    1     4
    1     5
    1     6
    1     7
    1     8
    2     1
    2     2
    2     3
    2     4
    2     5
    2     6
    2     7
    2     8
  Packets dropped on Transmit:
    queue     dropped  [cos-map]
    ---------------------------------------------
    1                         0  [0 1 ]
    2                         0  [2 3 4 ]
    3                         0  [6 7 ]
    4                         0  [5 ]
  Packets dropped on Receive:
    BPDU packets:  0
    queue              dropped  [cos-map]
    ------------------------------------------------
    1                         0  [0 1 2 3 4 5 6 7 ]
    2                         0  []
.
.
.
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos cos** | Defines the default MLS CoS value of a port or assigns the default CoS value to all incoming packets on the port. |
| **mls qos map** | Defines the MLS CoS-to-DSCP map and DSCP-to-CoS map. |
| **mls qos trust** | Configures the MLS port trust state and classifies traffic by an examination of the CoS or DSCP value. |
| **custom-queue-list** | Assigns a custom queue list to an interface. |
| **fair-queue (class-default)** | Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy. |
| **fair-queue (WFQ)** | Enables WFQ for an interface. |
| **priority-group** | Assigns the specified priority list to an interface. |
| **random-detect flow** | Enables flow-based WRED. |
| **random-detect (interface)** | Enables WRED or DWRED. |

| Command | Description |
|---|---|
| **random-detect (per VC)** | Enables per-VC WRED or per-VC DWRED. |
| **show frame-relay pvc** | Displays information and statistics about WFQ for a VIP-based interface. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |
| **show qm-sp port-data** | Displays information about the QoS manager switch processor. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# show mls qos statistics-export info

To display information about the multilayer switching (MLS)-statistics data-export status and configuration, use the **showmlsqosstatistics-exportinfo**command in EXEC mode

**show mls qos statistics-export info**

## Syntax Description

This command has no keywords or arguments.

## Command Default

This command has no default settings.

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

Quality of service (QoS)-statistics data export is not supported on Optical Service Module (OSM) interfaces.

## Examples

This example shows how to display information about the MLS-statistics data-export status and configuration:

```
Router# show mls qos statistics-export info
QoS Statistics Data Export Status and Configuration information
---------------------------------------------------------------
Export Status : enabled
Export Interval : 250 seconds
Export Delimiter : @
Export Destination : 172.20.52.3, UDP port 514 Facility local6, Severity debug

QoS Statistics Data Export is enabled on following ports:
---------------------------------------------------------
FastEthernet5/24

QoS Statistics Data export is enabled on following shared aggregate policers:
-----------------------------------------------------------------------------
aggr1M

QoS Statistics Data Export is enabled on following class-maps:
--------------------------------------------------------------
class3
```

## Related Commands

| Command | Description |
|---|---|
| **mls qos statistics-export (global configuration)** | Enables QoS-statistics data export globally. |
| **mls qos statistics-export (interface configuration)** | Enables per-port QoS-statistics data export. |
| **mls qos statistics-export aggregate-policer** | Enables QoS-statistics data export on the named aggregate policer. |
| **mls qos statistics-export class-map** | Enables QoS-statistics data export for a class map. |
| **mls qos statistics-export delimiter** | Sets the QoS-statistics data-export field delimiter. |
| **mls qos statistics-export destination** | Configures the QoS-statistics data-export destination host and UDP port number. |
| **mls qos statistics-export interval** | Specifies how often a port and/or aggregate-policer QoS-statistics data is read and exported. |

# show platform hardware acl entry global-qos

To display information about inbound and outbound access control list (ACL) ternary content addressable memory (TCAM) global Quality of Service (QoS) entries, use the**showplatformhardwareaclentryglobal-qos** command in privileged EXEC mode.

**show platform hardware acl entry global-qos** {**in**| **out**} {**arp**| **ip**| **ipv6**| **mac**| **mpls**} **[detail]**

## Syntax Description

| | |
|---|---|
| **in** | Displays inbound entries in the output. |
| **out** | Displays outbound entries in the output. |
| **arp** | Specifies the Address Resolution Protocol for entries. |
| **ip** | Specifies the Internet Protocolfor entries. |
| **ipv6** | Specifies the Internet Protocol, Version 6 for entries. |
| **mac** | Specifies the Media Access Control address for entries. |
| **mpls** | Specifies the Multiprotocol Label Switching Protocol for entries. |
| **detail** | Displays detailed information about the entries. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2XJC | This command was introduced. |

## Usage Guidelines

Cisco IOS-based switches support the wire-rate ACL and QoS feature with use of the TCAM. Enabling ACLs and policies does not decrease the switching or routing performance of the switch as long as the ACLs are fully loaded in the TCAM.

To implement the various types of ACLs and QoS policies in hardware, the Cisco IOS-based switches use hardware lookup tables (TCAM) and various hardware registers in the Supervisor Engine. When a packet arrives, the switch performs a hardware table lookup (TCAM lookup) and decides to either permit or deny the packet.

## Examples

The following sample output from the **showplatformhardwareaclentryglobal-qos** command displays one result for inbound Address Resolution Protocol entries:

```
Switch# show platform hardware acl entry global-qos in arp

0x0000000000000003 arp ip any any mac any
```

The following sample output from the **showplatformhardwareaclentryglobal-qos** command displays the *detailed* results for inbound Address Resolution Protocol entries (the legend provides definitions for abbreviations that may appear in the output):

```
Switch# show platform hardware acl entry global-qos in arp detail
-----------------------------------------------------------------------------------------------
ENTRY TYPE: A - ARP I - IPv4 M - MPLS O - MAC Entry S - IPv6(Six) C - Compaction L - L2V4
Suffix: D - dynamic entry E - exception entry R - reserved entry
FIELDS: FS - first_seen/from_rp ACOS - acos/group_id F - ip_frag FF - frag_flag DPORT -
dest_port SPORT - src_port LM - L2_miss GP - gpid_present ETYPE - enc_etype CEVLD -
ce_vlan_valid MM - mpls_mcast FN - exp_from_null IV - ip_hdr_vld MV - mpls_valid E_CAU -
exception_cause UK - U_key ACO - acos A/R - arp_rarp RR - req_repl GM - global_acl_fmt_match
 D-S-S-A - dest_mac_bcast, src_snd_mac_same, snd_tar_mac_same, arp_rarp_vld OM - ofe_mode
SVLAN - Src_vlan
-----------------------------------------------------------------------------------------------
```

| A | INDEX | LABEL | A/R | RR | IP SA | IP DA | SRC MAC | D-S-S-A | GM | LM | OM | RSLT | CNT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| AR V | 963 | 8191 | 1 | 7 | 0.0.0.0 | 0.0.0.0 | FFFF.FFFF.FFFF | 1-1-1-1 | 1 | 1 | 0 | [redacted] | 0 |
| AR M | 963 | 0x0000 | 0 | 0x0 | 0.0.0.0 | 0.0.0.0 | 0000.0000.0000 | 0-0-0-1 | 0 | 0 | 1 | | |

| Command | Description |
|---|---|
| **mls qos protocol** | Configures TCAM entries that are displayed by the **showplatformhardwareaclentryglobal-qos** command. |

# show platform hardware pp active infrastructure pi npd rx policer

To display punt policing statistics for all queues, use the **show platform hardware pp active infrastructure pi npd rx policer** command in privileged EXEC mode.

**show platform hardware pp active infrastructure pi npd rx policer**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled (no information about the punt policer is displayed).

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.5S | This command was introduced on the Cisco ASR 903 router. |

## Usage Guidelines

Use the **show platform hardware pp active infrastructure pi npd rx policer** command to view the punt rate and burst rate statistics for all queues and to verify the punt policier settings.

## Examples

The following is sample output from the **show platform hardware pp active infrastructure pi npd rx policer** command:

```
Router# show platform hardware pp active infrastructure pi npd rx policer

PUNT POLICER
Ring |          Queue Name |           Punt rate |          Burst rate
-----+---------------------+---------------------+--------------------
 0   |     SW FORWARDING Q |                 500 |                1000
 1   |  ROUTING PROTOCOL Q |                 500 |                1000
 2   |              ICMP Q |                 500 |                1000
 3   |              HOST Q |                1000 |                2000
 4   |       ACL LOGGING Q |                 500 |                1000
 5   |               STP Q |                3000 |                6000
 6   |       L2 PROTOCOL Q |                1000 |                2000
 7   |     MCAST CONTROL Q |                1000 |                2000
 8   |         BROADCAST Q |                 500 |                1000
 9   |               REP Q |                3000 |                6000
10   |               CFM Q |                3000 |                6000
11   |           CONTROL Q |                1000 |                2000
12   |       IP MPLS TTL Q |                1000 |                2000
13   |     DEFAULT MCAST Q |                 500 |                1000
14   |  MCAST ROUTE DATA Q |                 500 |                1000
15   |    MCAST MISMATCH Q |                 500 |                1000
16   |          RPF FAIL Q |                 500 |                1000
17   |  ROUTING THROTTLE Q |                 500 |                1000
```

```
18   |             MCAST Q |                500 |                1000
19   |          MPLS OAM Q |               1000 |                2000
20   |       IP MPLS MTU Q |                500 |                1000
21   |               PTP Q |               3000 |                6000
22   |          LINUX ND Q |                500 |                1000
23   |         KEEPALIVE Q |               1000 |                2000
24   |              ESMC Q |               3000 |                6000
25   |          FPGA BFD Q |               3000 |                6000
26   |          FPGA CCM Q |               3000 |                6000
27   |          FPGA CFE Q |               3000 |                6000
28   |          L2PT DUP Q |               4000 |                8000
```

The table below describes the significant fields shown in the display.

***Table 193: show platform hardware pp active infrastructure pi npd rx policer Field Descriptions***

| Field | Description |
|---|---|
| Ring | Unique number that identifies the queue. |
| Queue Name | Name of the queue. |
| Punt rate | Punt rate for the queue, in packets per second (pps). |
| Burst rate | The burst-rate for the queue, in packets per second (pps). |

## Related Commands

| Command | Description |
|---|---|
| **platform punt-police queue** | Enables punt policing on a queue and specifies the maximum punt rate and burst rate on a per-queue basis. |
| **show platform software infrastructure punt statistics** | Displays whether queue-based punt policing is enabled. |

# show platform hardware qfp active feature qos config global

To display whether the QoS: Packet Marking Statistics and QoS: Packet Matching Statistics features are currently enabled, use the **showplatformhardwareqfpactivefeatureqosconfigglobal** command in privileged EXEC mode.

**show platform hardware qfp active feature qos config global**

## Syntax Description

| | |
|---|---|
| **hardware** | Hardware |
| **qfp** | Quantum flow processor |
| **active** | Active instance |
| **feature** | Feature specific information |
| **qos** | Quality of Service (QoS) information |
| **config** | QoS config information |
| **global** | Global configuration |

## Command Default

Disabled (no information about the status of the QoS: Packet Marking Statistics or QoS: Packet Matching Statistics feature is displayed).

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.3S | This command was introduced. |

## Usage Guidelines

Both the QoS: Packet Marking Statistics and QoS: Packet Matching Statistics features are disabled by default. Use the **showplatformhardwareqfpactivefeatureqosconfigglobal** command to display whether they are enabled.

## Examples

The following example shows how to see if the QoS: Packet Marking Statistics or QoS: Packet Matching Statistics feature is enabled:

```
Router#
show platform hardware qfp active feature qos config global
```

```
Marker statistics are: enabled
Match per filter statistics are: enabled
```

The table below describes the significant fields shown in the display.

***Table 194: show platform hardware qfp active feature qos config global Field Descriptions***

| Field | Description |
|---|---|
| Marker statistics are: | The status of the QoS: Packet Marking Statistics feature, enabled or disabled. |
| Match per filter statistics are: | The status of the QoS: Packet Matching Statistics feature, enabled or disabled. |

## Related Commands

| Command | Description |
|---|---|
| **platform qos marker-statistics** | Displays the number of packets that have modified headers and have been classified into a category for local router processing. |
| **platform qos match-statistics per-filter** | Displays the display the number of packets and bytes matching a user-defined filter. |

# show platform lowq

To display the number of low queues configured on each interface, use the **showplatformlowq** command.

**show platform lowq**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC(#)

## Command History

| Release | Modification |
|---|---|
| 15.0(1) S | This command was introduced. |

## Usage Guidelines

Use the**showplatformlowq**command to check the number of queues per interface, if you are using low-queue line cards. If there are no queues configured on any line card, a message is displayed to show that low queue is empty.

## Examples

The following is a sample output of the **showplatformlowq**command.

```
Router# show platform lowq
TenGigabitEthernet10/1
Input Queue count:8     Output Queue count:8    Total Queue count:16
```

The following table describes the fields in the command:

| Field | Description |
|---|---|
| Input Queue Count | Number of input low queues on the interface. |
| Output Queue Count | Number of output low queues on the interface. |
| Total Queue Count | Sum of the input and output low queues. |

# show platform qos policy-map

To display the type and number of policy maps that are configured on the router, use the **showplatformqospolicy-map**command in privileged EXEC mode.

**show platform qos policy-map**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXE | This command was introduced for Cisco Catalyst 6500 series switches and Cisco 7600 series routers. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

On Cisco Catalyst 6500 series switches and Cisco 7600 series routers, you cannot attach a quality of service (QoS) policy map with **matchinputvlan** to an interface if you have already attached a QoS policy map to a VLAN interface (a logical interface that has been created with the **interfacevlan** command). If you attempt to use both types of service policies, you must remove both types of service policies before you can add the policy maps.

The **showplatformqospolicy-map** command shows whether the router is currently configured for **interfacevlan** and **matchinputvlan** service policies. It also shows the number of policy maps for each type.

## Examples

The following example shows a router that has service policies configured only on VLAN interfaces:

```
Router# show platform qos policy-map

 service policy configured on int vlan: TRUE
 # of int vlan service policy instances: 3
 match input vlan service policy configured: FALSE
 # of match input vlan service policy instances: 0
```

The following example shows a router that has service policies configured on VLAN interfaces and that has a service policy configured with **matchinputvlan**. In this configuration, you must remove all service policies from their interfaces, and then configure only one type or another.

```
Router# show platform qos policy-map

 service policy configured on int vlan: TRUE
 # of int vlan service policy instances: 1
 match input vlan service policy configured: TRUE
 # of match input vlan service policy instances: 1
```

The table below describes each field shown in the **showplatformqospolicy-map** command:

*Table 195: show platform qos policy-map Field Descriptions*

| Field | Description |
|---|---|
| service policy configured on int vlan | Indicates whether any QoS policy maps are configured on VLAN interfaces. |
| # of int vlan service policy instances | Number of QoS policy maps that are configured on VLAN interfaces. |
| match input vlan service policy configured | Indicates whether any QoS policy maps that use the **matchinputvlan** command are configured on interfaces. |
| # of match input vlan service policy instances | Number of QoS policy maps using the **matchinputvlan** command that are configured on interfaces. |

## Related Commands

| Command | Description |
|---|---|
| **match input vlan** | Configures a class map to match incoming packets that have a specific virtual local area network (VLAN) ID. |
| **match qos-group** | Identifies a specified QoS group value as a match criterion. |
| **mls qos trust** | Sets the trusted state of an interface, to determine which incoming QoS field on a packet, if any, should be preserved. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **service-policy** | Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

| Command | Description |
|---|---|
| **show platform qos policy-map** | Displays the type and number of policy maps that are configured on the router. |

# show platform software infrastructure punt statistics

To display whether queue-based punt policing is enabled, use the **show platform software infrastructure punt statistics** command in privileged EXEC mode.

**show platform software infrastructure punt statistics**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled (no information about punt policing statistic configuration is displayed).

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.5S | This command was introduced on the Cisco ASR 903 router. |

## Usage Guidelines

Use the **show platform software infrastructure punt statistics** command to verify that queue-based punt policing is enabled on a queue. If the feature is configured on your interface, the command output displays punt police statistics.

## Examples

The following is sample output from the **show platform software infrastructure punt statistics** command:

```
        Router# show platform software infrastructure punt statistics
UEA Punt Statistics

Global drops : 0

 Queue Name             | Rx count                   |  Drop count
------------------------+----------------------------+-----------------------
 SW FORWARDING Q        | 0                          | 0
 ROUTING PROTOCOL Q     | 0                          | 0
 ICMP Q                 | 0                          | 0
 HOST Q                 | 57115                      | 0
 ACL LOGGING Q          | 0                          | 0
 STP Q                  | 0                          | 0
 L2 PROTOCOL Q          | 6571                       | 0
 MCAST CONTROL Q        | 208839                     | 0
 BROADCAST Q            | 4                          | 0
 REP Q                  | 0                          | 0
 CFM Q                  | 0                          | 0
 CONTROL Q              | 0                          | 0
 IP MPLS TTL Q          | 0                          | 0
 DEFAULT MCAST Q        | 0                          | 0
 MCAST ROUTE DATA Q     | 0                          | 0
 MCAST MISMATCH Q       | 0                          | 0
 RPF FAIL Q             | 0                          | 0
 ROUTING THROTTLE Q     | 87                         | 0
 MCAST Q                | 0                          | 0
 MPLS OAM Q             | 0                          | 0
```

```
IP MPLS MTU Q           | 0                         | 0
PTP Q                   | 0                         | 0
LINUX ND Q              | 0                         | 0
KEEPALIVE Q             | 0                         | 0
ESMC Q                  | 0                         | 0
FPGA BFD Q              | 0                         | 0
FPGA CCM Q              | 0                         | 0
FPGA CFE Q              | 0                         | 0
L2PT DUP Q              | 0                         | 0
```

The table below describes the significant fields shown in the display.

***Table 196: show platform software infrastructure punt statistics Field Descriptions***

| Field | Description |
|---|---|
| Queue Name | Name of the queue. |
| Rx count | Number of received packet for the specified queue. |
| Drop count | Number of dropped packets for the specified queue. |

## Related Commands

| Command | Description |
|---|---|
| **platform punt-police queue** | Enables punt policing on a queue , and specifies the maximum punt rate and burst rate on a per-queue basis. |
| **show platform hardware pp active infrastructure pi npd rx policer** | Displays punt policing statistics for all queues. |

# show policy-manager events

To display detailed information about the policy-manager event statistics, use the **showpolicy-managerevents** command in privileged EXEC mode.

**show policy-manager events**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(1) | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| Cisco IOS XE Release 2.1 | This command was implemented on the Cisco ASR 1000 series routers. |

## Examples

The following is sample output from the **showpolicy-managerevents**command:

```
Router# show policy-manager events
Event Statistics
0          catastrophic
0          critical
0          high
0          medium
0          low
0          positive
The following events were discarded
0          unknown
Event buffer pool
Number of free event buffers = 300
Number of events awaiting processing by Policy Manager process = 0
```

The table below describes the significant fields shown in the display.

***Table 197: show policy-manager events Field Descriptions***

| Field | Description |
|---|---|
| catastrophic | Displays the total number of events in a catastrophic state. |
| critical | Displays the total number of events in a critical state. |

| Field | Description |
|---|---|
| high | Displays the total number of events in a high severity state. |
| medium | Displays the total number of events in a medium severity state. |
| low | Displays the total number of events in a low severity state. |
| positive | Displays the total number of events that are safe. |
| Number of free event buffers | Displays the total number of event buffers that are free. |
| Number of events awaiting processing by Policy Manager process | Displays the number of events that are yet to be processed by the policy manager. |

## Related Commands

| Command | Description |
|---|---|
| **show policy-manager policy** | Displays different policies of the policy manager. |
| **show policy-manager subsystem** | Displays subsystems of the policy manager. |

# show policy-manager policy

To display information about the policy-manager policy database, use the **showpolicy-managerpolicy** command in privileged EXEC mode.

### Cisco IOS SX, T, and XE Trains

**show policy-manager policy** [*policy-id*| **detail**| **subsystem** *subsystem-name* [**detail**| **policy-name** *name*]]

### Cisco IOS SR Train

**show policy-manager policy** [*policy-id*| **detail**| **event-id**| **policy-id**| **subsystem** *subsystem-name* [**detail**| **policy-name** *name*]]

## Syntax Description

| | |
|---|---|
| *policy-id* | (Optional) Displays information about the policy with the specified policy ID. The range is from 1 to 4294967295. |
| **detail** | (Optional) Displays policy database information in detail. |
| **subsystem** | (Optional) Displays information about the specified subsystem. |
| *subsystem-name* | (Optional) Name of the subsystem. |
| **policy-name** | (Optional) Displays information about the specified policy. |
| *name* | (Optional) Name of the policy. |
| **event-id** | (Optional) Displays information about the event ID table. |
| **policy-id** | (Optional) Displays information about the policy ID table. |

## Command Default

If no argument or keywords are specified, information about all policies is displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(24)T | This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T. |
| 12.2(33)SRC | This command was modified and integrated into a release earlier than Cisco IOS Release 12.2(33)SRC. The **event-id** and **policy-id** keywords were added. |
| 12.2(33)SXI | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |

## Examples

The following is sample output from the **showpolicy-managerpolicy** command. The field descriptions are self-explanatory.

```
Router# show policy-manager policy
Status (S) codes:
A = active
D = deactivated
S ID    Subsystem                Name
```

## Related Commands

| Command | Description |
|---|---|
| **show policy-manager events** | Displays detailed information about the policy-manager event statistics. |
| **show policy-manager subsystem** | Displays subsystems of the policy manager. |

# show policy-map

To display the configuration of all classes for a specified service policy map or of all classes for all existing policy maps, use the **showpolicy-map**command in user EXEC or privileged EXEC mode.

**show policy-map** [ *policy-map* ]

## Syntax Description

| | |
|---|---|
| *policy-map* | (Optional) Name of the service policy map whose complete configuration is to be displayed. The name can be a maximum of 40 characters. |

## Command Default

All existing policy map configurations are displayed.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE. |
| 12.0(7)S | This command was intergrated into Cisco IOS Release 12.0(7)S. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.2(4)T | This command was modified for two-rate traffic policing to display burst parameters and associated actions. |
| 12.2(8)T | The command was modified for the Policer Enhancement--Multiple Actions feature and the Weighted Random Early Detection (WRED)--Explicit Congestion Notification (ECN) feature. |
| 12.2(13)T | The following modifications were made:<br>• The output was modified for the Percentage-Based Policing and Shaping feature.<br>• This command was modified as part of the Modular QoS CLI (MQC) Unconditional Packet Discard feature. Traffic classes can now be configured to discard packets belonging to a specified class.<br>• This command was modified for the Enhanced Packet Marking feature. A mapping table (table map) can now be used to convert and propagate packet-marking values. |

| Release | Modification |
|---|---|
| 12.2(15)T | This command was modified to support display of Frame Relay voice-adaptive traffic-shaping information. |
| 12.0(28)S | The output of this command was modified for the QoS: Percentage-Based Policing feature to display the committed (conform) burst (bc) and excess (peak) burst (be) sizes in milliseconds (ms). |
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB, and the command was modified to display information about Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunnel marking. |
| 12.2(31)SB2 | This command was enhanced to display bandwidth-remaining ratios configured on traffic classes and ATM overhead accounting, and was implemented on the Cisco 10000 series router for the PRE3. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SRC | Support for the Cisco 7600 series router was added. |
| 12.4(15)T2 | This command was modified to display information about Generic Routing Encapsulation (GRE) tunnel marking.<br>**Note** For this release, GRE-tunnel marking is supported on the Cisco MGX Route Processor Module (RPM-XF) platform *only* . |
| 12.2(33)SB | This command was modified to display information about GRE-tunnel marking, and support for the Cisco 7300 series router was added. This command's output was modified on the Cisco 10000 series router for the PRE3 and PRE4. |
| Cisco IOS XE 2.1 | This command was integrated into Cisco IOS XE Release 2.1 and was implemented on the Cisco ASR 1000 series router. |
| 12.4(20)T | This command was modified. Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC). |

## Usage Guidelines

The **showpolicy-map** command displays the configuration of a policy map created using the **policy-map** command. You can use the **showpolicy-map** command to display all class configurations comprising any existing service policy map, whether or not that policy map has been attached to an interface. The command displays:

- ECN marking information only if ECN is enabled on the interface.

- Bandwidth-remaining ratio configuration and statistical information, if configured and used to determine the amount of unused (excess) bandwidth to allocate to a class queue during periods of congestion.

**Cisco 10000 Series Router**

In Cisco IOS Release 12.2(33)SB, the output of the show policy-map command is slightly different from previous releases when the policy is a hierarchical policy.

For example, in Cisco IOS Release 12.2(33)SB output similar to the following displays when you specify a hierarchical policy in the show policy-map command:

```
Router# show policy-map Bronze
policy-map bronze
 class class-default
 shape average 34386000
 service-policy Child
```

In Cisco IOS Release 12.2(31)SB, output similar to the following displays when you specify a hierarchical policy in the show policy-map command:

```
Router# show policy-map Gold
policy-map Gold
 Class class-default
 Average Rate Traffic Shaping
 cir 34386000 (bps)
 service-policy Child2
```

In Cisco IOS Release 12.2(33)SB, the output from the show policy-map command displays police actions on separate lines as shown in the following sample output:

```
Router# show policy-map Premium
Policy Map Premium
 Class P1
 priority
 police percent 50 25 ms 0 ms
 conform-action transmit
 exceed-action transmit
 violate-action drop
```

In Cisco IOS Release 12.2(31)SB, the output from the show policy-map command displays police actions on one line as shown in the following sample output:

```
Router# show policy-map Premium
Policy Map Premium
 Class P2
 priority
 police percent 50 25 ms 0 ms conform-action transmit exceed-action transmit violate- action
 drop
```

## Examples

This section provides sample output from typical **showpolicy-map**commands. Depending upon the interface or platform in use and the options enabled (for example, Weighted Fair Queueing [WFQ]), the output you see may vary slightly from the ones shown below.

**Weighted Fair Queueing: Example**

The following example displays the contents of the service policy map called po1. In this example, WFQ is enabled.

```
Router# show policy-map po1
Policy Map po1
 Weighted Fair Queueing
    Class class1
       Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class2
```

```
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class3
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class4
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class5
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class6
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class7
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class8
         Bandwidth 937 (kbps)  Max thresh 64 (packets)
```

The following example displays the contents of all policy maps on the router. Again, WFQ is enabled.

```
Router# show policy-map

Policy Map poH1
 Weighted Fair Queueing
    Class class1
       Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class2
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class3
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class4
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class5
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class6
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class7
Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class8
         Bandwidth 937 (kbps)  Max thresh 64 (packets)
Policy Map policy2
 Weighted Fair Queueing
    Class class1
       Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class2
        Bandwidth 300  (kbps)  Max thresh 64 (packets)
    Class class3
        Bandwidth 300 (kbps)  Max thresh 64 (packets)
    Class class4
        Bandwidth 300 (kbps)  Max thresh 64 (packets)
    Class class5
        Bandwidth 300 (kbps)  Max thresh 64 (packets)
    Class class6
        Bandwidth 300 (kbps)  Max thresh 64 (packets)
```

The table below describes the significant fields shown in the display.

***Table 198: show policy-map Field Descriptions--Configured for WFQ***

| Field | Description |
|---|---|
| Policy Map | Policy map name. |
| Class | Class name. |
| Bandwidth | Amount of bandwidth in kbps allocated to class. |
| Max thresh | Maximum threshold in number of packets. |

### Frame Relay Voice-Adaptive Traffic-Shaping: Example

The following sample output for the **show-policymap** command indicates that Frame Relay voice-adaptive traffic-shaping is configured in the class-default class in the policy map MQC-SHAPE-LLQ1 and that the deactivation timer is set to 30 seconds.

```
Router# show policy-map
  Policy Map VSD1
    Class VOICE1
      Strict Priority
      Bandwidth 10 (kbps) Burst 250 (Bytes)
    Class SIGNALS1
      Bandwidth 8 (kbps) Max Threshold 64 (packets)
    Class DATA1
      Bandwidth 15 (kbps) Max Threshold 64 (packets)
  Policy Map MQC-SHAPE-LLQ1
    Class class-default
      Traffic Shaping
         Average Rate Traffic Shaping
                 CIR 63000 (bps) Max. Buffers Limit 1000 (Packets)
                 Adapt to 8000 (bps)
                 Voice Adapt Deactivation Timer 30 Sec
      service-policy VSD1
```

**Note** In Cisco IOS Release 12.4(20)T, if an interface configured with a policy map is full of heavy traffic, the implicit policer allows the traffic as defined in the bandwidth statement of each traffic class.

The table below describes the significant fields shown in the display.

***Table 199: show policy-map Field Descriptions--Configured for Frame Relay Voice-Adaptive Traffic-Shaping***

| Field | Description |
|---|---|
| Strict Priority | Indicates the queueing priority assigned to the traffic in this class. |
| Burst | Specifies the traffic burst size in bytes. |
| Traffic Shaping | Indicates that Traffic Shaping is enabled. |
| Average Rate Traffic Shaping | Indicates the type of Traffic Shaping enabled. Choices are Peak Rate Traffic Shaping or Average Rate Traffic Shaping. |
| CIR | Committed Information Rate (CIR) in bps. |
| Max. Buffers Limit | Maximum memory buffer size in packets. |
| Adapt to | Traffic rate when shaping is active. |
| Voice Adapt Deactivation Timer | Indicates that Frame Relay voice-adaptive traffic-shaping is configured, and that the deactivation timer is set to 30 seconds. |
| service-policy | Name of the service policy configured in the policy map “MQC-SHAPE-LLQ1”. |

### Traffic Policing: Example

The following is sample output from the **showpolicy-map** command. This sample output displays the contents of a policy map called policy1. In policy 1, traffic policing on the basis of a committed information rate (CIR) of 20 percent has been configured, and the bc and be have been specified in milliseconds. As part of the traffic policing configuration, optional conform, exceed, and violate actions have been specified.

```
Router# show policy-map policy1
  Policy Map policy1
    Class class1
     police cir percent 20 bc 300 ms pir percent 40 be 400 ms
       conform-action transmit
       exceed-action drop
       violate-action drop
```

The table below describes the significant fields shown in the display.

***Table 200: show policy-map Field Descriptions--Configured for Traffic Policing***

| Field | Description |
|---|---|
| Policy Map | Name of policy map displayed. |
| Class | Name of the class configured in the policy map displayed. |
| police | Indicates that traffic policing on the basis of specified percentage of bandwidth has been enabled. The committed burst (Bc) and excess burst (Be) sizes have been specified in milliseconds (ms), and optional conform, exceed, and violate actions have been specified. |

### Two-Rate Traffic Policing: Example

The following is sample output from the **showpolicy-map** command when two-rate traffic policing has been configured. As shown below, two-rate traffic policing has been configured for a class called police. In turn, the class called police has been configured in a policy map called policy1. Two-rate traffic policing has been configured to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps.

```
Router(config)# class-map police
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class police
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Router(config-pmap-c)# interface serial3/0
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial3/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
The following sample output shows the contents of the policy map called policy1 :
Router# show policy-map policy1

 Policy Map policy1
  Class police
   police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action
   transmit exceed-action set-prec-transmit 2 violate-action drop
```

Traffic marked as conforming to the average committed rate (500 kbps) will be sent as is. Traffic marked as exceeding 500 kbps, but not exceeding 1 Mbps, will be marked with IP Precedence 2 and then sent. All traffic exceeding 1 Mbps will be dropped. The burst parameters are set to 10000 bytes.

The table below describes the significant fields shown in the display.

***Table 201: show policy-map Field Descriptions--Configured for Two-Rate Traffic Policing***

| Field | Description |
|---|---|
| police | Indicates that the **police** command has been configured to enable traffic policing. Also, displays the specified CIR, conform burst size (bc), peak information rate (PIR), and peak burst (BE) size used for marking packets. |
| conform-action | Displays the action to be taken on packets conforming to a specified rate. |
| exceed-action | Displays the action to be taken on packets exceeding a specified rate. |
| violate-action | Displays the action to be taken on packets violating a specified rate. |

### Multiple Traffic Policing Actions: Example

The following is sample output from the **showpolicy-map** command when the Policer Enhancement--Multiple Actions feature has been configured. The following sample output from the **showpolicy-map**command displays the configuration for a service policy called police. In this service policy, traffic policing has been configured to allow multiple actions for packets marked as conforming to, exceeding, or violating the CIR or the PIR shown in the example.

```
Router# show policy-map police
  Policy Map police
    Class class-default
     police cir 1000000 bc 31250 pir 2000000 be 31250
       conform-action transmit
       exceed-action set-prec-transmit 4
       exceed-action set-frde-transmit
       violate-action set-prec-transmit 2
       violate-action set-frde-transmit
```

Packets conforming to the specified CIR (1000000 bps) are marked as conforming packets. These are transmitted unaltered.

Packets exceeding the specified CIR (but not the specified PIR, 2000000 bps) are marked as exceeding packets. For these packets, the IP Precedence level is set to 4, the discard eligibility (DE) bit is set to 1, and the packet is transmitted.

Packets exceeding the specified PIR are marked as violating packets. For these packets, the IP Precedence level is set to 2, the DE bit is set to 1, and the packet is transmitted.

**Note** Actions are specified by using the *action* argument of the **police** command. For more information about the available actions, see the **police** command reference page.

The table below describes the significant fields shown in the display.

***Table 202: show policy-map Field Descriptions--Configured for Multiple Traffic Policing Actions***

| Field | Description |
|---|---|
| police | Indicates that the **police** command has been configured to enable traffic policing. Also, displays the specified CIR, BC, PIR, and BE used for marking packets. |
| conform-action | Displays the one or more actions to be taken on packets conforming to a specified rate. |
| exceed-action | Displays the one or more actions to be taken on packets exceeding a specified rate. |
| violate-action | Displays the one or more actions to be taken on packets violating a specified rate. |

### Explicit Congestion Notification: Example

The following is sample output from the **showpolicy-map** command when the WRED--Explicit Congestion Notification (ECN) feature has been configured. The words “explicit congestion notification” (along with the ECN marking information) included in the output indicate that ECN has been enabled.

```
Router# show policy-map
   Policy Map pol1
     Class class-default
       Weighted Fair Queueing
             Bandwidth 70 (%)
             exponential weight 9
             explicit congestion notification
             class    min-threshold    max-threshold    mark-probability
             ------------------------------------------------------------
             ------------------------------------------------------------

             0        -                -                1/10
             1        -                -                1/10
             2        -                -                1/10
             3        -                -                1/10
             4        -                -                1/10
             5        -                -                1/10
             6        -                -                1/10
             7        -                -                1/10
             rsvp     -                -                1/10
```

The table below describes the significant fields shown in the display.

*Table 203: show policy-map Field Descriptions--Configured for ECN*

| Field | Description |
|---|---|
| explicit congestion notification | Indication that Explicit Congestion Notification is enabled. |
| class | IP precedence value. |
| min-threshold | Minimum threshold. Minimum WRED threshold in number of packets. |
| max-threshold | Maximum threshold. Maximum WRED threshold in number of packets. |
| mark-probability | Fraction of packets dropped when the average queue depth is at the maximum threshold. |

### Modular QoS CLI (MQC) Unconditional Packet Discard: Example

The following example displays the contents of the policy map called policy1. All the packets belonging to the class called c1 are discarded.

```
Router# show policy-map
 policy1
 Policy Map policy1
  Class c1
   drop
```

The table below describes the significant fields shown in the display.

*Table 204: show policy-map Field Descriptions--Configured for MQC Unconditional Packet Discard*

| Field | Description |
|---|---|
| Policy Map | Name of the policy map being displayed. |
| Class | Name of the class in the policy map being displayed. |
| drop | Indicates that the packet discarding action for all the packets belonging to the specified class has been configured. |

### Percentage-Based Policing and Shaping: Example

The following example displays the contents of two service policy maps--one called policy1 and one called policy2. In policy1, traffic policing based on a CIR of 50 percent has been configured. In policy 2, traffic shaping based on an average rate of 35 percent has been configured.

```
Router# show policy-map policy1
Policy Map policy1
 class class1
    police cir percent 50
```

```
Router# show policy-map policy2
Policy Map policy2
 class class2
    shape average percent 35
```

The following example displays the contents of the service policy map called po1 :

```
Router# show policy-map po1
Policy Map po1
 Weighted Fair Queueing
    Class class1
Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class2
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class3
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class4
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
```

The following example displays the contents of all policy maps on the router:

```
Router# show policy-map

Policy Map poH1
 Weighted Fair Queueing
    Class class1
       Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class2
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class3
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
    Class class4
        Bandwidth 937 (kbps)  Max thresh 64 (packets)
Policy Map policy2
 Weighted Fair Queueing
    Class class1
       Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class2
        Bandwidth 300  (kbps)  Max thresh 64 (packets)
    Class class3
        Bandwidth 300 (kbps)  Max thresh 64 (packets)
    Class class4
        Bandwidth 300 (kbps)  Max thresh 64 (packets)
```

The table below describes the significant fields shown in the display.

***Table 205: show policy-map Field Descriptions--Configured for Percentage-Based Policing and Shaping***

| Field | Description |
|---|---|
| Policy Map | Name of policy map displayed. |
| Weighted Fair Queueing | Indicates that weighted fair queueing (WFQ) has been enabled. |
| Class | Name of class configured in policy map displayed. |
| Bandwidth | Bandwidth, in kbps, configured for this class. |
| Max threshold | Maximum threshold. Maximum WRED threshold in number of packets. |

### Enhanced Packet Marking: Example

The following sample output from the **showpolicy-map**command displays the configuration for policy maps called policy1 and policy2.

In policy1 , a table map called table-map-cos1 has been configured to determine the precedence based on the class of service (CoS) value. Policy map policy 1 converts and propagates the packet markings defined in the table map called table-map-cos1.

The following sample output from the **showpolicy-map**command displays the configuration for service polices called policy1 and policy2 . In policy1 , a table map called table-map1 has been configured to determine the precedence according to the CoS value. In policy2 , a table map called table-map2 has been configured to determine the CoS value according to the precedence value.

```
Router# show policy-map policy1
  Policy Map policy1
    Class class-default
      set precedence cos table table-map1
Router# show policy-map policy2
   Policy Map policy2
    Class class-default
      set cos precedence table table-map2
```

The table below describes the fields shown in the display.

***Table 206: show policy-map Field Descriptions--Configured for Enhanced Packet Marking***

| Field | Description |
|---|---|
| Policy Map | Name of the policy map being displayed. |
| Class | Name of the class in the policy map being displayed. |
| set precedence cos table table-map1<br>or<br>set cos precedence table table-map2 | Name of the set command used to set the specified value.<br>For instance, set precedence cos table-map1 indicates that a table map called table-map1 has been configured to set the precedence value on the basis of the values defined in the table map.<br>Alternately, set cos table table-map2 indicates that a table map called table-map2 has been configured to set the CoS value on the basis of the values defined in the table map. |

### Bandwidth-Remaining Ratio: Example

The following sample output for the show policy-map command indicates that the class-default class of the policy map named vlan10_policy has a bandwidth-remaining ratio of 10. When congestion occurs, the scheduler allocates class-default traffic 10 times the unused bandwidth allocated in relation to other subinterfaces.

```
Router# show policy-map vlan10_policy
  Policy Map vlan10_policy
    Class class-default
      Average Rate Traffic Shaping
      cir 1000000 (bps)
      bandwidth remaining ratio 10
      service-policy child_policy
```

The table below describes the fields shown in the display.

*Table 207: show policy-map Field Descriptions--Configured for Bandwidth-Remaining Ratio*

| Field | Description |
|---|---|
| Policy Map | Name of the policy map being displayed. |
| Class | Name of the class in the policy map being displayed. |
| Average Rate Traffic Shaping | Indicates that Average Rate Traffic Shaping is configured. |
| cir | Committed information rate (CIR) used to shape traffic. |
| bandwidth remaining ratio | Indicates the ratio used to allocate excess bandwidth. |

### ATM Overhead Accounting: Example

The following sample output for the show policy-map command indicates that ATM overhead accounting is enabled for the class-default class. The BRAS-DSLAM encapsulation is dot1q and the subscriber encapsulation is snap-rbe for the AAL5 service.

```
Policy Map unit-test
Class class-default
Average Rate Traffic Shaping
cir 10% account dot1q aal5 snap-rbe
```

The table below describes the significant fields shown in the display.

*Table 208: show policy-map Field Descriptions--Configured for ATM Overhead Accounting*

| Field | Description |
|---|---|
| Average Rate | Committed burst (Bc) is the maximum number of bits sent out in each interval. |
| cir 10% | Committed information rate (CIR) is 10 percent of the available interface bandwidth. |
| dot1q | BRAS-DSLAM encapsulation is 802.1Q VLAN. |
| aal5 | DSLAM-CPE encapsulation type is based on the ATM Adaptation Layer 5 service. AAL5 supports connection-oriented variable bit rate (VBR) services. |
| snap-rbe | Subscriber encapsulation type. |

### Tunnel-Marking: Example

In this sample output of the**showpolicy-map** command, the character string “ip precedence tunnel 4” indicates that tunnel marking (either L2TPv3 or GRE) has been configured to set the IP precedence value to 4 in the header of a tunneled packet.

**Note** In Cisco IOS Release 12.4(15)T2, GRE-tunnel marking is supported on the RPM-XF platform *only* .

```
Router# show policy-map
Policy Map TUNNEL_MARKING
    Class MATCH_FRDE
      set ip precedence tunnel 4
```

The table below describes the fields shown in the display.

***Table 209: show policy-map Field Descriptions--Configured for Tunnel Marking***

| Field | Description |
|---|---|
| Policy Map | Name of the policy map being displayed. |
| Class | Name of the class in the policy map being displayed. |
| set ip precedence tunnel | Indicates that tunnel marking has been configured. |

**HQF: Example 1**

The following sample output from the **showpolicy-map**command displays the configuration for a policy map called test1:

```
Router# show policy-map test1
  Policy Map test1
    Class class-default
      Average Rate Traffic Shaping
      cir 1536000 (bps)
      service-policy test2
```

The table below describes the fields shown in the display.

***Table 210: show policy-map Field Descriptions--Configured for HQF***

| Field | Description |
|---|---|
| Policy Map | Name of the policy map being displayed. |
| Class | Name of the class in the policy map being displayed. |
| Average Rate Traffic Shaping | Indicates that Average Rate Traffic Shaping is configured. |
| cir | Committed information rate (CIR) in bps. |
| service-policy | Name of the service policy configured in policy map “test1”. |

**HQF: Example 2**

The following sample output from the **showpolicy-map**command displays the configuration for a policy map called test2:

```
Router# show policy-map test2
  Policy Map test2
    Class RT
      priority 20 (%)
    Class BH
      bandwidth 40 (%)
      queue-limit 128 packets
    Class BL
      bandwidth 35 (%)
       packet-based wred, exponential weight 9

      dscp    min-threshold    max-threshold    mark-probablity
      ----------------------------------------------------------
      af21 (18)     100              400              1/10
      default (0)   -                -                1/10
```

The table below describes the fields shown in the display.

***Table 211: show policy-map Field Descriptions--Configured for HQF***

| Field | Description |
|---|---|
| Policy Map | Name of the policy map being displayed. |
| Class | Name of the class in the policy map being displayed. |
| Average Rate Traffic Shaping | Indicates that Average Rate Traffic Shaping is configured. |
| priority | Indicates the queueing priority percentage assigned to traffic in this class. |
| bandwidth | Indicates the bandwidth percentage allocated to traffic in this class. |
| queue-limit | Indicates the queue limit in packets for this traffic class. |
| packet-based wred, exponential weight | Indicates that random detect is being applied and the units used are packets. Exponential weight is a factor for calculating the average queue size used with WRED. |

| Field | Description |
|---|---|
| dscp | Differentiated services code point (DSCP). Values can be the following:<br>• 0 to 63--Numerical DSCP values. The default value is 0.<br>• af1 to af43--Assured forwarding (AF) DSCP values.<br>• cs1 to cs7--Type of service (ToS) precedence values.<br>• default--Default DSCP value.<br>• ef--Expedited forwarding (EF) DSCP values. |
| min-threshold | Minimum threshold. Minimum WRED threshold in number of packets. |
| max-threshold | Maximum threshold. Maximum WRED threshold in number of packets. |
| mark-probability | Fraction of packets dropped when the average queue depth is at the maximum threshold. |

## Related Commands

| Command | Description |
|---|---|
| **bandwidth** | Specifies or modifies the bandwidth allocated for a class belonging to a policy map, and enables ATM overhead accounting. |
| **bandwidth remaining ratio** | Specifies a bandwidth-remaining ratio for class queues and subinterface-level queues to determine the amount of unused (excess) bandwidth to allocate to the queue during congestion. |
| **class (policy map)** | Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy. |
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **drop** | Configures a traffic class to discard packets belonging to a specific class. |
| **police** | Configures traffic policing. |

| Command | Description |
|---|---|
| **police (two rates)** | Configures traffic policing using two rates, the CIR and the PIR. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **random-detect ecn** | Enables ECN. |
| **shape** | Shapes traffic to the indicated bit rate according to the algorithm specified, and enables ATM overhead accounting. |
| **show policy-map class** | Displays the configuration for the specified class of the specified policy map. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |
| **show running-config** | Displays the current configuration of the router. If configured, the command output includes information about ATM overhead accounting. |
| **show table-map** | Displays the configuration of a specified table map or of all table maps. |
| **table-map (value mapping)** | Creates and configures a mapping table for mapping and converting one packet-marking value to another. |

# show policy-map class

To display the configuration for the specified class of the specified policy map, use the **showpolicy-mapclass**command inEXEC mode.

**show policy-map** *policy-map* **class** *class-name*

## Syntax Description

| | |
|---|---|
| *policy-map* | The name of a policy map that contains the class configuration to be displayed. |
| *class-name* | The name of the class whose configuration is to be displayed. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE. |
| 12.0(7)S | This command was integrated into Cisco IOS Release 12.0(7)S. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR 1000 series routers. |

## Usage Guidelines

You can use the **showpolicy-mapclass** command to display any single class configuration for any service policy map, whether or not the specified service policy map has been attached to an interface.

## Examples

The following example displays configurations for the class called class7 that belongs to the policy map called po1:

```
Router# show policy-map po1 class class7
```

```
Class class7
 Bandwidth 937 (kbps) Max Thresh 64 (packets)
```

## Related Commands

| Command | Description |
|---|---|
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

# show policy-map control-plane

To display the configuration and statistics for a traffic class or all traffic classes in the policy maps attached to the control plane for aggregate or distributed control plane services, use the **showpolicy-mapcontrol-plane** command in privileged EXEC mode.

### Cisco 3660, 3800, 7200, 7400, and 7500 Series Routers

**show policy-map control-plane** [**type policy-type**] [**all**| **slot** *slot-number*] [**host**| **transit**| **cef-exception**] [**input** [**class** *class-name*]| **output** [**class** *class-name*]]

### Cisco 7600 and ASR 1000 Series Routers

**show policy-map control-plane [all]** [**input** [**class** *class-name*]| **output** [**class** *class-name*]]

## Syntax Description

| | |
|---|---|
| **type** *policy-type* | (Optional) Specifies policy-map type for which you want statistics (for example, port-filter or queue-threshold). |
| **all** | (Optional) Displays all QoS control plane policies used in aggregate and distributed control plane (CP) services. |
| **slot** *slot-number* | (Optional) Displays information about the quality of service (QoS) policy used to perform distributed CP services on the specified line card. |
| **host** | (Optional) Displays policy-map and class-map statistics for the host subinterface. |
| **transit** | (Optional) Displays policy-map and class-map statistics for the transit subinterface. |
| **cef-exception** | (Optional) Displays policy-map and class-map statistics for the Cef-exception subinterface. |
| **input** | (Optional) Displays statistics for the attached input policy. |
| **output** | (Optional) Displays statistics for the attached output policy.<br>**Note** The output keyword is supported only in Cisco IOS Release 12.3(4)T and later Cisco IOS 12.3T releases. |
| **class** *class-name* | (Optional) Name of the class whose configuration and statistics are to be displayed. |

**Command Default** Information displays for all classes of the policy map of the control plane.

**Command Modes** Privileged EXEC (#)

**Command History**

| Release | Modification |
|---|---|
| 12.2(18)S | This command was introduced. |
| 12.3(4)T | This command was integrated into Cisco IOS Release 12.3(4)T, and support for the **output** keyword was added. |
| 12.0(29)S | This command was integrated into Cisco IOS Release 12.0(29)S. |
| 12.2(18)SXD1 | This command was integrated into Cisco IOS Release 12.2(18)SXD1. |
| 12.0(30)S | The**slot***slot-number*parameter was added to support distributed CP services. |
| 12.4(4)T | Support was added for the**type***policy-type*keyword and argument combination and for the **host**, **transit**, and **cef-exception** keywords. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| Cisco IOS XE Release 2.2 | This command was implemented on Cisco ASR 1000 series routers. |

**Usage Guidelines** The**showpolicy-mapcontrol-plane** command displays information for aggregate and distributed control-plane policing services that manage the number or rate of control-plane (CP) packets sent to the process level of the route processor.

Information for distributed control-plane service is displayed for a specified line card. Distributed CP services are performed on a line card's distributed switch engine and manage CP traffic sent from all interfaces on the line card to the route processor, where aggregate CP services (for CP packets received from all line cards on the router) are performed.

**Examples** The following example shows that the policy map TEST is associated with the control plane. This policy map polices traffic that matches the class map TEST, while allowing all other traffic (that matches the class map called "class-default") to go through as is.

```
Router# show policy-map control-plane

Control Plane
Service-policy input:TEST
Class-map:TEST (match-all)
      20 packets, 11280 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:access-group 101
      police:
        8000 bps, 1500 limit, 1500 extended limit
        conformed 15 packets, 6210 bytes; action:transmit
```

```
        exceeded 5 packets, 5070 bytes; action:drop
        violated 0 packets, 0 bytes; action:drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
Class-map:class-default (match-any)
      105325 packets, 11415151 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match:any
```

The table below describes the significant fields shown in the display.

***Table 212: show policy-map control-plane Field Descriptions***

| Field | Description |
|---|---|
| Fields Associated with Classes or Service Policies | |
| Service-policy input | Name of the input service policy that is applied to the control plane. (This field will also show the output service policy, if configured.) |
| Class-map | Class of traffic being displayed. Traffic is displayed for each configured class. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| offered rate | Rate, in kbps, at which packets are coming into the class. |
| drop rate | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate. |
| Match | Match criteria for the specified class of traffic.<br>For more information about the variety of match criteria options available, see the "Applying QoS Features Using the MQC" module in the *Cisco IOS Quality of Service Solutions Configuration Guide* . |
| Fields Associated with Traffic Policing | |
| police | Indicates that the **police** command has been configured to enable traffic policing. |
| conformed | Displays the action to be taken on packets that conform to a specified rate. Displays the number of packets and bytes on which the action was taken. |
| exceeded | Displays the action to be taken on packets that exceed a specified rate. Displays the number of packets and bytes on which the action was taken. |

| Field | Description |
|---|---|
| violated | Displays the action to be taken on packets that violate a specified rate. Displays the number of packets and bytes on which the action was taken. |

## Related Commands

| Command | Description |
|---|---|
| **control-plane** | Enters control-plane configuration mode to apply a QoS policy to police traffic destined for the control plane. |
| **service-policy (control-plane)** | Attaches a policy map to the control plane for aggregate or distributed control-plane services. |

# show policy-map interface

To display the statistics and the configurations of the input and output policies that are attached to an interface, use the **show policy-map interface** command in user EXEC or privileged EXEC mode.

### ATM Shared Port Adapters

**show policy-map interface** *slot*/*subslot*/*port* **.**[ *subinterface* ]

### Cisco CMTS Routers

**show policy-map interface** *interface-type slot/subslot/port*

### Cisco 3660, 3845, 7200, 7400, 7500, Cisco ASR 903 Series Routers, and Cisco ASR 1000 Series Routers

**show policy-map interface** *type type-parameter* [**vc** [ *vpi* ]**[/]***vci*] [**dlci** *dlci*] [**input**| **output**] [**class** *class-name*]

### Cisco 6500 Series Switches

**show policy-map interface** [*interface-type interface-number*| **vlan** *vlan-id*] **[detailed]** [{**input**| **output**} [**class** *class-name*]]

**show policy-map interface** [**port-channel** *channel-number* [**class** *class-name*]]

### Cisco 7600 Series Routers

**show policy-map interface** [*interface-type interface-number*| **null 0**| **vlan** *vlan-id*] [**input**| **output**]

## Syntax Description

| | |
|---|---|
| *slot* | (CMTS and ATM shared port adapter only) Chassis slot number. See the appropriate hardware manual for slot information. For SIPs, see the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide. |
| */subslot* | (CMTS and ATM shared port adapter only) Secondary slot number on an SPA interface processor (SIP) where a SPA is installed. See the platform-specific SPA hardware installation guide and the corresponding “Specifying the Interface Address on an SPA” topic in the platform-specific SPA software configuration guide for subslot information. |

| | |
|---|---|
| *port* | (CMTS and ATM shared port adapter only) Port or interface number. See the appropriate hardware manual for port information. For SPAs, see the corresponding "Specifying the Interface Address" topics in the platform-specific SPA software configuration guide. |
| **.***subinterface* | (ATM shared port adapter only—Optional) Subinterface number. The number that precedes the period must match the number to which this subinterface belongs. The range is 1 to 4,294,967,293. |
| *type* | Type of interface or subinterface whose policy configuration is to be displayed. |
| *type-parameter* | Port, connector, interface card number, class-map name or other parameter associated with the interface or subinterface type. |
| **vc** | (Optional) For ATM interfaces only, shows the policy configuration for a specified PVC. |
| *vpi* / | (Optional) ATM network virtual path identifier (VPI) for this permanent virtual circuit (PVC). On the Cisco 7200 and 7500 series routers, this value ranges from 0 to 255.<br>The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0.<br>The absence of both the forward slash (/) and a *vpi* value defaults the *vpi* value to 0. If this value is omitted, information for all virtual circuits (VCs) on the specified ATM interface or subinterface is displayed. |
| *vci* | (Optional) ATM network virtual channel identifier (VCI) for this PVC. This value ranges from 0 to 1 less than the maximum value set for this interface by the **atmvc-per-vp** command. Typically, the lower values 0 to 31 are reserved for specific traffic (F4 Operation, Administration, and Maintenance [OAM], switched virtual circuit [SVC] signaling, Integrated Local Management Interface [ILMI], and so on) and should not be used.<br>The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only.<br>The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0. |

| | |
|---|---|
| **dlci** | (Optional) Indicates a specific PVC for which policy configuration will be displayed. |
| *dlci* | (Optional) A specific data-link connection identifier (DLCI) number used on the interface. Policy configuration for the corresponding PVC will be displayed when a DLCI is specified. |
| **input** | (Optional) Indicates that the statistics for the attached input policy will be displayed. |
| **output** | (Optional) Indicates that the statistics for the attached output policy will be displayed. |
| **class** *class-name* | (Optional) Displays the QoS policy actions for the specified class. |
| *interface-type* | (Optional) Interface type; possible valid values are **atm**, **ethernet**, **fastethernet**, **ge-wan gigabitethernet**, **pos**, **pseudowire** and **tengigabitethernet**. |
| *interface-number* | (Optional) Module and port number; see the "Usage Guidelines" section for valid values. |
| **vlan** *vlan-id* | (Optional) Specifies the VLAN ID; valid values are from 1 to 4094. |
| **detailed** | (Optional) Displays additional statistics. |
| **port-channel** *channel-number* | (Optional) Displays the EtherChannel port-channel interface. |
| **null 0** | (Optional) Specifies the null interface; the only valid value is 0. |

## Command Default

This command displays the packet statistics of all classes that are configured for all service policies on the specified interface or subinterface or on a specific permanent virtual circuit (PVC) on the interface.

When used with the ATM shared port adapter, this command has no default behavior or values.

## Command Modes

Privileged EXEC (#)

**ATM Shared Port Adapter**
User EXEC (>)

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.0(5)T | This command was introduced. |
| 12.0(5)XE | This command was integrated into Cisco IOS Release 12.0(5)XE. |
| 12.0(7)S | This command was integrated into Cisco IOS Release 12.0(7)S. |
| 12.0(28)S | This command was modified for the QoS: Percentage-Based Policing feature to include milliseconds when calculating the committed (conform) burst (bc) and excess (peak) burst (be) sizes. |
| 12.1(1)E | This command was integrated into Cisco IOS Release 12.1(1)E. |
| 12.1(2)T | This command was modified to display information about the policy for all Frame Relay PVCs on the interface or, if a DLCI is specified, the policy for that specific PVC. This command was also modified to display the total number of packets marked by the quality of service (QoS) set action. |
| 12.1(3)T | This command was modified to display per-class accounting statistics. |
| 12.2(4)T | This command was modified for two-rate traffic policing and can display burst parameters and associated actions. |
| 12.2(8)T | This command was modified for the Policer Enhancement—Multiple Actions feature and the WRED—Explicit Congestion Notification (ECN) feature.<br>For the Policer Enhancement—Multiple Actions feature, the command was modified to display the multiple actions configured for packets conforming to, exceeding, or violating a specific rate.<br>For the WRED—Explicit Congestion Notification (ECN) feature, the command displays ECN marking information. |

| Release | Modification |
|---|---|
| 12.2(13)T | The following modifications were made:<br>• This command was modified for the Percentage-Based Policing and Shaping feature.<br>• This command was modified for the Class-Based RTP and TCP Header Compression feature.<br>• This command was modified as part of the Modular QoS CLI (MQC) Unconditional Packet Discard feature. Traffic classes in policy maps can now be configured to discard packets belonging to a specified class.<br>• This command was modified to display the Frame Relay DLCI number as a criterion for matching traffic inside a class map.<br>• This command was modified to display Layer 3 packet length as a criterion for matching traffic inside a class map.<br>• This command was modified for the Enhanced Packet Marking feature. A mapping table (table map) can now be used to convert and propagate packet-marking values. |
| 12.2(14)SX | This command was modified. Support for this command was introduced on Cisco 7600 series routers. |
| 12.2(15)T | This command was modified to display Frame Relay voice-adaptive traffic-shaping information. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.3(14)T | This command was modified to display bandwidth estimation parameters. |
| 12.2(18)SXE | This command was integrated into Cisco IOS Release 12.2(18)SXE. This command was modified to display aggregate WRED statistics for the ATM shared port adapter. Note that changes were made to the syntax, defaults, and command modes. These changes are labelled “ATM Shared Port Adapter.” |
| 12.4(4)T | This command was modified. The **typeaccess-control** keywords were added to support flexible packet matching. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB, and the following modifications were made:<br>• This command was modified to display either legacy (undistributed processing) QoS or hierarchical queueing framework (HQF) parameters on Frame Relay interfaces or PVCs.<br>• This command was modified to display information about Layer 2 Tunnel Protocol Version 3 (L2TPv3) tunnel marking. |

| Release | Modification |
|---|---|
| 12.2(31)SB2 | The following modifications were made:<br>• This command was enhanced to display statistical information for each level of priority service configured and information about bandwidth-remaining ratios, and this command was implemented on the Cisco 10000 series router for the PRE3.<br>• This command was modified to display statistics for matching packets on the basis of VLAN identification numbers. As of Cisco IOS Release 12.2(31)SB2, matching packets on the basis of VLAN identification numbers is supported on Cisco 10000 series routers only. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC. |
| 12.4(15)T2 | This command was modified to display information about Generic Routing Encapsulation (GRE) tunnel marking.<br>**Note** As of this release, GRE-tunnel marking is supported on the Cisco MGX Route Processor Module (RPM-XF) platform *only* . |
| 12.2(33)SB | This command was modified to display information about GRE-tunnel marking, and support for the Cisco 7300 series router was added. |
| Cisco IOS XE 2.1 | This command was integrated into Cisco IOS XE Release 2.1 and was implemented on the Cisco ASR 1000 series router. |
| 12.4(20)T | This command was modified. Support was added for hierarchical queueing framework (HQF) using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC). |
| 12.2(33)SXI | This command was implemented on the Catalyst 6500 series switch and modified to display the strict level in the priority feature and the counts per level. |
| 12.2(33)SRE | This command was modified to automatically round off the bc and be values, in the MQC police policy map, to the interface's MTU size. |
| Cisco IOS XE Release 2.6 | The command output was modified to display information about subscriber QoS statistics. |
| 12.2(54)SG | This command was modified to display only the applicable count of policer statistics. |
| 12.2(33)SCF | This command was integrated into Cisco IOS Release 12.2(33)SCF. |
| Cisco IOS XE Release 3.7S | This command was implemented on Cisco ASR 903 Series Routers. |
| Cisco IOS XE Release 3.8S | This command was modified. The *pseudowire* interface type was added. |

| Release | Modification |
|---|---|
| Cisco IOS XE Release 3.8S | This command was modified. The *pseudowire* interface type was added on Cisco 1000 Series Routers. |
| Cisco IOS Release 15.3(1)S | This command was modified. The *pseudowire* interface type was added. |

## Usage Guidelines

**Cisco 3660, 3845, 7200, 7400, 7500, Cisco ASR 903 Series Routers, and Cisco ASR 1000 Series Routers**

The **show policy-map interface** command displays the packet statistics for classes on the specified interface or the specified PVC only if a service policy has been attached to the interface or the PVC.

The counters displayed after the **show policy-map interface** command is entered are updated only if congestion is present on the interface.

The **show policy-map interface** command displays policy information about Frame Relay PVCs only if Frame Relay Traffic Shaping (FRTS) is enabled on the interface.

The **show policy-map interface** command displays ECN marking information only if ECN is enabled on the interface.

To determine if shaping is active with HQF, check the queue depth field of the "(queue depth/total drops/no-buffer drops)" line in the **show policy-map interface** command output.

In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and the bytes delayed counters were removed for traffic shaping classes.

**Cisco 7600 Series Routers and Catalyst 6500 Series Switches**

The pos, atm, and ge-wan interfaces are not supported on Cisco 7600 series routers or Catalyst 6500 series switches that are configured with a Supervisor Engine 720

Cisco 7600 series routers and Catalyst 6500 series switches that are configured with a Supervisor Engine 2 display packet counters.

Cisco 7600 series routers and Catalyst 6500 series switches that are configured with a Supervisor Engine 720 display byte counters.

The output does not display policed-counter information; 0 is displayed in its place (for example, 0 packets, 0 bytes). To display dropped and forwarded policed-counter information, enter the **show mls qos** command.

On the Cisco 7600 series router, for OSM WAN interfaces only, if you configure policing within a policy map, the hardware counters are displayed and the class-default counters are not displayed. If you do not configure policing within a policy map, the class-default counters are displayed.

On the Catalyst 6500 series switch, the **show policy-map interface** command displays the strict level in the priority feature and the counts per level.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

**HQF**

When you configure HQF, the **show policy-map interface** command displays additional fields that include the differentiated services code point (DSCP) value, WRED statistics in bytes, transmitted packets by WRED, and a counter that displays packets output/bytes output in each class.

## Examples

This section provides sample output from typical **show policy-map interface** commands. Depending upon the interface or platform in use and the options enabled, the output you see may vary slightly from the ones shown below.

## Examples

The following sample output of the **show policy-map interface** command displays the statistics for the serial 3/1 interface, to which a service policy called mypolicy (configured as shown below) is attached. Weighted fair queueing (WFQ) has been enabled on this interface. See the table below for an explanation of the significant fields that commonly appear in the command output.

```
policy-map mypolicy
 class voice
  priority 128
 class gold
  bandwidth 100
 class silver
  bandwidth 80
  random-detect
Router# show policy-map interface serial3/1 output

 Serial3/1
  Service-policy output: mypolicy
    Class-map: voice (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 5
      Weighted Fair Queueing
        Strict Priority
        Output Queue: Conversation 264
        Bandwidth 128 (kbps) Burst 3200 (Bytes)
        (pkts matched/bytes matched) 0/0
        (total drops/bytes drops) 0/0
    Class-map: gold (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 2
      Weighted Fair Queueing
        Output Queue: Conversation 265
        Bandwidth 100 (kbps) Max Threshold 64 (packets)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
    Class-map: silver (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 1
      Weighted Fair Queueing
        Output Queue: Conversation 266
        Bandwidth 80 (kbps)
        (pkts matched/bytes matched) 0/0
        (depth/total drops/no-buffer drops) 0/0/0
         exponential weight: 9
         mean queue depth: 0
class     Transmitted       Random drop      Tail drop    Minimum Maximum  Mark
          pkts/bytes        pkts/bytes       pkts/bytes    thresh  thresh  prob
0            0/0               0/0              0/0           20      40  1/10
1            0/0               0/0              0/0           22      40  1/10
2            0/0               0/0              0/0           24      40  1/10
3            0/0               0/0              0/0           26      40  1/10
4            0/0               0/0              0/0           28      40  1/10
5            0/0               0/0              0/0           30      40  1/10
6            0/0               0/0              0/0           32      40  1/10
7            0/0               0/0              0/0           34      40  1/10
```

```
rsvp          0/0               0/0              0/0           36      40  1/10
Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

## Examples

The following sample output from the **show policy-map interface** command displays the statistics for the serial 3/2 interface, to which a service policy called p1 (configured as shown below) is attached. Traffic shaping has been enabled on this interface. See the table below for an explanation of the significant fields that commonly appear in the command output.

**Note** In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```
policy-map p1
 class c1
  shape average 320000
Router# show policy-map interface serial3/2 output

 Serial3/2
  Service-policy output: p1
    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 0
      Traffic Shaping
        Target    Byte   Sustain   Excess    Interval  Increment Adapt
        Rate      Limit  bits/int  bits/int  (ms)      (bytes)   Active
        320000    2000   8000      8000      25        1000      -
        Queue     Packets   Bytes     Packets   Bytes     Shaping
        Depth                         Delayed   Delayed   Active
        0         0         0         0         0         no
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

The table below describes significant fields commonly shown in the displays. The fields in the table are grouped according to the relevant QoS feature. A number in parentheses may appear next to the service-policy output name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

***Table 213: show policy-map interface Field Descriptions***

| Field | Description |
|---|---|
| Fields Associated with Classes or Service Policies | |
| Service-policy output | Name of the output service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |

| Field | Description |
|---|---|
| packets and bytes | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in kbps, of packets coming in to the class.<br>**Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only. |
| drop rate | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate. |
| **Note** In distributed architecture platforms (such as the Cisco 7500 series platform), the value of the transfer rate, calculated as the difference between the offered rate and the drop rate counters, can sporadically deviate from the average by up to 20 percent or more. This can occur while no corresponding burst is registered by independent traffic analyser equipment. | |
| Match | Match criteria specified for the class of traffic. Choices include criteria such as IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental (EXP) value, access groups, and QoS groups. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide* . |
| Fields Associated with Queueing (if Enabled) | |

| Field | Description |
|---|---|
| Output Queue | The weighted fair queueing (WFQ) conversation to which this class of traffic is allocated. |
| Bandwidth | Bandwidth, in either kbps or percentage, configured for this class and the burst size. |
| pkts matched/bytes matched | Number of packets (also shown in bytes) matching this class that were placed in the queue. This number reflects the total number of matching packets queued at any time. Packets matching this class are queued only when congestion exists. If packets match the class but are never queued because the network was not congested, those packets are not included in this total. However, if process switching is in use, the number of packets is always incremented even if the network is not congested. |
| depth/total drops/no-buffer drops | Number of packets discarded for this class. No-buffer indicates that no memory buffer exists to service the packet. |
| Fields Associated with Weighted Random Early Detection (WRED) (if Enabled) | |
| exponential weight | Exponent used in the average queue size calculation for a WRED parameter group. |
| mean queue depth | Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a fluctuating average. The minimum and maximum thresholds are compared against this value to determine drop decisions. |
| class | IP precedence level. |
| Transmitted pkts/bytes | Number of packets (also shown in bytes) passed through WRED and not dropped by WRED.<br>**Note** If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as "no-buffer drops") are not taken into account by the WRED packet counter. |
| Random drop pkts/bytes | Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence level. |

| Field | Description |
|---|---|
| Tail drop pkts/bytes | Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence level. |
| Minimum thresh | Minimum threshold. Minimum WRED threshold in number of packets. |
| Maximum thresh | Maximum threshold. Maximum WRED threshold in number of packets. |
| Mark prob | Mark probability. Fraction of packets dropped when the average queue depth is at the maximum threshold. |
| Fields Associated with Traffic Shaping (if Enabled) | |
| Target Rate | Rate used for shaping traffic. |
| Byte Limit | Maximum number of bytes that can be transmitted per interval. Calculated as follows:<br>((Bc+Be) /8) x 1 |
| Sustain bits/int | Committed burst (Bc) rate. |
| Excess bits/int | Excess burst (Be) rate. |
| Interval (ms) | Time interval value in milliseconds (ms). |
| Increment (bytes) | Number of credits (in bytes) received in the token bucket of the traffic shaper during each time interval. |
| Queue Depth | Current queue depth of the traffic shaper. |
| Packets | Total number of packets that have entered the traffic shaper system. |
| Bytes | Total number of bytes that have entered the traffic shaper system. |
| Packets Delayed | Total number of packets delayed in the queue of the traffic shaper before being transmitted. |
| Bytes Delayed | Total number of bytes delayed in the queue of the traffic shaper before being transmitted. |
| Shaping Active | Indicates whether the traffic shaper is active. For example, if a traffic shaper is active, and the traffic being sent exceeds the traffic shaping rate, a “yes” appears in this field. |

## Examples

The following sample output of the **show policy-map interface** command displays the statistics for the ATM shared port adapter interface 4/1/0.10, to which a service policy called prec-aggr-wred (configured as shown below) is attached. Because aggregate WRED has been enabled on this interface, the classthrough Mark Prob statistics are aggregated by subclasses. See the table below for an explanation of the significant fields that commonly appear in the command output.

```
Router(config)# policy-map prec-aggr-wred
Router(config-pmap)# class class-default
Router(config-pmap-c)# random-detect aggregate
Router(config-pmap-c)# random-detect precedence values 0 1 2 3 minimum thresh 10
maximum-thresh 100 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 4 5 minimum-thresh 40 maximum-thresh
 400 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 6 minimum-thresh 60 maximum-thresh
600 mark-prob 10
Router(config-pmap-c)# random-detect precedence values 7 minimum-thresh 70 maximum-thresh
700 mark-prob 10
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface ATM4/1/0.10 point-to-point
Router(config-if)# ip address 10.0.0.2 255.255.255.0
Router(config-if)# pvc 10/110
Router(config-if)# service-policy output prec-aggr-wred

Router# show policy-map interface atm4/1/0.10

 ATM4/1/0.10: VC 10/110 -
  Service-policy output: prec-aggr-wred
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        Exp-weight-constant: 9 (1/512)
        Mean queue depth: 0
        class       Transmitted     Random drop      Tail drop     Minimum   Maximum  Mark
 pkts/bytes pkts/bytes pkts/bytes thresh thresh prob

        0  1  2  3       0/0              0/0             0/0           10      100  1/10
        4  5             0/0              0/0             0/0           40      400  1/10
        6                0/0              0/0             0/0           60      600  1/10
        7                0/0              0/0             0/0           70      700  1/10
```

## Examples

The following sample output of the **show policy-map interface** command displays the statistics for the ATM shared port adapter interface 4/1/0.11, to which a service policy called dscp-aggr-wred (configured as shown below) is attached. Because aggregate WRED has been enabled on this interface, the class through Mark Prob statistics are aggregated by subclasses. See the table below for an explanation of the significant fields that commonly appear in the command output.

```
Router(config)# policy-map dscp-aggr-wred
Router(config-pmap)# class class-default
Router(config-pmap-c)# random-detect dscp-based aggregate minimum-thresh 1 maximum-thresh
10 mark-prob 10
Router(config-pmap-c)# random-detect dscp values 0 1 2 3 4 5 6 7 minimum-thresh 10
maximum-thresh 20 mark-prob 10
Router(config-pmap-c)# random-detect dscp values 8 9 10 11 minimum-thresh 10 maximum-thresh
 40 mark-prob 10
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface ATM4/1/0.11 point-to-point
Router(config-subif)# ip address 10.0.0.2 255.255.255.0
```

```
Router(config-subif)# pvc 11/101
Router(config-subif)# service-policy output dscp-aggr-wred
Router# show policy-map interface atm4/1/0.11

 ATM4/1/0.11: VC 11/101 -
  Service-policy output: dscp-aggr-wred
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        Exp-weight-constant: 0 (1/1)
        Mean queue depth: 0
        class       Transmitted     Random drop      Tail drop     Minimum   Maximum  Mark
                  pkts/bytes pkts/bytes pkts/bytes thresh thresh prob
        default          0/0              0/0             0/0            1      10  1/10
        0  1  2  3
        4  5  6  7       0/0              0/0             0/0           10      20  1/10
        8  9  10 11      0/0              0/0             0/0           10      40  1/10
```

The table below describes the significant fields shown in the display when aggregate WRED is configured for an ATM shared port adapter.

***Table 214: show policy-map interface Field Descriptions—Configured for Aggregate WRED on ATM Shared Port Adapter***

| Field | Description |
|---|---|
| exponential weight | Exponent used in the average queue size calculation for a Weighted Random Early Detection (WRED) parameter group. |
| mean queue depth | Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a fluctuating average. The minimum and maximum thresholds are compared against this value to determine drop decisions. |
| **Note** When Aggregate Weighted Random Early Detection (WRED) is enabled, the following WRED statistics will be aggregated based on their subclass (either their IP precedence or differentiated services code point (DSCP) value). | |
| class | IP precedence level or differentiated services code point (DSCP) value. |
| Transmitted pkts/bytes | Number of packets (also shown in bytes) passed through WRED and not dropped by WRED.<br>**Note** If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as "no-buffer drops") are not taken into account by the WRED packet counter. |

| Field | Description |
|---|---|
| Random drop pkts/bytes | Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence level or DSCP value. |
| Tail drop pkts/bytes | Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence level or DSCP value. |
| Minimum thresh | Minimum threshold. Minimum WRED threshold in number of packets. |
| Maximum thresh | Maximum threshold. Maximum WRED threshold in number of packets. |
| Mark prob | Mark probability. Fraction of packets dropped when the average queue depth is at the maximum threshold. |

## Examples

The following sample output shows that Frame Relay voice-adaptive traffic shaping is currently active and has 29 seconds left on the deactivation timer. With traffic shaping active and the deactivation time set, this means that the current sending rate on DLCI 201 is minCIR, but if no voice packets are detected for 29 seconds, the sending rate will increase to CIR.

**Note** In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```
Router# show policy interface Serial3/1.1

 Serial3/1.1:DLCI 201 -
  Service-policy output:MQC-SHAPE-LLQ1

    Class-map:class-default (match-any)
      1434 packets, 148751 bytes
      30 second offered rate 14000 bps, drop rate 0 bps
      Match:any
      Traffic Shaping
           Target/Average   Byte   Sustain   Excess    Interval  Increment
             Rate           Limit  bits/int  bits/int  (ms)      (bytes)
            63000/63000     1890   7560      7560      120       945

        Adapt  Queue     Packets   Bytes     Packets   Bytes     Shaping
        Active Depth                         Delayed   Delayed   Active
        BECN   0         1434      162991    26        2704      yes
        Voice Adaptive Shaping active, time left 29 secs
```

The table below describes the significant fields shown in the display. Significant fields that are not described in the table below are described in the table above (for “show policy-map interface Field Descriptions”).

*Table 215: show policy-map interface Field Descriptions—Configured for Frame Relay Voice-Adaptive Traffic Shaping*

| Field | Description |
|---|---|
| Voice Adaptive Shaping active/inactive | Indicates whether Frame Relay voice-adaptive traffic shaping is active or inactive. |
| time left | Number of seconds left on the Frame Relay voice-adaptive traffic shaping deactivation timer. |

## Examples

The following is sample output from the **show policy-map interface** command when two-rate traffic policing has been configured. In the example below, 1.25 Mbps of traffic is sent ("offered") to a policer class.

```
Router# show policy-map interface serial3/0


 Serial3/0
  Service-policy output: policy1
   Class-map: police (match all)
    148803 packets, 36605538 bytes
    30 second offered rate 1249000 bps, drop rate 249000 bps
    Match: access-group 101
    police:
     cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
     conformed 59538 packets, 14646348 bytes; action: transmit
     exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
     violated 29731 packets, 7313826 bytes; action: drop
     conformed 499000 bps, exceed 500000 bps violate 249000 bps
   Class-map: class-default (match-any)
    19 packets, 1990 bytes
    30 seconds offered rate 0 bps, drop rate 0 bps
    Match: any
```

The two-rate traffic policer marks 500 kbps of traffic as conforming, 500 kbps of traffic as exceeding, and 250 kbps of traffic as violating the specified rate. Packets marked as conforming will be sent as is, and packets marked as exceeding will be marked with IP Precedence 2 and then sent. Packets marked as violating the specified rate are dropped.

The table below describes the significant fields shown in the display.

*Table 216: show policy-map interface Field Descriptions—Configured for Two-Rate Traffic Policing*

| Field | Description |
|---|---|
| police | Indicates that the **police** command has been configured to enable traffic policing. Also, displays the specified CIR, conform burst size, peak information rate (PIR), and peak burst size used for marking packets. |
| conformed | Displays the action to be taken on packets conforming to a specified rate. Displays the number of packets and bytes on which the action was taken. |

| Field | Description |
|---|---|
| exceeded | Displays the action to be taken on packets exceeding a specified rate. Displays the number of packets and bytes on which the action was taken. |
| violated | Displays the action to be taken on packets violating a specified rate. Displays the number of packets and bytes on which the action was taken. |

## Examples

The following is sample output from the **show policy-map** command when the Policer Enhancement—Multiple Actions feature has been configured. The sample output from the **show policy-map interface** command displays the statistics for the serial 3/2 interface, to which a service policy called "police" (configured as shown below) is attached.

```
policy-map police
 class class-default
  police cir 1000000 pir 2000000
   conform-action transmit
   exceed-action set-prec-transmit 4
   exceed-action set-frde-transmit
   violate-action set-prec-transmit 2
   violate-action set-frde-transmit

Router# show policy-map interface serial3/2

Serial3/2: DLCI 100 -
Service-policy output: police
    Class-map: class-default (match-any)
      172984 packets, 42553700 bytes
      5 minute offered rate 960000 bps, drop rate 277000 bps
      Match: any
     police:
         cir 1000000 bps, bc 31250 bytes, pir 2000000 bps, be 31250 bytes
       conformed 59679 packets, 14680670 bytes; actions:
         transmit
exceeded 59549 packets, 14649054 bytes; actions:
         set-prec-transmit 4
         set-frde-transmit
       violated 53758 packets, 13224468 bytes; actions:
         set-prec-transmit 2
         set-frde-transmit
       conformed 340000 bps, exceed 341000 bps, violate 314000 bps
```

The sample output from **show policy-map interface** command shows the following:

- 59679 packets were marked as conforming packets (that is, packets conforming to the CIR) and were transmitted unaltered.
- 59549 packets were marked as exceeding packets (that is, packets exceeding the CIR but not exceeding the PIR). Therefore, the IP Precedence value of these packets was changed to an IP Precedence level of 4, the discard eligibility (DE) bit was set to 1, and the packets were transmitted with these changes.
- 53758 packets were marked as violating packets (that is, exceeding the PIR). Therefore, the IP Precedence value of these packets was changed to an IP Precedence level of 2, the DE bit was set to 1, and the packets were transmitted with these changes.

**Note** Actions are specified by using the *action* argument of the **police** command. For more information about the available actions, see the **police** command reference page.

The table below describes the significant fields shown in the display.

***Table 217: show policy-map interface Field Descriptions—Configured for Multiple Traffic Policing Actions***

| Field | Description |
|---|---|
| police | Indicates that the **police** command has been configured to enable traffic policing. Also, displays the specified CIR, conform burst size (BC), PIR, and peak burst size (BE) used for marking packets. |
| conformed, packets, bytes, actions | Displays the number of packets (also shown in bytes) marked as conforming to a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately. |
| exceeded, packets, bytes, actions | Displays the number of packets (also shown in bytes) marked as exceeding a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately. |
| violated, packets, bytes, actions | Displays the number of packets (also shown in bytes) marked as violating a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately. |

## Examples

The following is sample output from the **show policy-map interface** command when the WRED — Explicit Congestion Notification (ECN) feature has been configured. The words “explicit congestion notification” included in the output indicate that ECN has been enabled.

```
Router# show policy-map interface Serial4/1

 Serial4/1
  Service-policy output:policy_ecn
        Class-map:prec1 (match-all)
          1000 packets, 125000 bytes
          30 second offered rate 14000 bps, drop rate 5000 bps
          Match:ip precedence 1
          Weighted Fair Queueing
            Output Queue:Conversation 42
            Bandwidth 20 (%)
            Bandwidth 100 (kbps)
             (pkts matched/bytes matched) 989/123625
        (depth/total drops/no-buffer drops) 0/455/0
             exponential weight:9
             explicit congestion notification
             mean queue depth:0
     class   Transmitted  Random drop  Tail drop   Minimum     Maximum     Mark
             pkts/bytes   pkts/bytes    pkts/bytes threshold   threshold   probability
       0       0/0          0/0          0/0          20          40        1/10
```

```
  1      545/68125       0/0           0/0           22            40          1/10
  2        0/0           0/0           0/0           24            40          1/10
  3        0/0           0/0           0/0           26            40          1/10
  4        0/0           0/0           0/0           28            40          1/10
  5        0/0           0/0           0/0           30            40          1/10
  6        0/0           0/0           0/0           32            40          1/10
  7        0/0           0/0           0/0           34            40          1/10
rsvp       0/0           0/0           0/0           36            40          1/10
class    ECN Mark
       pkts/bytes
  0      0/0
  1     43/5375
  2      0/0
  3      0/0
  4      0/0
  5      0/0
  6      0/0
  7      0/0
rsvp     0/0
```

The table below describes the significant fields shown in the display.

***Table 218: show policy-map interface Field Descriptions—Configured for ECN***

| Field | Description |
|---|---|
| explicit congestion notification | Indication that Explicit Congestion Notification is enabled. |
| mean queue depth | Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a moving average. The minimum and maximum thresholds are compared against this value to determine drop decisions. |
| class | IP precedence value. |
| Transmitted pkts/bytes | Number of packets (also shown in bytes) passed through WRED and not dropped by WRED.<br>**Note** If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as "no-buffer drops") are not taken into account by the WRED packet counter. |
| Random drop pkts/bytes | Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence value. |
| Tail drop pkts/bytes | Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence value. |
| Minimum threshold | Minimum WRED threshold in number of packets. |

| Field | Description |
|---|---|
| Maximum threshold | Maximum WRED threshold in number of packets. |
| Mark probability | Fraction of packets dropped when the average queue depth is at the maximum threshold. |
| ECN Mark pkts/bytes | Number of packets (also shown in bytes) marked by ECN. |

## Examples

The following sample output from the **show policy-map interface** command shows the RTP header compression has been configured for a class called “prec2” in the policy map called “p1”.

The **show policy-map interface** command output displays the type of header compression configured (RTP), the interface to which the policy map called “p1” is attached (Serial 4/1), the total number of packets, the number of packets compressed, the number of packets saved, the number of packets sent, and the rate at which the packets were compressed (in bits per second (bps)).

In this example, User Datagram Protocol (UDP)/RTP header compressions have been configured, and the compression statistics are included at the end of the display.

```
Router# show policy-map interface Serial4/1

Serial4/1
Service-policy output:p1
    Class-map:class-default (match-any)
      1005 packets, 64320 bytes
      30 second offered rate 16000 bps, drop rate 0 bps
      Match:any
compress:
          header ip rtp
          UDP/RTP Compression:
          Sent:1000 total, 999 compressed,
                41957 bytes saved, 17983 bytes sent
                3.33 efficiency improvement factor
                99% hit ratio, five minute miss rate 0 misses/sec, 0 max
                 rate 5000 bps
```

The table below describes the significant fields shown in the display.

***Table 219: show policy-map interface Field Descriptions—Configured for Class-Based RTP and TCP Header Compression***

| Field | Description |
|---|---|
| Service-policy output | Name of the output service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets, bytes | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |

| Field | Description |
|---|---|
| offered rate | Rate, in kbps, of packets coming in to the class.<br>**Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only. |
| UDP/RTP Compression | Indicates that RTP header compression has been configured for the class. |
| Sent total | Count of every packet sent, both compressed packets and full-header packets. |
| Sent compressed | Count of number of compressed packets sent. |
| bytes saved | Total number of bytes saved (that is, bytes not needing to be sent). |
| bytes sent | Total number of bytes sent for both compressed and full-header packets. |
| efficiency improvement factor | The percentage of increased bandwidth efficiency as a result of header compression. For example, with RTP streams, the efficiency improvement factor can be as much as 2.9 (or 290 percent). |
| hit ratio | Used mainly for troubleshooting purposes, this is the percentage of packets found in the context database. In most instances, this percentage should be high. |
| five minute miss rate | The number of new traffic flows found in the last five minutes. |
| misses/sec max | The average number of new traffic flows found per second, and the highest rate of new traffic flows to date. |

| Field | Description |
|---|---|
| rate | The actual traffic rate (in bits per second) after the packets are compressed. |

**Note** A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

## Examples

The following sample output from the **show policy-map interface** command displays the statistics for the Serial2/0 interface, to which a policy map called "policy1" is attached. The discarding action has been specified for all the packets belonging to a class called "c1." In this example, 32000 bps of traffic is sent ("offered") to the class and all of them are dropped. Therefore, the drop rate shows 32000 bps.

```
Router# show policy-map interface

 Serial2/0
 Serial2/0
  Service-policy output: policy1
    Class-map: c1 (match-all)
       10184 packets, 1056436 bytes
       5 minute offered rate 32000 bps, drop rate 32000 bps
       Match: ip precedence 0
       drop
```

The table below describes the significant fields shown in the display.

***Table 220: show policy-map interface Field Descriptions—Configured for MQC Unconditional Packet Discard***

| Field | Description |
|---|---|
| Service-policy output | Name of the output service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets, bytes | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |

| Field | Description |
|---|---|
| offered rate | Rate, in kbps, of packets coming in to the class.<br>**Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only. |
| drop rate | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate. |
| **Note** In distributed architecture platforms (such as the Cisco 7500), the value of the transfer rate, calculated as the difference between the offered rate and the drop rate counters, can sporadically deviate from the average by up to 20 percent or more. This can occur while no corresponding burst is registered by independent traffic analyser equipment. | |
| Match | Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and QoS groups. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide* . |
| drop | Indicates that the packet discarding action for all the packets belonging to the specified class has been configured. |

**Note** A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

## Examples

The following sample output from the **show policy-map interface** command shows traffic policing configured using a CIR based on a bandwidth of 20 percent. The CIR and committed burst (Bc) in milliseconds (ms) are included in the display.

```
Router# show policy-map interface Serial3/1

  Service-policy output: mypolicy
    Class-map: gold (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      police:
          cir 20 % bc 10 ms
          cir 2000000 bps, bc 2500 bytes
          pir 40 % be 20 ms
          pir 4000000 bps, be 10000 bytes
     conformed 0 packets, 0 bytes; actions:
      transmit
     exceeded 0 packets, 0 bytes; actions:
       drop
      violated 0 packets, 0 bytes; actions:
       drop
      conformed 0 bps, exceed 0 bps, violate 0 bps
```

The table below describes the significant fields shown in the display. A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

***Table 221: show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping.***

| Field | Description |
|---|---|
| Service-policy output | Name of the output service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets, bytes | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |

| Field | Description |
|---|---|
| offered rate | Rate, in kbps, of packets coming in to the class.<br>**Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only. |
| police | Indicates that traffic policing based on a percentage of bandwidth has been enabled. Also, displays the bandwidth percentage, the CIR, and the committed burst (Bc) size in ms. |
| conformed, actions | Displays the number of packets and bytes marked as conforming to the specified rates, and the action to be taken on those packets. |
| exceeded, actions | Displays the number of packets and bytes marked as exceeding the specified rates, and the action to be taken on those packets. |

## Examples

The following sample output from the **show policy-map interface** command (shown below) displays the statistics for the serial 3/2 interface. Traffic shaping has been enabled on this interface, and an average rate of 20 percent of the bandwidth has been specified.

**Note** In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```
Router# show policy-map interface Serial3/2

Serial3/2
  Service-policy output: p1
    Class-map: c1 (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
```

```
Match: any
Traffic Shaping
  Target/Average      Byte   Sustain    Excess      Interval  Increment  Adapt
  Rate              Limit  bits/int  bits/int    (ms)     (bytes)   Active
   20 %                        10 (ms)    20 (ms)
  201500/201500       1952   7808       7808        38         976       -
  Queue     Packets   Bytes     Packets   Bytes     Shaping
  Depth                         Delayed   Delayed   Active
  0         0         0         0         0         no
```

The table below describes the significant fields shown in the display. A number in parentheses may appear next to the service-policy output name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

***Table 222: show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping (with Traffic Shaping Enabled).***

| Field | Description |
|---|---|
| Service-policy output | Name of the output service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets, bytes | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in kbps, of packets coming in to the class.<br>**Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only. |
| drop rate | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate. |

| Field | Description |
|---|---|
| Match | Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and quality of service (QoS) groups. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Quality of Service Solutions Configuration Guide*. |
| Traffic Shaping | Indicates that traffic shaping based on a percentage of bandwidth has been enabled. |
| Target/Average Rate | Rate (percentage) used for shaping traffic and the number of packets meeting that rate. |
| Byte Limit | Maximum number of bytes that can be transmitted per interval. Calculated as follows:<br>((Bc+Be) /8 ) x 1 |
| Sustain bits/int | Committed burst (Bc) rate. |
| Excess bits/int | Excess burst (Be) rate. |
| Interval (ms) | Time interval value in milliseconds (ms). |
| Increment (bytes) | Number of credits (in bytes) received in the token bucket of the traffic shaper during each time interval. |
| Adapt Active | Indicates whether adaptive shaping is enabled. |
| Queue Depth | Current queue depth of the traffic shaper. |
| Packets | Total number of packets that have entered the traffic shaper system. |
| Bytes | Total number of bytes that have entered the traffic shaper system. |
| Packets Delayed | Total number of packets delayed in the queue of the traffic shaper before being transmitted.<br>**Note** In Cisco IOS Release 12.4(20)T, this counter was removed. |
| Bytes Delayed | Total number of bytes delayed in the queue of the traffic shaper before being transmitted.<br>**Note** In Cisco IOS Release 12.4(20)T, this counter was removed. |

| Field | Description |
|---|---|
| Shaping Active | Indicates whether the traffic shaper is active. For example, if a traffic shaper is active, and the traffic being sent exceeds the traffic shaping rate, a “yes” appears in this field. |

## Examples

The following sample output from the **show policy-map interface** command displays the packet statistics for the Ethernet4/1 interface, to which a service policy called “mypolicy” is attached. The Layer 3 packet length has been specified as a match criterion for the traffic in the class called “class1”.

```
Router# show policy-map interface Ethernet4/1

  Ethernet4/1
  Service-policy input: mypolicy
    Class-map: class1 (match-all)
       500 packets, 125000 bytes
       5 minute offered rate 4000 bps, drop rate 0 bps
       Match: packet length min 100 max 300
       QoS Set
         qos-group 20
           Packets marked 500
```

The table below describes the significant fields shown in the display. A number in parentheses may appear next to the service-policy input name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

***Table 223: show policy-map interface Field Descriptions—Configured for Packet Classification Based on Layer 3 Packet Length.***

| Field | Description |
|---|---|
| Service-policy input | Name of the input service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets, bytes | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |

| Field | Description |
|---|---|
| offered rate | Rate, in kbps, of packets coming in to the class.<br>**Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only. |
| drop rate | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate. |
| Match | Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and QoS groups. |
| QoS Set, qos-group, Packets marked | Indicates that class-based packet marking based on the QoS group has been configured. Includes the qos-group number and the number of packets marked. |

## Examples

The following sample output of the **show policy-map interface** command shows the service policies attached to a FastEthernet subinterface. In this example, a service policy called “policy1” has been attached. In “policy1”, a table map called “table-map1” has been configured. The values in “table-map1” will be used to map the precedence values to the corresponding class of service (CoS) values.

```
Router# show policy-map interface

 FastEthernet1/0.1
  Service-policy input: policy1
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      QoS Set
        precedence cos table table-map1
          Packets marked 0
```

The table below describes the fields shown in the display. A number in parentheses may appear next to the service-policy input name and the class-map name. The number is for Cisco internal use only and can be disregarded.

***Table 224: show policy-map interface Field Descriptions—Configured for Enhanced Packet Marking.***

| Field | Description |
|---|---|
| Service-policy input | Name of the input service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets, bytes | Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in kbps, of the packets coming into the class. |
| Match | Match criteria specified for the class of traffic. Choices include criteria such as Precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) group (set). For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Quality of Service Solutions Configuration Guide*. |
| QoS Set | Indicates that QoS group (set) has been configured for the particular class. |
| precedence cos table table-map1 | Indicates that a table map (called "table-map1") has been used to determine the precedence value. The precedence value will be set according to the CoS value defined in the table map. |
| Packets marked | Total number of packets marked for the particular class. |

## Examples

The following is sample output from the **show policy-map interface** command. This sample displays the statistics for the serial 2/0 interface on which traffic policing has been enabled. The committed (conform) burst (bc) and excess (peak) burst (be) are specified in milliseconds (ms).

```
Router# show policy-map interface serial2/0
```

```
Serial2/0
 Service-policy output: policy1 (1050)
   Class-map: class1 (match-all) (1051/1)
     0 packets, 0 bytes
     5 minute offered rate 0 bps, drop rate 0 bps
     Match: ip precedence 0  (1052)
     police:
         cir 20 % bc 300 ms
         cir 409500 bps, bc 15360 bytes
         pir 40 % be 400 ms
         pir 819000 bps, be 40960 bytes
       conformed 0 packets, 0 bytes; actions:
         transmit
       exceeded 0 packets, 0 bytes; actions:
         drop
       violated 0 packets, 0 bytes; actions:
         drop
       conformed 0 bps, exceed 0 bps, violate 0 bps
   Class-map: class-default (match-any) (1054/0)
     0 packets, 0 bytes
     5 minute offered rate 0 bps, drop rate 0 bps
     Match: any  (1055)
       0 packets, 0 bytes
       5 minute rate 0 bps
```

In this example, the CIR and PIR are displayed in bps, and both the committed burst (bc) and excess burst (be) are displayed in bits.

The CIR, PIR bc, and be are calculated on the basis of the formulas described below.

## Examples

When calculating the CIR, the following formula is used:

- CIR percentage specified (as shown in the output from the **show policy-map** command) * bandwidth (BW) of the interface (as shown in the output from the**show interfaces** command) = total bits per second

According to the output from the **show interfaces** command for the serial 2/0 interface, the interface has a bandwidth (BW) of 2048 kbps.

```
Router# show interfaces serial2/0

Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

The following values are used for calculating the CIR:

20 % * 2048 kbps = 409600 bps

## Examples

When calculating the PIR, the following formula is used:

- PIR percentage specified (as shown in the output from the **show policy-map** command) * bandwidth (BW) of the interface (as shown in the output from the**show interfaces** command) = total bits per second

According to the output from the **show interfaces** command for the serial 2/0 interface, the interface has a bandwidth (BW) of 2048 kbps.

```
Router# show interfaces serial2/0

Serial2/0 is administratively down, line protocol is down
  Hardware is M4T
  MTU 1500 bytes, BW 2048 Kbit, DLY 20000 usec, rely 255/255, load 1/255
```

The following values are used for calculating the PIR:

40 % * 2048 kbps = 819200 bps

**Note** Discrepancies between this total and the total shown in the output from the **show policy-map interface** command can be attributed to a rounding calculation or to differences associated with the specific interface configuration.

## Examples

When calculating the bc, the following formula is used:

- The bc in milliseconds (as shown in the **show policy-map** command) * the CIR in bits per seconds = total number bytes

The following values are used for calculating the bc:

300 ms * 409600 bps = 15360 bytes

## Examples

When calculating the bc and the be, the following formula is used:

- The be in milliseconds (as shown in the **show policy-map** command) * the PIR in bits per seconds = total number bytes

The following values are used for calculating the be:

400 ms * 819200 bps = 40960 bytes

The table below describes the significant fields shown in the display.

***Table 225: show policy-map interface Field Descriptions***

| Field | Description |
|---|---|
| Service-policy output | Name of the output service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets and bytes | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in kbps, of packets coming in to the class. |
| drop rate | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate. |

| Field | Description |
|---|---|
| Match | Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) groups. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Quality of Service Solutions Configuration Guide* . |
| police | Indicates that traffic policing has been enabled. Display includes the CIR, PIR (in both a percentage of bandwidth and in bps) and the bc and be in bytes and milliseconds. Also displays the optional conform, exceed, and violate actions, if any, and the statistics associated with these optional actions. |

## Examples

The following sample output from the **show policy-map interface** command displays statistics for the Fast Ethernet 0/1 interface on which bandwidth estimates for quality of service (QoS) targets have been generated.

The Bandwidth Estimation section indicates that bandwidth estimates for QoS targets have been defined. These targets include the packet loss rate, the packet delay rate, and the timeframe in milliseconds. Confidence refers to the drop-one-in value (as a percentage) of the targets. Corvil Bandwidth means the bandwidth estimate in kilobits per second.

When no drop or delay targets are specified, "none specified, falling back to drop no more than one packet in 500" appears in the output.

```
Router# show policy-map interface FastEthernet0/1

 FastEthernet0/1
  Service-policy output: my-policy
    Class-map: icmp (match-all)
      199 packets, 22686 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: access-group 101
      Bandwidth Estimation:
        Quality-of-Service targets:
          drop no more than one packet in 1000 (Packet loss < 0.10%)
          delay no more than one packet in 100 by 40 (or more) milliseconds
            (Confidence: 99.0000%)
        Corvil Bandwidth: 1 kbits/sec
    Class-map: class-default (match-any)
      112 packets, 14227 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      Bandwidth Estimation:
        Quality-of-Service targets:
          <none specified, falling back to drop no more than one packet in 500
        Corvil Bandwidth: 1 kbits/sec
```

## Examples

The following sample output from the **show policy-mapinterface** command shows that shaping is active (as seen in the queue depth field) with HQF enabled on the serial 4/3 interface. All traffic is classified to the class-default queue.

**Note** In HQF images for Cisco IOS Releases 12.4(20)T and later, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```
Router# show policy-map interface serial4/3

 Serial4/3
  Service-policy output: shape
    Class-map: class-default (match-any)
      2203 packets, 404709 bytes
      30 second offered rate 74000 bps, drop rate 14000 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 64/354/0
      (pkts output/bytes output) 1836/337280
      shape (average) cir 128000, bc 1000, be 1000
      target shape rate 128000
        lower bound cir 0,  adapt to fecn 0
      Service-policy : LLQ
        queue stats for all priority classes:

          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
        Class-map: c1 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 1
          Priority: 32 kbps, burst bytes 1500, b/w exceed drops: 0
        Class-map: class-default (match-any)
          2190 packets, 404540 bytes
          30 second offered rate 74000 bps, drop rate 14000 bps
          Match: any
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 63/417/0
          (pkts output/bytes output) 2094/386300
```

## Examples

**Note** As of Cisco IOS Release 12.2(31)SB2, matching packets on the basis of VLAN ID numbers is supported on the Catalyst 1000 platform only.

The following is a sample configuration in which packets are matched and classified on the basis of the VLAN ID number. In this sample configuration, packets that match VLAN ID number 150 are placed in a class called “class1.”

```
Router# show class-map

Class Map match-all class1 (id 3)
Match vlan 150
```

Class1 is then configured as part of the policy map called “policy1.” The policy map is attached to Fast Ethernet subinterface 0/0.1.

The following sample output of the **show policy-map interface** command displays the packet statistics for the policy maps attached to Fast Ethernet subinterface 0/0.1. It displays the statistics for policy1, in which class1 has been configured.

```
Router# show policy-map interface

FastEthernet0/0.1
! Policy-map name.
Service-policy input: policy1
! Class configured in the policy map.
Class-map: class1 (match-all)
0 packets, 0 bytes
5 minute offered rate 0 bps, drop rate 0 bps
! VLAN ID 150 is the match criterion for the class.
Match: vlan 150
police:
cir 8000000 bps, bc 512000000 bytes
conformed 0 packets, 0 bytes; actions:
transmit
exceeded 0 packets, 0 bytes; actions:
drop
conformed 0 bps, exceed 0 bps
Class-map: class-default (match-any)
10 packets, 1140 bytes
5 minute offered rate 0 bps, drop rate 0 bps
Match: any
10 packets, 1140 bytes
5 minute rate 0 bps
```

The table below describes the significant fields shown in the display. A number in parentheses may appear next to the service-policy input name and the class-map name. The number is for Cisco internal use only and can be disregarded.

***Table 226: show policy-map interface Field Descriptions—Packets Matched on the Basis of VLAN ID Number.***

| Field | Description |
|---|---|
| Service-policy input | Name of the input service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets, bytes | Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in kbps, of the packets coming into the class. |

| Field | Description |
|---|---|
| Match | Match criteria specified for the class of traffic. Choices include criteria such as VLAN ID number, precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) group (set). For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide* . |

## Examples

The following example shows how to display the statistics and the configurations of all the input and output policies that are attached to an interface on a Cisco 7600 series router:

```
Router# show policy-map interface

 FastEthernet5/36
  service-policy input: max-pol-ipp5
    class-map: ipp5 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
  class ipp5
    police 2000000000 2000000 conform-action set-prec-transmit 6 exceed-action p
oliced-dscp-transmit
```

The following example shows how to display the input-policy statistics and the configurations for a specific interface on a Cisco 7600 series router:

```
Router# show policy-map interface fastethernet 5/36 input

 FastEthernet5/36
  service-policy input: max-pol-ipp5
    class-map: ipp5 (match-all)
      0 packets, 0 bytes
      5 minute rate 0 bps
      match: ip precedence 5
  class ipp5
    police 2000000000 2000000 conform-action set-prec-transmit 6 exceed-action p
oliced-dscp-transmit
```

The table below describes the significant fields shown in the display.

***Table 227: show policy-map interface Field Descriptions—Cisco 7600 Series Routers***

| Field | Description |
|---|---|
| service-policy input | Name of the input service policy applied to the specified interface. |
| class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |

| Field | Description |
|---|---|
| packets, bytes | Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| minute rate | Rate, in kbps, of the packets coming into the class. |
| match | Match criteria specified for the class of traffic. Choices include criteria such as VLAN ID number, precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) group (set). For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide* . |
| class | Precedence value. |
| police | Indicates that the **police** command has been configured to enable traffic policing. |

## Examples

The following example shows the automatic rounding-off of the **bc** and **be** values, in the MQC police policy-map, to the interface's MTU size in a Cisco 7200 series router. The rounding-off is done only when the bc and be values are lesser than the interface's MTU size.

```
Router# show policy-map interface

Service-policy output: p2
Service-policy output: p2
    Class-map: class-default (match-any)
      2 packets, 106 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: any
        2 packets, 106 bytes
        30 second rate 0 bps
      police:
          cir 10000 bps, bc 4470 bytes
          pir 20000 bps, be 4470 bytes
        conformed 0 packets, 0 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps, violate 0000 bps
```

## Examples

The following sample output from the show policy-map interface command shows the types of statistical information that displays when multiple priority queues are configured. Depending upon the interface in use and the options enabled, the output that you see may vary slightly from the output shown below.

```
Router# show policy-map interface

Serial2/1/0
Service-policy output: P1
Queue statistics for all priority classes:
.
.
.
Class-map: Gold (match-all)
0 packets, 0 bytes   /*Updated for each priority level configured.*/
5 minute offered rate 0 bps, drop rate 0 bps
Match: ip precedence 2
Priority: 0 kbps, burst bytes 1500, b/w exceed drops: 0
Priority Level 4:
0 packets, 0 bytes
```

## Examples

The following sample output from the show policy-map interface command indicates that bandwidth-remaining ratios are configured for class queues. As shown in the example, the classes precedence_0, precedence_1, and precedence_2 have bandwidth-remaining ratios of 20, 40, and 60, respectively.

```
Router# show policy-map interface GigabitEthernet1/0/0.10

  Service-policy output: vlan10_policy
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      Queueing
      queue limit 250 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 1000000, bc 4000, be 4000
      target shape rate 1000000
      bandwidth remaining ratio 10
      Service-policy : child_policy
        Class-map: precedence_0 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 0
          Queueing
          queue limit 62 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 20
        Class-map: precedence_1 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 1
          Queueing
          queue limit 62 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 500000, bc 2000, be 2000
          target shape rate 500000
          bandwidth remaining ratio 40
        Class-map: precedence_2 (match-all)
          0 packets, 0 bytes
```

```
    30 second offered rate 0 bps, drop rate 0 bps
    Match: ip precedence 2
    Queueing
    queue limit 62 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    shape (average) cir 500000, bc 2000, be 2000
    target shape rate 500000
    bandwidth remaining ratio 60
  Class-map: class-default (match-any)
    0 packets, 0 bytes
    30 second offered rate 0 bps, drop rate 0 bps
    Match: any
      0 packets, 0 bytes
      30 second rate 0 bps

    queue limit 62 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
```

The table below describes the significant fields shown in the display.

***Table 228: show policy-map interface Field Descriptions—Configured for Bandwidth-Remaining Ratios***

| Field | Description |
|---|---|
| Service-policy output | Name of the output service policy applied to the specified interface. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets, bytes | Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| bandwidth remaining ratio | Indicates the ratio used to allocate excess bandwidth. |

## Examples

In this sample output of the **show policy-map interface** command, the character string “ip dscp tunnel 3” indicates that L2TPv3 tunnel marking has been configured to set the DSCP value to 3 in the header of a tunneled packet.

```
Router# show policy-map interface

 Serial0
  Service-policy input: tunnel
    Class-map: frde (match-all)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: fr-de
      QoS Set
        ip dscp tunnel 3
          Packets marked 0
    Class-map: class-default (match-any)
      13736 packets, 1714682 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
```

```
        13736 packets, 1714682 bytes
        30 second rate 0 bps
```

The table below describes the significant fields shown in the display.

***Table 229: show policy-map interface Field Descriptions—Configured for Tunnel Marking***

| Field | Description |
|---|---|
| service-policy input | Name of the input service policy applied to the specified interface. |
| class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets, bytes | Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in kbps, of packets coming in to the class. |
| drop rate | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate. |
| match | Match criteria specified for the class of traffic. In this example, the Frame Relay Discard Eligible (DE) bit has been specified as the match criterion.<br>For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide*. |
| ip dscp tunnel | Indicates that tunnel marking has been configured to set the DSCP in the header of a tunneled packet to a value of 3. |

## Examples

The following output from the show policy-map interface command indicates that ATM overhead accounting is enabled for shaping and disabled for bandwidth:

```
Router# show policy-map interface

Service-policy output:unit-test
Class-map: class-default (match-any)
100 packets, 1000 bytes
30 second offered rate 800 bps, drop rate 0 bps
Match: any
shape (average) cir 154400, bc 7720, be 7720
target shape rate 154400
```

```
overhead accounting: enabled
bandwidth 30% (463 kbps)
overhead accounting: disabled
queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(packets output/bytes output) 100/1000
```

The table below describes the significant fields shown in the display.

***Table 230: show policy-map interface Field Descriptions—Configured for Traffic Shaping Overhead Accounting for ATM***

| Field | Description |
|---|---|
| service-policy output | Name of the output service policy applied to the specified interface. |
| class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets, bytes | Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in kbps, of packets coming in to the class. |
| drop rate | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate. |
| match | Match criteria specified for the class of traffic. In this example, the Frame Relay Discard Eligible (DE) bit has been specified as the match criterion.<br>For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide*. |
| target shape rate | Indicates that traffic shaping is enabled at the specified rate. |
| overhead accounting | Indicates whether overhead accounting is enabled or disabled for traffic shaping. |
| bandwidth | Indicates the percentage of bandwidth allocated for traffic queueing. |
| overhead accounting: | Indicates whether overhead accounting is enabled or disabled for traffic queueing. |

## Examples

The following output from the show policy-map interface command displays the configuration for Fast Ethernet interface 0/0:

**Note** In HQF images for Cisco IOS Releases 12.4(20)T and later releases, the packets delayed and bytes delayed counters were removed for traffic shaping classes.

```
Router# show policy-map interface FastEthernet0/0
 FastEthernet0/0

  Service-policy output: test1

    Class-map: class-default (match-any)
      129 packets, 12562 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 129/12562
      shape (average) cir 1536000, bc 6144, be 6144
      target shape rate 1536000

      Service-policy : test2

        queue stats for all priority classes:

          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0

        Class-map: RT (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip dscp ef (46)
          Priority: 20% (307 kbps), burst bytes 7650, b/w exceed drops: 0


        Class-map: BH (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip dscp af41 (34)
          Queueing
          queue limit 128 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth 40% (614 kbps)

        Class-map: BL (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip dscp af21 (18)
          Queueing
          queue limit 64 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth 35% (537 kbps)
            Exp-weight-constant: 9 (1/512)
            Mean queue depth: 0 packets
            dscp     Transmitted   Random drop   Tail drop   Minimum   Maximum   Mark
                     pkts/bytes    pkts/bytes    pkts/bytes  thresh    thresh    prob

            af21     0/0           0/0           0/0         100       400       1/10

        Class-map: class-default (match-any)
          129 packets, 12562 bytes
```

```
30 second offered rate 0 bps, drop rate 0 bps
Match: any

queue limit 64 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 129/12562
```

The table below describes the significant fields shown in the display.

***Table 231: show policy-map interface Field Descriptions—Configured for HQF***

| Field | Description |
|---|---|
| FastEthernet | Name of the interface. |
| service-policy output | Name of the output service policy applied to the specified interface. |
| class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets, bytes | Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in kbps, of packets coming in to the class. |
| drop rate | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate. |
| Match | Match criteria specified for the class of traffic.<br>**Note** For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide*. |
| Queueing | Indicates that queueing is enabled. |
| queue limit | Maximum number of packets that a queue can hold for a class policy configured in a policy map. |
| bandwidth | Indicates the percentage of bandwidth allocated for traffic queueing. |

| Field | Description |
|---|---|
| dscp | Differentiated services code point (DSCP). Values can be the following:<br>• 0 to 63—Numerical DSCP values. The default value is 0.<br>• af1 to af43—Assured forwarding (AF) DSCP values.<br>• cs1 to cs7—Type of service (ToS) precedence values.<br>• default—Default DSCP value.<br>• ef—Expedited forwarding (EF) DSCP values. |

## Examples

The following example shows the new output fields associated with the QoS: Policies Aggregation Enhancements feature beginning in Cisco IOS XE Release 2.6 for subscriber statistics. The new output fields begin with the label "Account QoS Statistics."

```
Router# show policy-map interface port-channel 1.1

Port-channel1.1
   Service-policy input: input_policy
     Class-map: class-default (match-any)
       0 packets, 0 bytes
       5 minute offered rate 0000 bps, drop rate 0000 bps
       Match: any
       QoS Set
       dscp default
       No packet marking statistics available
   Service-policy output: Port-channel_1_subscriber
     Class-map: EF (match-any)
       105233 packets, 6734912 bytes
       5 minute offered rate 134000 bps, drop rate 0000 bps
       Match: dscp ef (46)
       Match: access-group name VLAN_REMARK_EF
       Match: qos-group 3
       Account QoS statistics
         Queueing
           Packets dropped 0 packets/0 bytes
       QoS Set
       cos 5
       No packet marking statistics available
       dscp ef
       No packet marking statistics available
     Class-map: AF4 (match-all)
       105234 packets, 6734976 bytes
       5 minute offered rate 134000 bps, drop rate 0000 bps
       Match: dscp cs4 (32)
       Account QoS statistics
         Queueing
           Packets dropped 0 packets/0 bytes
       QoS Set
       cos 4
       No packet marking statistics available
     Class-map: AF1 (match-any)
       315690 packets, 20204160 bytes
       5 minute offered rate 402000 bps, drop rate 0000 bps
       Match: dscp cs1 (8)
```

```
      Match: dscp af11 (10)
      Match: dscp af12 (12)
      Account QoS statistics
        Queueing
          Packets dropped 0 packets/0 bytes
      QoS Set
      cos 1
      No packet marking statistics available
    Class-map: class-default (match-any) fragment Port-channel_BE
      315677 packets, 20203328 bytes
      5 minute offered rate 402000 bps, drop rate 0000 bps
      Match: any
      Queueing
        queue limit 31250 bytes
        (queue depth/total drops/no-buffer drops) 0/0/0
        (pkts output/bytes output) 315679/20203482
        bandwidth remaining ratio 1
```

## Examples

The following example shows how to display the policer statistics (the packet and byte count). The output displays only the applicable count (either packets or bytes) with the actual number.

```
Router# show policy-map interface GigabitEthernet 3/1 input

GigabitEthernet3/1
  Service-policy input: in1
    Class-map: p1 (match-all)
      0 packets
      Match:  precedence 1
           QoS Set
             ip precedence 7
      police:
          cir 20 %
          cir 200000000 bps, bc 6250000 bytes
        conformed 0 bytes; actions:
          transmit
        exceeded 0 bytes; actions:
          drop
        conformed 0000 bps, exceed 0000 bps
    Class-map: class-default (match-any)
      10000000 packets
      Match: any
      police:
          cir 20 %
          cir 200000000 bps, bc 6250000 bytes
        conformed 174304448 bytes; actions:
          transmit
        exceeded 465695552 bytes; actions:
          drop
        conformed 4287000 bps, exceed 11492000 bps
```

## Examples

The following example shows how to display the statistics and the configurations of the input and output service policies that are attached to an interface:

```
Router# show policy-map interface GigabitEthernet 1/2/0

Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *23:02:40.857 pst Thu Mar 3 2011

 GigabitEthernet1/2/0

  Service-policy input: policy-in

    Class-map: class-exp-0 (match-all)
      6647740 packets, 9304674796 bytes
      30 second offered rate 3234000 bps, drop rate 0 bps
      Match: mpls experimental topmost 0
      QoS Set
```

```
      precedence 3
        Packets marked 6647740

  Class-map: class-default (match-any)
    1386487 packets, 1903797872 bytes
    30 second offered rate 658000 bps, drop rate 0 bps
    Match: any

Service-policy output: policy-out

  Class-map: class-pre-1 (match-all)
    2041355 packets, 2857897000 bytes
    30 second offered rate 986000 bps, drop rate 0 bps

    Match: ip precedence 1
    QoS Set
      mpls experimental topmost 1
        Packets marked 2041355

  Class-map: class-default (match-any)
    6129975 packets, 8575183331 bytes
    30 second offered rate 2960000 bps, drop rate 0 bps
    Match: any
```

The table below describes the significant fields shown in the display.

***Table 232: show policy-map interface Field Descriptions—Cisco Catalyst 4000 Series Routers***

| Field | Description |
|---|---|
| class-map | Displays the class of traffic. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| conformed | Displays the action to be taken on packets conforming to a specified rate. Also displays the number of packets and bytes on which the action was taken. |
| drop | Indicates that the packet discarding action for all the packets belonging to the specified class has been configured. |
| exceeded | Displays the action to be taken on packets exceeding a specified rate. Displays the number of packets and bytes on which the action was taken. |
| match | Match criteria specified for the class of traffic. |
| packets, bytes | Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| police | Indicates that the **police** command has been configured to enable traffic policing. Also displays the specified CIR, conform burst size, peak information rate (PIR), and peak burst size used for marking packets. |

| Field | Description |
|---|---|
| QoS Set | Indicates that QoS group (set) has been configured for the particular class. |
| service-policy input | Name of the input service policy applied to the specified interface. |

## Examples

The following example shows how to display the class maps configured for a pseudowire interface:

```
Router# show policy-map interface pseudowire2
 pseudowire2
  Service-policy output: pw_brr

    Class-map: prec1 (match-all)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 1
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 1

    Class-map: prec2 (match-all)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 2
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 2

    Class-map: prec3 (match-all)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: ip precedence 3
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 3

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 4166 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      bandwidth remaining ratio 4
Device#
```

The table below describes the significant fields shown in the display.

*Table 233: show policy-map interface Field Descriptions—Pseudowire Policy Map Information*

| Field | Description |
|---|---|
| bandwidth | Indicates the percentage of bandwidth allocated for traffic queueing. |
| Class-map | Displays the class of traffic. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| Match | Match criteria specified for the class of traffic. |
| packets, bytes | Number of the packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| Queueing | Indicates that queueing is enabled. |
| queue limit | Maximum number of packets that a queue can hold for a class policy configured in a policy map. |
| service-policy output | Name of the output service policy applied to the specified interface. |

## Related Commands

| Command | Description |
|---|---|
| **bandwidth remaining ratio** | Specifies a bandwidth-remaining ratio for class queues and subinterface-level queues to determine the amount of unused (excess) bandwidth to allocate to the queue during congestion. |
| **class-map** | Creates a class map to be used for matching packets to a specified class. |
| **compression header ip** | Configures RTP or TCP IP header compression for a specific class. |
| **drop** | Configures a traffic class to discard packets belonging to a specific class. |
| **match fr-dlci** | Specifies the Frame Relay DLCI number as a match criterion in a class map. |
| **match packet length (class-map)** | Specifies the length of the Layer 3 packet in the IP header as a match criterion in a class map. |

| Command | Description |
|---|---|
| **police** | Configures traffic policing. |
| **police (percent)** | Configures traffic policing on the basis of a percentage of bandwidth available on an interface. |
| **police (two rates)** | Configures traffic policing using two rates, the CIR and the PIR. |
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **priority** | Specifies that low-latency behavior must be given to a traffic class and configures multiple priority queues. |
| **random-detect ecn** | Enables ECN. |
| **shape (percent)** | Specifies average or peak rate traffic shaping on the basis of a percentage of bandwidth available on an interface. |
| **show class-map** | Display all class maps and their matching criteria. |
| **show frame-relay pvc** | Displays statistics about PVCs for Frame Relay interfaces. |
| **show interfaces** | Displays statistics for all interfaces configured on a router or access server. |
| **show mls qos** | Displays MLS QoS information. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map class** | Displays the configuration for the specified class of the specified policy map. |
| **show table-map** | Displays the configuration of a specified table map or of all table maps. |
| **table-map (value mapping)** | Creates and configures a mapping table for mapping and converting one packet-marking value to another. |

# show policy-map interface brief

To display information about only the active policy maps attached to an interface, use the **showpolicy-mapinterfacebrief**command in privileged EXEC mode.

**show policy-map interface** [**input**| **output**] **brief** [ *policy-map-name* ] [**vrf** [ *vrf-id* ]] **[timestamp]**

## Syntax Description

| | |
|---|---|
| **input** | (Optional) Indicates that only the information about the active input policy maps will be displayed. |
| **output** | (Optional) Indicates that only the information about the active output policy maps will be displayed. |
| **brief** | Indicates that the name of all the active policy maps (both input and output policy maps) and the interfaces to which the policy maps are attached will be displayed. The active input policy maps will be displayed first, followed by the output policy maps. |
| *policy-map-name* | (Optional) Name of an active policy map to be displayed. |
| **vrf** | (Optional) Indicates that the active policy maps for Virtual Private Network (VPN) routing and forwarding (VRF) instances will be displayed. |
| *vrf-id* | (Optional) A specific VRF identifier. |
| **timestamp** | (Optional) Indicates that the date and time when the policy map was attached will be displayed, along with the ID of the user who attached the policy map. |

## Command Default

If no optional keywords or arguments are specified, all policy maps (even those that are not active) are displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(28)SB | This command was introduced. |
| 12.2(33)SRB | This command was integrated into Cisco IOS Release 12.2(33)SRB. |

| Release | Modification |
|---|---|
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |

## Usage Guidelines

The **showpolicy-mapinterfacebrief**command displays the name of the active policy maps and the interfaces to which those policy maps are attached. An active policy map is one that is attached to an interface.

The optional keywords and arguments allow you to tailor the information displayed about VPNs, time stamps, and user IDs.

If you do not specify any optional keywords or arguments, all policy maps (even those that are not active) are displayed.

**VPN Information Reported**

The **showpolicy-mapinterfacebrief**command can be used for VRF interfaces in applications that use VPNs. To specify VRF interfaces, use the **vrf** keyword with the *vrf-id* argument.

**Time-stamp and User ID Information Reported**

If the optional **timestamp** keyword is used with the **showpolicy-mapinterfacebrief**command, the time and date when a policy map was attached to an interface appear in the display. In addition to the time and date information, the name (that is, the user ID) of the person who attached the policy map to the interface will be displayed.

**Note** If the network software is reloaded (reinstalled), the time-stamp information (the time and date information) obtained will not be retained for any of the policy maps attached to interfaces on the network. Instead, the time and date information displayed will be the time and date when the software was reloaded.

**Method for Obtaining User Information**

The user information included in the display is obtained from the information that you enter when you log in to the router. For example, if you are using the SSH Secure Shell utility to log in to a router, you would typically enter your username and password. However, it is not always possible to obtain the user information. Instances where user information cannot be obtained include the following:

- Not all routers require user information when you log in. Therefore, you may not be prompted to enter your username when you log in to a router.
- If you are connecting to a console port using the Telnet utility in a DOS environment, you do not need to enter user information.
- The user information cannot be retrieved because of system constraints or other factors.

If the user information cannot be obtained, the words “by unknown” will be displayed.

**Hierarchical Policy Map Information**

For a hierarchical policy map structure, only the information about the parent policy maps is displayed. Information about child policy maps is not displayed.

**ATM PVCs**

For ATM permanent virtual circuits (PVCs), policy maps do not remain associated with the interface if the ATM PVC is not working properly (that is, the ATM PVC is “down”). Therefore, if an ATM PVC is down, and a policy map is attached to an interface, the **showpolicy-mapinterfacebrief**command does not include information about the policy maps in the command output.

**Examples**

The information that is displayed by the **showpolicy-mapinterfacebrief**command varies according to the optional keywords and arguments that you specify.

The following sections list the significant keyword and argument combinations used with the command and describe the corresponding information displayed.

**Examples**

The **showpolicy-mapinterfacebrief** command displays *all* the attached policy maps (both input policy maps and output policy maps) along with the information about the interfaces to which the policy maps are attached. The input policy maps are displayed first, followed by the output policy maps.

```
Service-policy input: policyname1
interface s2/0/1
interface s6/0/0
Service-policy output: policyname1interface s2/0/1 interface s6/0/0
```

**Examples**

The **showpolicy-mapinterfacebrieftimestamp** command displays *all* the attached policy maps (both input policy maps and output policy maps) along with the information about the interfaces to which the policy maps are attached. The input policy maps are displayed first, followed by the output policy maps.

The **timestamp** keyword displays the time and date when the policy map was attached to the specific interface, along with the user ID of the person who attached the policy map to the interface.

```
Service-policy input: parentpolicy1
Service-policy input: childpolicy1
interface s2/0/1 - applied 20:43:04 on 25/12/01 by user1
interface s6/0/1 - applied 19:43:04 on 25/12/01 by user1
Service-policy output: policyname2
interface s2/0/2 - applied 21:47:04 on 24/12/01 by user1
interface s6/0/1 - applied 19:43:04 on 25/12/01 by user1
```

**Examples**

The **showpolicy-mapinterfacebrief***policy-map-name* command displays the policy map attached as *either* an input policy map *or* an output policy map, along with the information about the interface to which the policy map is attached. Only the policy map specified by the *policy-map-name* argument is displayed.

For example, the display for the **showpolicy-mapinterfacebriefpolicyname1** command is as follows:

```
Service-policy input: policyname1
interface s2/0/1
interface s6/0/0
Service-policy output: policyname1
interface s1/0/2
interface s3/0/0
```

**Examples**

The **showpolicy-mapinterfacebrief***policy-map-name***timestamp** command displays the policy map attached as *either* an input policy map *or* an output policy map, along with the information about the interface to which it is attached. Only the policy map specified by the *policy-map-name* argument is displayed.

The **timestamp** keyword displays the time and date when the policy map was attached to the specific interface, along with the user ID of the person who attached the policy map to the interface.

For example, the display for the **showpolicy-mapinterfacebriefpolicyname2timestamp** command is as follows:

```
Service-policy input: policyname2
interface s2/0/2 - applied 21:47:04 on 24/12/01 by user1
interface s6/0/1 - applied 19:43:04 on 25/12/01 by user1
Service-policy output: policyname2
interface s4/0/2 - applied 12:47:04 on 24/12/01 by user1
interface s7/0/1 - applied 14:43:04 on 25/12/01 by user1
```

**Examples** The **showpolicy-mapinterfaceoutputbrief** command displays the attached *output* policy maps, along with the information about the interfaces to which they are attached.

```
Service-policy output: policyname1
```

**Examples** The **showpolicy-mapinterfaceoutputbrieftimestamp** command displays the attached *output* policy maps, along with the information about the interfaces to which they are attached.

The **timestamp** keyword displays the time and date when the policy map was attached to the specific interface, along with the user ID of the person who attached the policy map to the interface.

```
Service-policy output: policyname2
interface s2/0/2 - applied 21:47:04 on 24/12/01 by user1
interface s6/0/1 - applied 19:43:04 on 25/12/01 by user1
```

**Examples** The **showpolicy-mapinterfaceinputbrief** command displays the attached *input* policy maps, along with the information about the interfaces to which they are attached.

```
Service-policy input: policyname2
interface s2/0/2
interface s6/0/1
```

**Examples** The **showpolicy-mapinterfaceinputbrieftimestamp** command displays the attached *input* policy maps, along with the information about the interfaces to which they are attached.

The **timestamp** keyword displays the time and date when the policy map was attached to the specific interface, along with the user ID of the person who attached the policy map to the interface.

```
Service-policy input: policyname2
interface s2/0/2 - applied 21:47:04 on 24/12/01 by user1
interface s6/0/1 - applied 19:43:04 on 25/12/01 by user1
```

**Examples** The **showpolicy-mapinterfaceoutputbrief***policy-map-name* command displays the attached *output* policy map, along with the information about the interface to which it is attached. Only the policy map specified by the *policy-map-name* argument is displayed.

For example, the display for the **showpolicy-mapinterfaceoutputbriefpolicyname1**command is as follows:

```
Service-policy output: policyname1
interface s2/0/1
interface s6/0/0
```

**Examples**

The **showpolicy-mapinterfaceoutputbrief***policy-map-name***timestamp** command displays the attached *output* policy map, along with the information about the interface to which it is attached. Only the policy map specified by the *policy-map-name* argument is displayed.

The **timestamp** keyword displays the time and date when the policy map was attached to the specific interface, along with the user ID of the person who attached the policy map to the interface.

For example, the display for the **showpolicy-mapinterfaceoutputbriefpolicyname2timestamp** command is as follows:

```
Service-policy output: policyname2
interface s2/0/2 - applied 21:47:04 on 24/12/01 by user1
interface s6/0/1 - applied 19:43:04 on 25/12/01 by user1
```

**Examples**

The **showpolicy-mapinterfaceinputbrief***policy-map-name* command displays the attached *input* policy map, along with the information about the interface to which it is attached. Only the policy map specified by the *policy-map-name* argument is displayed.

For example, the display for the **showpolicy-mapinterfaceinputbriefpolicyname1** command is as follows:

```
Service-policy input: policyname1
interface s2/0/1
interface s6/0/0
```

**Examples**

The **showpolicy-mapinterfaceinputbrief***policy-map-name***timestamp** command displays the attached *input* policy map, along with the information about the interface to which it is attached. Only the policy map specified by the *policy-map-name* argument is displayed.

The **timestamp** keyword displays the time and date when the policy map was attached to the specific interface, along with the user ID of the person who attached the policy map to the interface.

For example, the display for the **showpolicy-mapinterfaceinputbriefpolicyname2timestamp** command is as follows:

```
Service-policy input: policyname2
interface s2/0/2 - applied 21:47:04 on 24/12/01 by user1
interface s6/0/1 - applied 19:43:04 on 25/12/01 by user1
```

**Examples**

The**showpolicy-mapinterfacebriefvrf** command displays *all* the policy maps (both input policy maps and output policy maps), along with information about the interfaces and the VRFs to which the policy maps are attached.

```
Service-policy input: policyname1
VRFA   interface s2/0/1
VRFB   interface s6/0/0
Service-policy output: policyname2
VRFC   interface s2/0/2
VRFB   interface s6/0/1
```

**Examples**

The **showpolicy-mapinterfacebriefvrftimestamp** command displays *all* the policy maps (both input policy maps and output policy maps), along with information about the interfaces and the VRFs to which the policy maps are attached.

The **timestamp** keyword displays the time and date when the policy map was attached to the specific interface, along with the user ID of the person who attached the policy map to the interface.

```
Service-policy input: policyname1
VRFA   interface s2/0/1 - applied 21:47:04 on 23/12/01 by user1
VRFB   interface s6/0/0 - applied 21:47:04 on 23/12/01 by user1
Service-policy output: policyname2
VRFC   interface s2/0/3 - applied 20:47:04 on 23/12/01 by user1
VRFD   interface s6/0/2 - applied 20:49:04 on 21/12/01 by user1
```

In some network configurations, the policy map may be attached to the interface initially, and then at a later time, the interface can be configured to act as a VRF interface. In this kind of network configuration, the time-stamp information displays the time when the policy map was attached to the interface. The display does not include the time when the interface was configured to act as a VRF interface. Displaying only the time when the policy map is attached to the interface also applies to the scenarios that are described in the following paragraph for other network configurations.

In other network configurations, a VRF may be attached to multiple interfaces as described in the following scenarios:

- The policy map is also attached to both the interfaces and the VRFs. In this network configuration, all the interfaces should be shown in the display for the VRF, under the policy map name, as follows:

```
Service-policy input: policyname1
VRF1 interface s2/0/1 - applied 21:47:37 on 23/12/01 by user1
     interface atm0/0 - applied 11:37:57 on 21/11/01 by user1
```

- The policy map is not attached to all interfaces to which the specific VRF is attached. In this network configuration, only the VRF interfaces that have that policy map configured are displayed.

## Examples

The **showpolicy-mapinterfacebrief***policy-map-name***vrftimestamp** command displays the policy maps attached as *either* an input policy map *or* an output policy map, along with information about the interface and VRF to which the policy map is attached. Only the policy map specified by the *policy-map-name* argument is displayed.

The **timestamp** keyword displays the time and date when the policy map was attached to the specific interface, along with the user ID of the person who attached the policy map to the interface.

For example, the display for the **showpolicy-mapinterfacebriefpolicyname1vrftimestamp** command is as follows:

```
Service-policy input: policyname1
VRF1   interface s2/0/1 - applied 21:47:04 on 23/12/01 by user1
Service-policy output: policyname1
VRF2   interface s6/0/1 - applied 21:47:04 on 23/12/01 by user1
```

## Examples

The **showpolicy-mapinterfacebrief***policy-map-name***vrf***vrf-id***timestamp** command displays *all* the policy maps (both the input policy maps and the output policy maps), along with information about the interface and VRF to which the policy maps are attached. Only the policy map and VRF specified by the *policy-map-name* argument and the *vrf-id* argument are displayed.

The **timestamp** keyword displays the time and date when the policy map was attached to the specific interface, along with the user ID of the person who attached the policy map to the interface.

For example, the display for **showpolicy-mapinterfacebriefpolicyname1vrfVRFAtimestamp**command is as follows:

```
Service-policy input: policyname1
VRFA   interface s2/0/1 - applied 21:47:04 on 23/12/01 by user1
Service-policy output: policyname1
VRFA   interface s6/0/1 - applied 21:47:04 on 23/12/01 by user1
```

**Examples**

The **showpolicy-mapinterfaceoutputbriefvrf** command displays the attached *output* policy maps, along with information about the interface and VRF to which the policy maps are attached.

```
Service-policy output: policyname2
VRFC   interface s2/0/2
VRFA   interface s6/0/1
```

**Examples**

The **showpolicy-mapinterfaceoutputbriefvrftimestamp**command displays the attached *output* policy maps, along with information about the interface and VRF to which the policy maps are attached.

The **timestamp** keyword displays the time and date when the policy map was attached to the specific interface, along with the user ID of the person who attached the policy map to the interface.

```
Service-policy output: policyname2
VRFC   interface s2/0/2 - applied 21:47:04 on 23/12/01 by user1
VRFA   interface s6/0/1 - applied 21:47:04 on 23/12/01 by user1
```

**Examples**

The **showpolicy-mapinterfaceinputbriefvrf** command displays the attached *input* policy maps, along with information about the interface and VRF to which the policy maps are attached.

```
Service-policy input: policyname1
VRFA   interface s2/0/1
VRFB   interface s6/0/0
Service-policy input: policyname2
VRFC   interface s2/0/2
VRFB   interface s6/0/1
```

**Examples**

The **showpolicy-mapinterfaceinputbriefvrftimestamp** command displays the attached *input* policy maps, along with information about the interface and VRF to which the policy maps are attached.

The **timestamp** keyword displays the time and date when the policy map was attached to the specific interface, along with the user ID of the person who attached the policy map to the interface.

```
Service-policy input: policyname1
VRFA   interface s2/0/1 - applied 21:47:04 on 23/12/01 by user1
VRFB   interface s6/0/0 - applied 21:47:04 on 23/12/01 by user1
Service-policy input: policyname2
VRFC   interface s2/0/3 - applied 20:47:04 on 23/12/01 by user1
VRFD   interface s6/0/2 - applied 20:49:04 on 21/12/01 by user1
```

**Examples**

The **showpolicy-mapinterfaceinputbriefvrf***vrf-id* command displays the attached *input* policy maps, along with information about the interface and VRF to which the policy maps are attached. Only the policy maps attached to the VRF specified by the *vrf-id* argument are displayed.

For example, the display for the **showpolicy-mapinterfaceinputbriefvrfVRFA** command is as follows:

```
Service-policy input: policyname1
VRFA   interface s2/0/1
Service-policy input: policyname2
VRFA   interface s6/0/1
```

**Examples**

The **showpolicy-mapinterfaceoutputbriefvrf***vrf-id* command displays the attached *output* policy maps, along with information about the interface and VRF to which the policy maps are attached. Only the policy maps attached to the VRF specified by the *vrf-id* argument are displayed.

For example, the display for the **showpolicy-mapinterfaceoutputbriefvrfVRFB** command is as follows:

```
Service-policy output: policyname1
VRFB   interface s2/0/1
Service-policy output: policyname2
VRFB   interface s6/0/1
```

**Examples**

The **showpolicy-mapinterfaceinputbriefvrf***vrf-id***timestamp** command displays the attached *input* policy maps, along with information about the interface and VRF to which the policy maps are attached. Only the policy maps attached to the VRF specified by the *vrf-id* argument are displayed.

The **timestamp** keyword displays the time and date when the policy map was attached to the specific interface, along with the user ID of the person who attached the policy map to the interface.

For example, the display for the **showpolicy-mapinterfaceinputbriefvrfVRFAtimestamp** command is as follows:

```
Service-policy input: policyname1
VRFA   interface s2/0/1 - applied 21:47:04 on 23/12/01 by user1
Service-policy input: policyname2
VRFA   interface s6/0/1 - applied 21:47:04 on 23/12/01 by user1
```

**Examples**

The **showpolicy-mapinterfaceoutputbriefvrf***vrf-id***timestamp** command displays the attached *output* policy maps, along with information about the interface and VRF to which the policy maps are attached. Only the policy maps attached to the VRF specified by the *vrf-id* argument are displayed.

The **timestamp** keyword displays the time and date when the policy map was attached to the specific interface, along with the user ID of the person who attached the policy map to the interface.

For example, the display for the **showpolicy-mapinterfaceoutputbriefvrfVRFBtimestamp**command is as follows:

```
Service-policy output: policyname1
VRFB   interface s2/0/1 - applied 21:47:04 on 23/12/01 by user1
Service-policy output: policyname2
VRFB   interface s6/0/1 - applied 21:47:04 on 23/12/01 by user1
```

The table below describes the significant fields shown in the various displays.

***Table 234: show policy-map interface brief Field Descriptions***

| Field | Description |
|---|---|
| Service-policy output: policyname2 | Output policy map name. |
| Service-policy input: policyname2 | Input policy map name. |

| Field | Description |
|---|---|
| interface s2/0/1 | Interface to which the policy map is attached. |
| VRFA | VRF to which the policy map is attached. |
| applied 21:47:04 on 23/12/01 | Time and date when the policy map was attached to the interface or VRF. |
| by user1 | User ID of the person who attached the policy map to the interface or VRF. |

## Related Commands

| Command | Description |
|---|---|
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |

# show policy-map interface service group

To display the policy-map information for service groups that have members attached to an interface, use the **showpolicy-mapinterfaceservicegroup**command in privileged EXEC mode.

**show policy-map interface** *type number* **service group** [ *service-group-identifier* ]

## Syntax Description

| | |
|---|---|
| *type* | Interface type. For more information, use the question mark (?) online help function. |
| *number* | Interface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function. |
| *service-group-identifier* | (Optional) Service-group number. Enter the number of an existing service group |

## Command Default

If a service group number is not specified, policy-map information for all service groups is displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRE | This command was introduced. |

## Usage Guidelines

Use the **showpolicy-mapinterfaceservicegroup** command to display information about one or more service groups with members that are attached to an interface or port-channel. The information displayed includes the policy maps attached to the interface or port-channel, the QoS features configured in those policy maps (for example, traffic policing or traffic queueing), and the corresponding packet statistics. Before using this command, the policy maps and service groups must be created.

## Examples

The following is an example of the **showpolicy-mapinterfaceservicegroup** command. In this example, service group 1 is specified. Service group 1 contains two policy maps (service policies), policy1 and policy2. Traffic policing is enabled in the policy1 policy map. Traffic queueing is enabled in the policy2 policy map.

```
Router# show policy-map interface gigabitEthernet 9/5 service group 1

 GigabitEthernet9/5: Service Group 1

  Service-policy input: policy1

    Class-map: class-default (match-any)
```

```
    0 packets, 0 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: any
    police:
        cir 200000 bps, bc 6250 bytes
      conformed 0 packets, 0 bytes; actions:
        transmit
      exceeded 0 packets, 0 bytes; actions:
        drop
      conformed 0000 bps, exceed 0000 bps

Service-policy output: policy2

Counters last updated 00:00:34 ago

  Class-map: class-default (match-any)
    0 packets, 0 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: any
    Queueing
    queue limit 131072 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    bandwidth remaining ratio 2
```

The table below describes the significant fields shown in the display.

***Table 235: show policy-map interface service group Field Descriptions***

| Field | Description |
|---|---|
| GigabitEthernet9/5: Service Group 1 | Interface and service-group number. |
| Service-policy input: policy1 Service-policy output: policy2 | Service-policy (policy-map) names and whether the policy is in the input (ingress) or the output (egress) direction on the interface. |
| police | Indicates that traffic policing is enabled. Statistics associated with traffic policing are also displayed. |
| Queueing | Indicates that a traffic queueing mechanism is enabled. Statistics associated with traffic queueing are also displayed. |

## Related Commands

| Command | Description |
|---|---|
| **show policy-map interface** | Displays the statistics and the configurations of the input and output policies that are attached to an interface. |
| **show policy-map interface service instance** | Displays the policy-map information for a given service instance under an interface or port-channel. |

# show policy-map interface service instance

To display the policy-map information for a given service instance under a port channel, use the show policy-map interface service instance command in user EXEC or privileged EXEC mode.

**show policy-map interface x service instance y**

## Syntax Description

| | |
|---|---|
| x | The number of the interface or the port channel. |
| y | The number of the service instance. |

## Command Modes

User EXEC Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRC | This command was introduced on the Cisco 7600 series routers. |

## Examples

The following example shows the policy-map output for a hierarchical policy on a given service instance 1 under port channel 1:

```
Router# show policy-map interface port-channel 1 service instance 1
Port-channel1: EFP 1
  Service-policy output: hqos-pc-brr
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 5000 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 20000000, bc 80000, be 80000
      target shape rate 20000000
      bandwidth remaining ratio 2
      Service-policy : flat-pc-brr
        Class-map: cos5 (match-all)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps

          Match: cos  5
          Queueing
          queue limit 2500 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
          shape (average) cir 10000000, bc 40000, be 40000
          target shape rate 10000000
        Class-map: class-default (match-any)
          0 packets, 0 bytes
          5 minute offered rate 0 bps, drop rate 0 bps
          Match: any
          Queueing
```

```
queue limit 2500 packets
(queue depth/total drops/no-buffer drops) 0/0/0
(pkts output/bytes output) 0/0
shape (average) cir 10000000, bc 40000, be 40000
target shape rate 10000000
```

The table below describes the significant fields shown in the display.

***Table 236: show policy-map interface service instance Field DescriptionsA number in parentheses may appear next to the service-policy output name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.***

| Field | Description |
|---|---|
| Fields Associated with Classes or Service Policies | |
| Service-policy output | Name of the output service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets and bytes | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in kbps, of packets coming in to the class.<br>**Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only. |
| drop rate | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate. |

| Field | Description |
|---|---|
| Match | Match criteria specified for the class of traffic. Choices include criteria such as IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental (EXP) value, access groups, and QoS groups. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide* . |
| Fields Associated with Queueing (if Enabled) | |
| Output Queue | The weighted fair queueing (WFQ) conversation to which this class of traffic is allocated. |
| Bandwidth | Bandwidth, in either kbps or percentage, configured for this class and the burst size. |
| pkts matched/bytes matched | Number of packets (also shown in bytes) matching this class that were placed in the queue. This number reflects the total number of matching packets queued at any time. Packets matching this class are queued only when congestion exists. If packets match the class but are never queued because the network was not congested, those packets are not included in this total. However, if process switching is in use, the number of packets is always incremented even if the network is not congested. |
| depth/total drops/no-buffer drops | Number of packets discarded for this class. No-buffer indicates that no memory buffer exists to service the packet. |
| Fields Associated with Weighted Random Early Detection (WRED) (if Enabled) | |
| exponential weight | Exponent used in the average queue size calculation for a WRED parameter group. |
| mean queue depth | Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a fluctuating average. The minimum and maximum thresholds are compared against this value to determine drop decisions. |
| class | IP precedence level. |

| Field | Description |
|---|---|
| Transmitted pkts/bytes | Number of packets (also shown in bytes) passed through WRED and not dropped by WRED.<br>**Note** If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped *after* the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as "no-buffer drops") are not taken into account by the WRED packet counter. |
| Random drop pkts/bytes | Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence level. |
| Tail drop pkts/bytes | Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence level. |
| Minimum thresh | Minimum threshold. Minimum WRED threshold in number of packets. |
| Maximum thresh | Maximum threshold. Maximum WRED threshold in number of packets. |
| Mark prob | Mark probability. Fraction of packets dropped when the average queue depth is at the maximum threshold. |
| Fields Associated with Traffic Shaping (if Enabled) | |
| Target Rate | Rate used for shaping traffic. |
| Byte Limit | Maximum number of bytes that can be transmitted per interval. Calculated as follows:<br>((Bc+Be) /8) x 1 |
| Sustain bits/int | Committed burst (Bc) rate. |
| Excess bits/int | Excess burst (Be) rate. |
| Interval (ms) | Time interval value in milliseconds (ms). |
| Increment (bytes) | Number of credits (in bytes) received in the token bucket of the traffic shaper during each time interval. |
| Queue Depth | Current queue depth of the traffic shaper. |

| Field | Description |
|---|---|
| Packets | Total number of packets that have entered the traffic shaper system. |
| Bytes | Total number of bytes that have entered the traffic shaper system. |
| Packets Delayed | Total number of packets delayed in the queue of the traffic shaper before being transmitted. |
| Bytes Delayed | Total number of bytes delayed in the queue of the traffic shaper before being transmitted. |
| Shaping Active | Indicates whether the traffic shaper is active. For example, if a traffic shaper is active, and the traffic being sent exceeds the traffic shaping rate, a “yes” appears in this field. |

## Related Commands

| Command | Description |
|---|---|
| **show policy-map interface** | Displays the statistics and the configurations of the input and output policies that are attached to an interface. |

# show policy-map mgre

To display statistics about a specific QoS policy as it is applied to a tunnel endpoint, use the **showpolicy-mapmgre**command in user EXEC or privileged EXEC mode.

**show policy-map mgre** [ *tunnel-interface-name* ] [*tunnel-destination overlay-address*]

## Syntax Description

| | |
|---|---|
| *tunnel-interface-name* | (Optional) Name of a tunnel interface. |
| *tunnel-destination overlay-address* | (Optional) Tunnel destination overlay address (such as the tunnel endpoint address). |

## Command Default

All existing policy map configurations are displayed.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(22)T | This command was introduced. |

## Usage Guidelines

You can specify the tunnel destination overlay address to display the output from a particular session.

## Examples

The following is sample output from the **showpolicy-mapmgre**command:

```
Router# show policy-map mgre tunnel 0 192.168.1.2
Tunnel0  <--> 192.168.1.2
  Service-policy output: set_out
    Class-map: test (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 101
      QoS Set
        precedence 3
          Packets marked 0
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

The table below describes the significant fields shown in the display.

*Table 237: show policy-map mgre Field Description*

| Field | Description |
|---|---|
| Tunnel0 | Name of the tunnel endpoint. |
| 192.168.1.2 | Tunnel destination overlay address. |
| Service-policy output | Name of the output service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets and bytes | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in kbps, of packets coming in to the class.<br>**Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only. |
| drop rate | Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate. |

| Field | Description |
|---|---|
| Match | Match criteria specified for the class of traffic. Choices include criteria such as IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental (EXP) value, access groups, and QoS groups. For more information about the variety of match criteria that are available, see the "Classifying Network Traffic" module in the *Cisco IOS Quality of Service Solutions Configuration Guide* . |
| QoS Set, qos-group, Packets marked | Indicates that class-based packet marking based on the QoS group has been configured. Includes the qos-group number and the number of packets marked. |

## Related Commands

| Command | Description |
|---|---|
| **ip nhrp group** | Configures a NHRP group on a spoke. |
| **ip nhrp map** | Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network. |
| **ip nhrp map group** | Adds NHRP groups to QoS policy mappings on a hub. |
| **show dmvpn** | Displays DMVPN-specific session information. |
| **show ip nhrp** | Displays NHRP mapping information. |
| **show ip nhrp group-map** | Displays the details of NHRP group mappings on a hub and the list of tunnels using each of the NHRP groups defined in the mappings. |

# show policy-map multipoint

To display the statistics about a specific quality of service (QoS) for a multipoint tunnel interface, use the **showpolicy-mapmultipoint**command in privileged EXEC mode.

**show policy-map multipoint** [**tunnel** *interface-number* [ *tunnel-destination-address* ]] [**input** [**class** *class-name*]] [**output** [**class** *class-name*]]

## Syntax Description

| | |
|---|---|
| **tunnel** | (Optional) Displays the tunnel interface. |
| *interface-number* | (Optional) Module and port number. |
| *tunnel-destination- address* | (Optional) Tunnel destination overlay address (such as the tunnel endpoint address). |
| **input** | (Optional) Indicates that the statistics for the attached input policy will be displayed. |
| **output** | (Optional) Indicates that the statistics for the attached output policy will be displayed. |
| **class** *class-name* | (Optional) Displays the QoS policy actions for the specified class. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(22)T | This command was introduced. |

## Usage Guidelines

Use the **showpolicy-mapmultipoint**command to display the quality of service (QoS) policy map for a multipoint tunnel interface.

## Examples

The following is sample output from the **showpolicy-mapmultipoint**command:

```
Router# show
policy-map multipoint
Interface Tunnel1 <--> 10.1.1.1
  Service-policy output: parent-policy-out
    Class-map: class-default (match-any)
      9839 packets, 869608 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
```

```
      Queueing
      queue limit 250 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 5000/710000
      shape (average) cir 1000000, bc 4000, be 4000
      target shape rate 1000000
      Service-policy : child-policy-out
        queue stats for all priority classes:
          Queueing
          queue limit 300 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 5000/710000
Interface Tunnel1 <--> 10.1.2.1
  Service-policy output: parent-policy-out
    Class-map: class-default (match-any)
      4723 packets, 479736 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 250 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 1000000, bc 4000, be 4000
      target shape rate 1000000
      Service-policy : child-policy-out
        queue stats for all priority classes:

          queue limit 300 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
```

## Related Commands

| Command | Description |
|---|---|
| **show platform qos policy-map** | Displays the type and number of policy maps that are configured on the router. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

# show policy-map session

To display the quality of service (QoS) policy map in effect for the Subscriber Service Switch (SSS) session, use the**showpolicy-mapsession**command in user EXEC or privileged EXEC mode.

**show policy-map session** [**uid** *uid-number*] [**input class** *class-name*| **output class** *class-name*]

## Syntax Description

| | |
|---|---|
| **uid** | (Optional) Defines a unique session ID. |
| *uid-number* | (Optional) Unique session ID. Range is from 1 to 65535. |
| **input** | (Optional) Displays the upstream traffic of the unique session. |
| **output** | (Optional) Displays the downstream traffic of the unique session. |
| **class** | (Optional) Identifies the class that is part of the QoS policy-map definition. |
| *class-name* | (Optional) Class name that is part of the QoS policy-map definition. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.3(8)T | This command was introduced. |
| 12.2(28)SB | This command was integrated into Cisco IOS Release 12.2(28)SB. This command was also modified to include per-session traffic shaping and traffic queueing statistics, if applicable. |
| 12.2(33)SRC | This command was integrated into Cisco IOS Release 12.2(33)SRC, and support for the Cisco 7600 series router was added. |
| 12.2(33)SB | Support for the Cisco 7300 series router was added. This command was also modified to include traffic shaping overhead accounting for ATM statistics, if applicable. |

## Usage Guidelines

Use the **showpolicy-mapsession** command with the **uid** keyword to verify the QoS policy map of a unique session ID in the input and output streams in the SSS session. Use the **showpolicy-mapsession** command with the optional **class***class-name*keywordargument combination to display statistics for a particular class. If you use the **showpolicy-mapsession** command without the **class***class-name*keyword argument combination, statistics for all the classes defined in the QoS policy map display.

## Examples

This section contains sample output from the **showpolicy-mapsession** command.

**Note** The output of the **showpolicy-mapsession** command varies according to the QoS feature configured in the policy map. For instance, if traffic shaping or traffic queueing is configured in the policy maps, the statistics for those features will be included and the output will vary accordingly from what is shown in this section. Additional self-explanatory fields may appear, but the output will be very similar.

The following example from the **showpolicy-mapsession** command displays QoS policy-map statistics for traffic in the downstream direction for the QoS policy maps configured:

```
Router# show policy-map session uid 401 output
 SSS session identifier 401 -
  Service-policy output: downstream-policy
    Class-map: customer1234 (match-any)
      4464 packets, 249984 bytes
      5 minute offered rate 17000 bps, drop rate 0 bps
      Match: ip dscp cs1  cs2  cs3  cs4
        4464 packets, 249984 bytes
        5 minute rate 17000 bps
      QoS Set
        dscp af11
          Packets marked 4464
    Class-map: customer56 (match-any)
      2232 packets, 124992 bytes
      5 minute offered rate 8000 bps, drop rate 0 bps
      Match: ip dscp cs5  cs6
        2232 packets, 124992 bytes
        5 minute rate 8000 bps
      police:
          cir 20000 bps, bc 10000 bytes
          pir 40000 bps, be 10000 bytes
        conformed 2232 packets, 124992 bytes; actions:
          set-dscp-transmit af21
        exceeded 0 packets, 0 bytes; actions:
          set-dscp-transmit af22
        violated 0 packets, 0 bytes; actions:
          set-dscp-transmit af23
        conformed 8000 bps, exceed 0 bps, violate 0 bps
    Class-map: customer7 (match-any)
      1116 packets, 62496 bytes
      5 minute offered rate 4000 bps, drop rate 4000 bps
      Match: ip dscp cs7
        1116 packets, 62496 bytes
        5 minute rate 4000 bps
      drop
    Class-map: class-default (match-any)
      1236 packets, 68272 bytes
      5 minute offered rate 4000 bps, drop rate 0 bps
      Match: any
```

The table below describes the significant fields shown in the display.

*Table 238: show policy-map session Field Descriptions -- Traffic in the Downstream Direction*

| Field | Description |
|---|---|
| SSS session identifier | Unique session identifier. |
| Service-policy output | Name of the output service policy applied to the specified interface or virtual circuit (VC). |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets and bytes | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in bps, of packets coming in to the class.<br>**Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation [GRE] tunnel and an IP Security [IPsec] tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPsec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only. |
| drop rate | Rate, in bps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate. |

| Field | Description |
|---|---|
| Match | Match criteria specified for the class of traffic. Choices include criteria such as IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental (EXP) value, access groups, and QoS groups. For more information about the variety of availablematch criteria options, see the "Applying QoS Features Using the MQC" module of the *Cisco IOS Quality of Service Solutions Configuration Guide* . |
| QoS Set | Indicates that packet marking is in place. |
| dscp | Value used in packet marking. |
| Packets marked | The number of packets marked. |
| police | Indicates that the **police** command has been configured to enable traffic policing. Also, displays the specified committed information rate (CIR), conform burst (bc) size, peak information rate (PIR), and peak burst (be) size used for marking packets. |
| conformed | Displays the action to be taken on packets that conform to a specified rate. Displays the number of packets and bytes on which the action was taken. |
| exceeded | Displays the action to be taken on packets that exceed a specified rate. Displays the number of packets and bytes on which the action was taken. |
| violated | Displays the action to be taken on packets that violate a specified rate. Displays the number of packets and bytes on which the action was taken. |

The following example from the **showpolicy-mapsession**command displays QoS policy-map statistics for traffic in the upstream direction for all the QoS policy maps configured:

```
Router# show policy-map
 session
 uid
 401
 input
 SSS session identifier 401 -
  Service-policy input: upstream-policy
    Class-map: class-default (match-any)
      1920 packets, 111264 bytes
      5 minute offered rate 7000 bps, drop rate 5000 bps
      Match: any
      police:
          cir 8000 bps, bc 1500 bytes
        conformed 488 packets, 29452 bytes; actions:
          transmit
```

```
exceeded 1432 packets, 81812 bytes; actions:
  drop
conformed 7000 bps, exceed 5000 bps
```

The table below describes the significant fields shown in the display.

***Table 239: show policy-map session Field Descriptions -- Traffic in the Upstream Direction***

| Field | Description |
|---|---|
| SSS session identifier | Unique session identifier. |
| Service-policy input | Name of the input service policy applied to the specified interface or VC. |
| Class-map | Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class. |
| packets and bytes | Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed. |
| offered rate | Rate, in bps, of packets coming in to the class.<br>**Note** If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified *before* they enter a combination of tunnels (for example, a generic routing encapsulation [GRE] tunnel and an IP Security [IPsec] tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only *one* tunnel encapsulation, or may include the overhead for *all* tunnel encapsulations. In most of the GRE and IPsec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only. |
| drop rate | Rate, in bps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate. |

| Field | Description |
|---|---|
| Match | Match criteria specified for the class of traffic. Choices include criteria such as IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental (EXP) value, access groups, and QoS groups. For more information about the variety of available match criteria options, see the "Applying QoS Features Using the MQC" module of the *Cisco IOS Quality of Service Solutions Configuration Guide* . |
| police | Indicates that the **police** command has been configured to enable traffic policing. Also, displays the specified committed information rate (CIR), conform burst (bc) size, peak information rate (PIR), and peak burst (be) size used for marking packets. |
| conformed | Displays the action to be taken on packets that conform to a specified rate. Displays the number of packets and bytes on which the action was taken. |
| exceeded | Displays the action to be taken on packets that exceed a specified rate. Displays the number of packets and bytes on which the action was taken. |
| violated | Displays the action to be taken on packets that violate a specified rate. Displays the number of packets and bytes on which the action was taken. |

## Examples

The following is sample output of the **showpolicy-mapsession** command when per-session traffic shaping and traffic queueing are enabled. With per-session traffic shaping and queueing configured, traffic shaping and traffic queueing statistics are included in the output.

**Note** The QoS: Per-Session Shaping and Queueing on LNS feature does not support packet marking. That is, this feature does not support the use of the **set** command to mark packets. Therefore, statistics related to packet marking are not included in the output.

```
Router# show policy-map session
uid 1 output
 SSS session identifier 1 -
  Service-policy output: parent
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets, 0 bytes
        30 second rate 0 bps
      Queueing
      queue limit 128 packets
```

```
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 512000, bc 12800, be 12800
      target shape rate 512000
      Service-policy : child
        Class-map: prec0 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 0
          Queueing
          queue limit 38 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          bandwidth 30% (153 kbps)
  Class-map: prec2 (match-all)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: ip precedence 2
          Queueing
          queue limit 44 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
          shape (average) cir 212000, bc 7632, be 7632
          target shape rate 212000
        Class-map: class-default (match-any)
          0 packets, 0 bytes
          30 second offered rate 0 bps, drop rate 0 bps
          Match: any
            0 packets, 0 bytes
            30 second rate 0 bps
          queue limit 44 packets
          (queue depth/total drops/no-buffer drops) 0/0/0
          (pkts output/bytes output) 0/0
```

The table below describes the significant fields related to per-session traffic shaping and queueing shown in the display.

***Table 240: show policy-map session Field Descriptions--Per-Session Traffic Shaping and Queueing Configured***

| Field | Description |
|---|---|
| Queueing | Indicates that traffic queueing is enabled. |
| queue limit | Displays the queue limit, in packets. |
| queue depth | Current queue depth of the traffic shaper. |
| shape (average) cir, bc, be | Indicates that average rate traffic shaping is enabled. Displays the committed information rate (CIR), the committed burst (bc) rate, and the excess burst (be) rate in bytes. |
| target shape rate | Displays the traffic shaping rate, in bytes. |

Traffic Shaping Overhead Accounting for ATM: Example

The following output from the show policy-map session command indicates that ATM overhead accounting is enabled for shaping.

```
Router# show policy-map session
uid 2
output
```

```
SSS session identifier 2 -
Service-policy output:  ATM_OH_POLICY
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0 bps, drop rate 0 bps
      Match: any
      Queueing
      queue limit 2500 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 10000000, bc 40000, be 40000
      target shape rate 10000000
       Overhead Accounting Enabled
```

The table below describes the significant fields displayed.

***Table 241: show policy-map session Field Descriptions--Traffic Shaping Overhead Accounting for ATM Configured***

| Field | Description |
|---|---|
| target shape rate | Displays the traffic shaping rate, in bytes. |
| Overhead Accounting Enabled | Indicates that overhead accounting is enabled. |

## Related Commands

| Command | Description |
|---|---|
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |
| **show sss session** | Displays SSS session status. |

# show policy-map target service-group

To display the policy-map information about service groups comprising Ethernet Virtual Circuits (EVCs), sub interfaces or sessions as members on the main interface or port channel, use the **showpolicy-maptargetservice-group** command in privileged EXEC mode.

**show policy-map target service-group** [*service-group-identifier*]

## Syntax Description

| | |
|---|---|
| *service-group-identifier* | Service group identification number. |

## Command Default

Policy-map information for all existing service groups is displayed.

## Command Modes

Privileged EXEC(#)

## Command History

| Release | Modification |
|---|---|
| 15.1(1)S | This command is introduced. |

## Usage Guidelines

You should create the service groups and policy maps before using this command.

## Examples

This is a sample output of the **showpolicy-maptargetservice-group**command.

```
Router# show policy-map target service-group 1000
Port-channel1: Service Group 1000
Service-policy output: policy1
Counters last updated 02:04:11 ago
Class-map: class-default (match-any)
      0 packets, 0 bytes
      30 second offered rate 0000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 768 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 0/0
      shape (average) cir 20000000, bc 80000, be 80000
      target shape rate 20000000
```

The table below describes the fields shown in the **showpolicy-maptargetservice-group**command.

***Table 242: Field Descriptions***

| Field | Description |
|---|---|
| Port-channel: Service Group | Specifies the interface type and service-group number. |
| Service-policy output | Specifies the output service-policy name. |

| Field | Description |
|---|---|
| Class-map | Specifies the class of traffic. |
| Queuing | Indicates that a traffic queuing mechanism is enabled. Statistics for traffic queuing are also displayed. |

## Related Commands

| Command | Description |
|---|---|
| **show policy-map interface** | Displays the statistics and the configurations of the input and output policies that are attached to an interface. |
| **show policy-map interface service instance** | Displays the policy-map information for a given service instance under an interface or port-channel. |

# show policy-map type access-control

To display the access control for a specific policy map, use the **showpolicy-maptypeaccess-control**command in privileged EXEC mode.

**show policy-map type access-control** [[*policy-map-name* [**class** *class-map-name*]| **apn** *index-number*] **control-plane** [**all**| **subinterface**] [**input** [**class** *class-map-name*]| **output** [**class** *class-map-name*]]| **interface** *type number* [**vc** *vpivci*| **vp** *vpi* [ *subinterface* ]| **input** [**class** *class-map-name*]| **output** [**class** *class-map-name*]] **session** [**uid** *id*] [**input** [**class** *class-map-name*]| **output** [*class class-map-name*]]]

### Cisco ASR 1000 Series

**show policy-map type access-control** [**control-plane** [**all** [**brief** {**timestamp**| **vrfs timestamp**}| **class** *class-map-name*| **service-instance** [ *target-identifier* ]]| **interface** [*type number* [**service-instance** [ *target-identifier* ]]]| **session** [**uid [id]**] [**input** [**class** *class-map-name*]| **output class** [ *class-map-name* ]]]]

## Syntax Description

| | |
|---|---|
| *policy-map name* | (Optional) Policy-map name. |
| **class** *class-map-name* | (Optional) Displays the Quality of Service (QoS) policy actions for the specified class. |
| **apn** *index-number* | (Optional) Displays information about the Access Point Name (APN)-related policy. |
| **control-plane** | (Optional) Displays information about control plane policy. |
| **all** | (Optional) Displays all control plane policies. |
| **subinterface** | (Optional) Displays statistics and policy details for an individual class for one of the following subinterfaces: **cef-exception**, **host**, **transit**. |
| **input** | (Optional) Indicates that the statistics for the attached input policy are displayed. |
| output | (Optional) Indicates that the statistics for the attached output policy are displayed. |
| **interface** [*typenumber*] | (Optional) Displays information about the Cisco IOS QoS policy interface. |
| **vc** | (Optional) Displays the service policy for a specified virtual channel (VC). |

| | |
|---|---|
| *vpi* / | (Optional) Virtual path identifier (VPI) for this permanent virtual circuit (PVC). The absence of the slash mark ("/") and a VPI value defaults the VPI value to 0. On the Cisco 7200 and 7500 series routers, this value ranges from 0 to 255. The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0. |
| *vci* | (Optional) Virtual channel identifier (VCI) for this PVC. This value ranges from 0 to 1 less than the maximum value set for this interface by the **atmvc-per-vp** command. Typically, lower values 0 to 31 are reserved for specific traffic (F4 Operation, Administration, and Maintenance (OAM), switched virtual circuit (SVC) signaling, Integrated Local Management Interface (ILMI), and so on) and should not be used. |
| **session** | (Optional) Displays information about the session QoS policy. |
| **uid** [*id*] | (Optional) Displays the session user identifier (uid) for a policy map based on the Subscriber Service Switch (SSS) unique identifier. |
| **brief** | (Optional) Dispays a brief description of policy maps. |
| **timestamp** | Displays time when the policy map was attached to the interface. |
| **vrfs** | Displays information about the interface associated with a virtual private network (VPN). |
| **service instance** | (Optional) Displays information about the service instance for an interface. |
| *target-identifier* | (Optional) Target identifier for a service instance. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(22)T | This command was introduced. |
| Cisco IOS XE Release 2.1 | This command was implemented on Cisco ASR Aggregation Services 1000 series routers. |

| Release | Modification |
|---|---|
| 15.0(1)M | The command was modified. The output was modified to display encrypted filter information. |

## Usage Guidelines

Use this command to display the access control for a specific policy-map.

## Examples

The following is sample output from the **showpolicy-maptypeaccess-control**command. The fields are self-explanatory.

```
Router# show policy-map type access-control
Policy Map type access-control tcp_policy
    Class psirt1 (encrypted FPM filter)
      drop
    Class psirt2 (encrypted FPM filter)
      drop
    Class psirt11 (encrypted FPM filter)
      drop
  Policy Map type access-control udp_policy
    Class slammer
      drop
  Policy Map type access-control fpm-policy
    Class ip_tcp_stack
      service-policy tcp_policy
    Class ip_udp_stack
      service-policy udp_policy
```

## Related Commands

| Command | Description |
|---|---|
| **show platform qos policy-map** | Displays the type and number of policy maps that are configured on the router. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

# show policy-map type nat

To display the policy-map for Network Address Translation (NAT), use the **showpolicy-maptypeNAT** command in privileged EXEC mode.

**show policy-map nat** *policymap-name*
[**class** *classmap-name*]
|**apn** *index-number* | **interface** *type-number*
[**input class** *classmap-name*]
|**outputclass** *classmap-name*
[**session uid** *id*]
**input** [**class** *classmap-name*] | **output class** *classmap-name*

## Syntax Description

| | |
|---|---|
| *policymap-name* | (Optional) Policy-map name. |
| **class** *classmap-name* | (Optional) Displays the QoS policy actions for the specified class. |
| **apn** *index-number* | (Optional) Displays Access Point Name (APN) related policy information. |
| **interface** [*typenumber*] | (Optional) Displays Cisco IOS Quality of Service (QoS) Policy Interface information . |
| **session** | (Optional) Displays session QoS Policy information. |
| **uid** [*id*] | Displays session user identifier (uid) for a policy-map based on the Subscriber Service Switch (SSS) unique identifier. |
| **input** | (Optional) Indicates that the statistics for the attached input policy is displayed. |
| output | (Optional) Indicates that the statistics for the attached output policy is displayed. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(11)T | This command was introduced. |

## Examples

The following is sample output from the **showpolicy-maptypeNAT**command:

```
Router# show policy-map type NAT
Policy Map ipnat-policyxx-in2out
Class ipnat-default
Class ipnat-class-acl-1
Class ipnat-class-acl-2
Class ipnat-class-acl-3
Policy Map ipnat-policyxx-out2in
Class ipnat-default
```

## Related Commands

| Command | Description |
|---|---|
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |
| **show platform qos policy-map** | Displays the type and number of policy maps that are configured on the router. |

# show policy-map type port-filter

To display information about policing of packets going to closed or nonlistened TCP/UDP ports, use the **showpolicy-maptypeport-filter**command in privileged EXEC mode.

**show queue** *interface-name interface-number queue-number* **vc** *vc vpi/vci*

## Syntax Description

| | |
|---|---|
| *policy-map-name* | (Optional) Policy-map name. |
| **class** *class-map-name* | (Optional) Displays the QoS policy actions for the specified class. |
| **apn** *index-number* | (Optional) Displays Access Point Name (APN) related policy information. |
| **control-plane** | (Optional) Displays information about control plane policy. |
| **all** | (Optional) Displays all control plane policies. |
| **subinterface** | (Optional) Displays statistics and policy details for an individual class for one of the following subinterfaces: **cef-exception**, **host**, **transit**. |
| **interface** [*typenumber*] | (Optional) Displays Cisco IOS QoS policy interface information. |
| | (Optional) Displays the service policy for a specified virtual channel (VC). |
| *vpi* **/**<br>**vc** | (Optional) virtual path identifier (VPI) for this PVC. The absence of the "/" and a vpi value defaults the vpi value to 0. On the Cisco 7200 and 7500 series routers, this value ranges from 0 to 255. The vpi and vci arguments cannot both be set to 0; if one is 0, the other cannot be 0. |
| *vci* | (Optional) virtual channel identifier (VCI) for this PVC. This value ranges from 0 to 1 less than the maximum value set for this interface by the atm vc-per-vp command. Typically, lower values 0 to 31 are reserved for specific traffic (F4 Operation, Administration, and Maintenance (OAM), switched virtual circuit (SVC) signalling, Integrated Local Management Interface (ILMI), and so on) and should not be used. |

| | |
|---|---|
| **vp** | Optional) Displays the service policy for a specified virtual path (VP). |
| **session** | (Optional) Displays session QoS Policy information. |
| **uid** [*id*] | Displays the session user identifier (uid) for a policy map based on the Subscriber Service Switch (SSS) unique identifier. |
| **input** | (Optional) Indicates that the statistics for the attached input policy is displayed. |
| output | (Optional) Indicates that the statistics for the attached output policy is displayed. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(22)T | This command was introduced. |

## Usage Guidelines

Port filtering feature allows policing of packets going to closed or nonlistened TCP/UDP ports, while queue thresholding limits the number of packets for a specified protocol that is allowed in the control-plane IP input queue.

## Examples

The following example shows sample output for the **showpolicy-maptypeport-filter**command.

```
Router# show policy-map type port-filter
Policy Map type port-filter p1
Policy Map type port-filter p4
```

## Related Commands

| Command | Description |
|---|---|
| **show platform qos policy-map** | Displays the type and number of policy maps that are configured on the router. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |

| Command | Description |
|---|---|
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |

# show protocol phdf

To display protocol information from a specific protocol header description file (PHDF), use the **showprotocolphdf**command in privileged EXEC mode.

**show protocol phdf** *protocol-name*

## Syntax Description

| | |
|---|---|
| *protocol-name* | Loaded PHDF. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.4(4)T | This command was introduced. |
| 12.2(18)ZY | This command integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA). |

## Examples

The following example shows how to define FPM traffic classes for slammer packets (UDP port 1434). The match criteria defined within the class maps is for slammer packets with an IP length not to exceed 404 bytes, UDP port 1434, and pattern 0x4011010 at 224 bytes from start of IP header. This example also shows how to define the service policy “fpm-policy” and apply it to the gigabitEthernet interface. Show commands have been issued to verify the FPM configuration. (Note that PHDFs are not displayed in show output because they are in XML format.)

```
Router(config)# load protocol disk2:ip.phdf
Router(config)# load protocol disk2:udp.phdf
Router(config)# class-map type stack match-all ip-udp
Router(config-cmap)# description “match UDP over IP packets”
Router(config-cmap)# match field ip protocol eq 0x11 next udp
Router(config)# class-map type access-control match-all slammer
Router(config-cmap)# description “match on slammer packets”
Router(config-cmap)# match field udp dest-port eq 0x59A
Router(config-cmap)# match field ip length eq 0x194
Router(config-cmap)# match start 13-start offset 224 size 4 eq 0x4011010
Router(config)# policy-map type access-control fpm-udp-policy
Router(config-pmap)# description “policy for UDP based attacks”
Router(config-pmap)# class slammer
Router(config-pmap-c)# drop
Router(config)# policy-map type access-control fpm-policy
Router(config-pmap)# description “drop worms and malicious attacks”
Router(config-pmap)# class ip-udp
Router(config-pmap-c)# service-policy fpm-udp-policy
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input fpm-policy
Router# show protocols phdf ip
Protocol ID: 1
```

```
Protocol name: IP
Description: Definition-for-the-IP-protocol
Original file name: disk2:ip.phdf
Header length: 20
Constraint(s):
Total number of fields: 12
Field id: 0, version, IP-version
Fixed offset. offset 0
Constant length. Length: 4
Field id: 1, ihl, IP-Header-Length
Fixed offset. offset 4
Constant length. Length: 4
Field id: 2, tos, IP-Type-of-Service
Fixed offset. offset 8
Constant length. Length: 8
Field id: 3, length, IP-Total-Length
Fixed offset. offset 16
Constant length. Length: 16
Field id: 4, identification, IP-Identification
Fixed offset. offset 32
Constant length. Length: 16
Field id: 5, flags, IP-Fragmentation-Flags
Fixed offset. offset 48
Constant length. Length: 3
Field id: 6, fragment-offset, IP-Fragmentation-Offset
Fixed offset. offset 51
Constant length. Length: 13
Field id: 7, ttl, Definition-for-the-IP-TTL
Fixed offset. offset 64
Constant length. Length: 8
Field id: 8, protocol, IP-Protocol
Fixed offset. offset 72
Constant length. Length: 8
Field id: 9, checksum, IP-Header-Checksum
Fixed offset. offset 80
Constant length. Length: 16
Field id: 10, source-addr, IP-Source-Address
Fixed offset. offset 96
Constant length. Length: 32
Field id: 11, dest-addr, IP-Destination-Address
Fixed offset. offset 128
Constant length. Length: 32
Router# show protocols phdf udp
Protocol ID: 3
Protocol name: UDP
Description: UDP-Protocol
Original file name: disk2:udp.phdf
Header length: 8
Constraint(s):
Total number of fields: 4
Field id: 0, source-port, UDP-Source-Port
Fixed offset. offset 0
Constant length. Length: 16
Field id: 1, dest-port, UDP-Destination-Port
Fixed offset. offset 16
Constant length. Length: 16
Field id: 2, length, UDP-Length
Fixed offset. offset 32
Constant length. Length: 16
Field id: 3, checksum, UDP-Checksum
Fixed offset. offset 48
Constant length. Length: 16
```

## Related Commands

| Command | Description |
|---|---|
| **load protocol** | Loads a PHDF onto a router. |

# show qbm client

To display quality of service (QoS) bandwidth manager (QBM) clients (applications) and their IDs, use the **showqbmclient**command in user EXEC or privileged EXEC mode.

**show qbm client**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRC | This command was introduced. |
| Cisco IOS XE Releas 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

Use the **showqbmclient** command to confirm that a subset of Cisco IOS software has registered with QBM.

A subset of Cisco IOS software becomes a client of QBM by calling a QBM registration application programming interface (API) and receiving an ID. If the subset has not registered, then it is not a client.

## Examples

The following is sample output from the**showqbmclient** command when RSVP aggregation is enabled:

```
Router# show qbm client
Client Name                             Client ID
RSVP BW Admit                           1
RSVP rfc3175 AggResv                    2
```

The table below describes the significant fields shown in the display.

*Table 243: show qbm client command Field Descriptions*

| Field | Description |
|---|---|
| Client Name | The name of the application.<br>• RSVP BW Admit--The RSVP QBM client used for admitting bandwidth into QBM bandwidth pools.<br>• RSVP rfc3175 AggResv--RSVP aggregation as defined in RFC 3175, *AggregationofRSVPforIPv4andIPv6Reservations*.<br>• This client is used to create and maintain QBM bandwidth pools for RSVP aggregate reservations. |
| Client ID | The identifier of the application. One client ID exists per client. |

## Related Commands

| Command | Description |
|---|---|
| **debug qbm** | Enables debugging output for QBM options. |
| **show qbm pool** | Displays allocated QBM pools and associated objects. |

# show qbm pool

To display allocated quality of service (QoS) bandwidth manager (QBM) pools and identify the objects with which they are associated, use the **showqbmpool** command in user EXEC or privileged EXEC mode.

**show qbm pool** [**id** *pool-id*]

## Syntax Description

| | |
|---|---|
| **id** *pool-id* | (Optional) Displays the identifier for a specified bandwidth pool that is performing admission control. The values must be between 0x0 and 0xffffffff; there is no default. |

## Command Default

If you enter the **showqbmpool**command without the optional keyword/argument combination, the command displays information for all configured QBM pools.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRC | This command was introduced. |
| Cisco IOS XE Release 2.6 | This command was integrated into Cisco IOS XE Release 2.6. |

## Usage Guidelines

Use the **showqbmpool** command to display information for all configured QBM pools or for a specified pool. If you enter a pool ID that does not exist, you receive an error message.

This command is useful for troubleshooting QBM operation.

## Examples

The following sample output is from the **showqbmpool** command when RSVP aggregation is enabled:

```
Router# show qbm pool
Total number of pools allocated:  1
Pool ID 0x00000009
Associated object:  'RSVP 3175 AggResv 192.168.40.1->192.168.50.1_ef(46)'
  Minimum:         300Kbps
  Oper Status:     OPERATIONAL
  Oper Minimum:    300Kbps
Used Bandwidth:  80Kbps
```

The table below describes the significant fields shown in the display.

*Table 244: show qbm pool command Field Descriptions*

| Field | Description |
|---|---|
| Total number of pools allocated | The number of QBM pools configured. |
| Pool ID | The QBM pool identifier. |
| Associated object | The application (or client) associated with the QBM pool. This string is provided by the client and as a result, the client chooses the string, not QBM. For example, RSVP 3175 AggResv 192.168.40.1->192.168.50.1_ef(46) means the QBM pool is associated with the RSVP aggregate reservation with source endpoint (aggregator) having IP address 192.168.40.1, destination endpoint (deaggregator) having IP address 192.168.50.1, and differentiated services code point (DSCP) expedited forwarding (EF). |
| Minimum | The pool's minimum bandwidth guarantee. (Units may vary.) |
| Oper Status | Status of the application. Values are the following:<br>• OPERATIONAL--Application is enabled.<br>• NON-OPERATIONAL--Application is disabled. |
| Oper Minimum | Defines the minimum bandwidth guarantee that the pool is able to enforce. This value may differ from the pool's minimum bandwidth guarantee because of operational conditions. For example, if the pool is associated with an interface and the interface is down, its Oper Status is NON-OPERATIONAL, then the operational minimum is N/A. |
| Used Bandwidth | The bandwidth reserved by applications/clients using this pool. N/A displays instead of 0 when the pool's Oper Status is NON-OPERATIONAL. |

The following sample output is from the **showqbmpool** command with a specified pool ID:

```
Router# show qbm pool id 0x000000006
Pool ID 0x00000009
Associated object:  'RSVP 3175 AggResv 192.168.40.1->192.168.50.1_ef(46)'
  Minimum:         300Kbps
  Oper Status:     OPERATIONAL
  Oper Minimum:    300Kbps
Used Bandwidth:  80Kbps
```

See the table above for a description of the fields.

## Related Commands

| Command | Description |
|---|---|
| **debug qbm** | Enables debugging output for QBM options. |
| **show qbm client** | Displays registered QBM clients. |

# show qdm status

To display the status of the active Quality of Service Device Manager (QDM) clients that are connected to the router, use the **showqdmstatus** command in EXEC mode.

**show qdm status**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.1(1)E | This command was introduced. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

## Usage Guidelines

The **showqdmstatus** command can be used on the Cisco 7600 series router.

The output of the **showqdmstatus**command includes the following information:

- Number of connected clients
- Client IDs
- Version of the client software
- IP addresses of the connected clients
- Duration of the connection

**Note** QDM is not supported on Optical Service Module (OSM) interfaces.

## Examples

The following example illustrates the **showqdmstatus**output when two QDM clients are connected to the router:

```
Router# show qdm status
Number of QDM Clients :2
QDM Client v1.0(0.13)-System_1 @ 172.16.0.0 (id:30)
     connected since 09:22:36 UTC Wed Mar 15 2000
QDM Client v1.0(0.12)-System_2 @ 172.31.255.255 (id:29)
     connected since 17:10:23 UTC Tue Mar 14 2000
```

## Related Commands

| Command | Description |
|---|---|
| **disconnect qdm** | Disconnects a QDM client. |

# show queue

**Note** Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **showqueue**command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

**Note** Effective with Cisco IOS XE Release 3.2S, the **showqueue**command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* .

To display the contents of packets inside a queue for a particular interface or virtual circuit (VC), use the **showqueue**command in user EXEC or privileged EXECmode.

**show queue** *interface-name interface-number* [**queue-number**][ **vc vpi/ vci**]

## Syntax Description

| | |
|---|---|
| *interface-name* | The name of the interface. |
| *interface-number* | The number of the interface. |
| *queue-number* | (Optional) The number of the queue. The queue number is a number from 1 to 16. |
| **vc** | (Optional) For ATM interfaces only, shows the fair queueing configuration for a specified permanent virtual circuit (PVC). The name can be up to 16 characters long. |
| *vpi* / | (Optional) ATM network virtual path identifier (VPI) for this PVC. The absence of the "/" and a *vpi* value defaults the *vpi* value to 0.<br>On the Cisco 7200 and Cisco 7500 series routers, this value ranges from 0 to 255.<br>The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0.<br>If this value is omitted, information for all VCs on the specified ATM interface or subinterface is displayed. |

| | |
|---|---|
| *vci* | (Optional) ATM network virtual channel identifier (VCI) for this PVC. This value ranges from 0 to 1 less than the maximum value set for this interface by the **atmvc-per-vp** command. Typically, lower values 0 to 31 are reserved for specific traffic (F4 Operation, Administration, and Maintenance (OAM), switched virtual circuit (SVC) signalling, Integrated Local Management Interface (ILMI), and so on) and should not be used.<br>The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only.<br>The *vpi* and *vci* arguments cannot both be set to 0; if one is 0, the other cannot be 0. |

**Command Modes**

User EXEC (>) Privileged EXEC (#)

**Command History**

| Release | Modification |
|---|---|
| 10.2 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T, but without support for hierarchical queueing framework (HQF). See the "Usage Guidelines" for additional information. |
| Cisco IOS XE Release 2.6 | This command was modified. This command was hidden. |
| 15.0(1)S | This command was modified. This command was hidden. |
| 15.1(3)T | This command was modified. This command was hidden. |
| Cisco IOS XE Release 3.2S | This command was replaced by an MQC command (or sequence of MQC commands). |

**Usage Guidelines**

This command displays the contents of packets inside a queue for a particular interface or VC.

This command does not support VIP-distributed Weighted Random Early Detection WRED (DWRED). You can use the **vc** keyword and the **showqueue** command arguments to display output for a PVC only on Enhanced ATM port adapters (PA-A3) that support per-VC queueing.

This command does not support HQF. Use the **showpolicy-map** and the **showpolicy-mapinterface** commands to gather HQF information and statistics.

## Examples

The following examples show sample output when the **showqueue** command is entered and either weighted fair queueing (WFQ), WRED, or flow-based WRED are configured.

## Examples

The following is sample output from the **showqueue**command for PVC 33 on the atm2/0.33 ATM subinterface. Two conversations are active on this interface. WFQ ensures that both data streams receive equal bandwidth on the interface while they have messages in the pipeline.

```
Router# show queue
 atm2/0.33 vc 33
Interface ATM2/0.33 VC 0/33
  Queueing strategy: weighted fair
  Total output drops per VC: 18149
  Output queue: 57/512/64/18149 (size/max total/threshold/drops)
     Conversations  2/2/256 (active/max active/max total)
     Reserved Conversations 3/3 (allocated/max allocated)
  (depth/weight/discards/tail drops/interleaves) 29/4096/7908/0/0
  Conversation 264, linktype: ip, length: 254
  source: 10.1.1.1, destination: 10.0.2.20, id: 0x0000, ttl: 59,
  TOS: 0 prot: 17, source port 1, destination port 1
  (depth/weight/discards/tail drops/interleaves) 28/4096/10369/0/0
  Conversation 265, linktype: ip, length: 254
  source: 10.1.1.1, destination: 10.0.2.20, id: 0x0000, ttl: 59,
  TOS: 32 prot: 17, source port 1, destination port 2
```

The table below describes the significant fields shown in the display.

***Table 245: show queue Field Descriptions for WFQ***

| Field | Description |
|---|---|
| Queueing strategy | Type of queueing active on this interface. |
| Total output drops per VC | Total output packet drops. |
| Output queue | Output queue size, in packets. Max total defines the aggregate queue size of all the WFQ flows. Threshold is the individual queue size of each conversation. Drops are the dropped packets from all the conversations in WFQ. |
| Conversations | WFQ conversation number. A conversation becomes inactive or times out when its queue is empty. Each traffic flow in WFQ is based on a queue and represented by a conversation. Max active is the number of active conversations that have occurred since the queueing feature was configured. Max total is the number of conversations allowed simultaneously. |

| Field | Description |
|---|---|
| Reserved Conversations | Traffic flows not captured by WFQ, such as class-based weighted fair queueing (CBWFQ) configured by the bandwidth command or a Resource Reservation Protocol (RSVP) flow, have a separate queue that is represented by a reserved conversation. Allocated is the current number of reserved conversations. Max allocated is the maximum number of allocated reserved conversations that have occurred. |
| depth | Queue depth for the conversation, in packets. |
| weight | Weight used in WFQ. |
| discards | Number of packets dropped from the conversation's queue. |
| tail drops | Number of packets dropped from the conversation when the queue is at capacity. |
| interleaves | Number of packets interleaved. |
| linktype | Protocol name. |
| length | Packet length. |
| source | Source IP address. |
| destination | Destination IP address. |
| id | Packet ID. |
| ttl | Time to live count. |
| TOS | IP type of service. |
| prot | Layer 4 protocol number. |

## Examples

The following is sample output from the **showqueue** command issued for serial interface 1 on which flow-based WRED is configured. The output shows information for each packet in the queue; the data identifies the packet by number, the flow-based queue to which the packet belongs, the protocol used, and so forth.

```
Router# show queue Serial1
   Output queue for Serial1 is 2/0

   Packet 1, flow id:160, linktype:ip, length:118, flags:0x88
     source:10.1.3.4, destination:10.1.2.2, id:0x0000, ttl:59,
     TOS:32 prot:17, source port 1, destination port 515
```

```
      data:0x0001 0x0203 0x0405 0x0607 0x0809 0x0A0B 0x0C0D
            0x0E0F 0x1011 0x1213 0x1415 0x1617 0x1819 0x1A1B

   Packet 2, flow id:161, linktype:ip, length:118, flags:0x88
     source:10.1.3.5, destination:10.1.2.2, id:0x0000, ttl:59,
     TOS:64 prot:17, source port 1, destination port 515
       data:0x0001 0x0203 0x0405 0x0607 0x0809 0x0A0B 0x0C0D
            0x0E0F 0x1011 0x1213 0x1415 0x1617 0x1819 0x1A1B
```

The table below describes the significant fields shown in the display.

***Table 246: show queue Field Descriptions for Flow-Based WRED***

| Field | Description |
|---|---|
| Packet | Packet number. |
| flow id | Flow-based WRED number. |
| linktype | Protocol name. |
| length | Packet length. |
| flags | Internal version-specific flags. |
| source | Source IP address. |
| destination | Destination IP address. |
| id | Packet ID. |
| ttl | Time to live count. |
| prot | Layer 4 protocol number. |
| data | Packet data. |

## Examples

The following is sample output from the **showqueue**command issued for serial interface 3 on which WRED is configured. The output has been truncated to show only 2 of the 24 packets.

```
Router# show queue Serial3
   Output queue for Serial3 is 24/0

   Packet 1, linktype:ip, length:118, flags:0x88
     source:10.1.3.25, destination:10.1.2.2, id:0x0000, ttl:59,
     TOS:192 prot:17, source port 1, destination port 515
       data:0x0001 0x0203 0x0405 0x0607 0x0809 0x0A0B 0x0C0D
            0x0E0F 0x1011 0x1213 0x1415 0x1617 0x1819 0x1A1B

   Packet 2, linktype:ip, length:118, flags:0x88
     source:10.1.3.26, destination:10.1.2.2, id:0x0000, ttl:59,
     TOS:224 prot:17, source port 1, destination port 515
       data:0x0001 0x0203 0x0405 0x0607 0x0809 0x0A0B 0x0C0D
            0x0E0F 0x1011 0x1213 0x1415 0x1617 0x1819 0x1A1B
```

## Related Commands

| Command | Description |
|---|---|
| **atm vc-per-vp** | Sets the maximum number of VCIs to support per VPI. |
| **custom-queue-list** | Assigns a custom queue list to an interface. |
| **fair-queue (class-default)** | Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy. |
| **fair-queue (WFQ)** | Enables WFQ for an interface. |
| **priority-group** | Assigns the specified priority list to an interface. |
| **random-detect (interface)** | Enables WRED or DWRED. |
| **random-detect flow** | Enables flow-based WRED. |
| **show frame-relay pvc** | Displays information and statistics about WFQ for a VIP-based interface. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# show queueing

**Note** Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **showqueueing**command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide* .

**Note** Effective with Cisco IOS XE Release 3.2S, the **showqueueing**command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* .

To list all or selected configured queueing strategies, use the **showqueueing** command in user EXEC or privileged EXEC mode.

**show queueing** [**custom**| **fair**| **priority**| **random-detect** [**interface** *atm-subinterface* [**vc** [[ *vpi* ] *vci*]]]]

## Syntax Description

| | |
|---|---|
| **custom** | (Optional) Status of the custom queueing list configuration. |
| **fair** | (Optional) Status of the fair queueing configuration. |
| **priority** | (Optional) Status of the priority queueing list configuration. |
| **random-detect** | (Optional) Status of the Weighted Random Early Detection (WRED) and distributed WRED (DWRED) configuration, including configuration of flow-based WRED. |
| **interface** *atm-subinterface* | (Optional) Displays the WRED parameters of every virtual circuit (VC) with WRED enabled on the specified ATM subinterface. |
| **vc** | (Optional) Displays the WRED parameters associated with a specific VC. If desired, both the virtual path identifier (VPI) and virtual circuit identifier (VCI) values, or just the VCI value, can be specified. |

| | |
|---|---|
| *vpi* / | (Optional) Specifies the VPI. If the *vpi* argument is omitted, 0 is used as the VPI value for locating the permanent virtual circuit (PVC). If the *vpi* argument is specified, the/separator is required. |
| *vci* | (Optional) Specifies the VCI. |

**Command Default**

If no optional keyword is entered, this command shows the configuration of all interfaces.

**Command Modes**

User EXEC (>) Privileged EXEC (#)

**Command History**

| Release | Modification |
|---|---|
| 10.3 | This command was introduced. |
| 12.0(4)T | This command was integrated into Cisco IOS Release 12.0(4)T. The **red** keyword was changed to **random-detect**. |
| 12.1(2)T | This command was modified. This command was modified to include information about the Frame Relay PVC Interface Priority Queueing (FR PIPQ) feature. |
| 12.2(2)T | This command was integrated into Cisco IOS Release 12.2(2)T. |
| 12.0(24)S | This command was integrated into Cisco IOS Release 12.0(24)S. |
| 12.2(14)S | This command was integrated into Cisco IOS Release 12.2(14)S. |
| 12.2(18)SXF2 | This command was integrated into Cisco IOS Release 12.2(18)SXF2. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| Cisco IOS XE Release 2.6 | This command was modified. This command was hidden. |
| 15.0(1)S | This command was modified. This command was hidden. |
| 15.1(3)T | This command was modified. This command was hidden. |
| Cisco IOS XE Release 3.2S | This command was replaced by an MQC command (or sequence of MQC commands). |

**Usage Guidelines**

This command does not support HQF. Use the **showpolicy-map** and the **showpolicy-mapinterface** commands to gather HQF information and statistics.

## Examples

This section provides sample output from **showqueueing**commands. Depending upon the interface or platform in use and the options enabled, the output that you see may vary slightly from the examples shown below.

## Examples

The following sample output shows that FR PIPQ (referred to as "DLCI priority queue") is configured on serial interface 0. The output also shows the size of the four data-link connection identifier (DLCI) priority queues.

```
Router# show queueing
Current fair queue configuration:
  Interface           Discard     Dynamic      Reserved
                      threshold   queue count  queue count
  Serial3/1           64          256          0
  Serial3/3           64          256          0
Current DLCI priority queue configuration:
  Interface           High    Medium  Normal  Low
                      limit   limit   limit   limit
  Serial0             20      40      60      80
Current priority queue configuration:
List   Queue  Args
1      low    protocol ipx
1      normal protocol vines
1      normal protocol appletalk
1      normal protocol ip
1      normal protocol decnet
1      normal protocol decnet_node
1      normal protocol decnet_rout
1      normal protocol decnet_rout
1      medium protocol xns
1      high   protocol clns
1      normal protocol bridge
1      normal protocol arp
Current custom queue configuration:
Current random-detect configuration:
```

## Examples

The following is sample output from the **showqueueing** command. There are two active conversations in serial interface 0. Weighted fair queueing (WFQ) ensures that both of these IP data streams--both using TCP--receive equal bandwidth on the interface while they have messages in the pipeline, even though more FTP data is in the queue than remote-procedure call (RCP) data.

```
Router# show queueing
Current fair queue configuration:
Interface           Discard     Dynamic      Reserved
                    threshold   queue count  queue count
  Serial0             64          256          0
  Serial1             64          256          0
  Serial2             64          256          0
  Serial3             64          256          0
Current priority queue configuration:
List   Queue  Args
1      high   protocol cdp
2      medium interface Ethernet1
Current custom queue configuration:
Current random-detect configuration:
  Serial5
    Queueing strategy:random early detection (WRED)
    Exp-weight-constant:9 (1/512)
    Mean queue depth:40
    Class   Random       Tail    Minimum    Maximum     Mark
              drop       drop  threshold  threshold  probability
      0       1401       9066        20         40      1/10
      1          0          0        22         40      1/10
      2          0          0        24         40      1/10
```

```
3          0          0         26         40       1/10
4          0          0         28         40       1/10
5          0          0         31         40       1/10
6          0          0         33         40       1/10
7          0          0         35         40       1/10
rsvp       0          0         37         40       1/10
```

**Examples** The following is sample output from the **showqueueingcustom** command:

```
Router# show queueing custom
Current custom queue configuration:
List   Queue  Args
3      10     default
3      3      interface Tunnel3
3      3      protocol ip
3      3      byte-count 444 limit 3
```

**Examples** The following is sample output from the**showqueueingrandom-detect** command. The output shows that the interface is configured for flow-based WRED to ensure fair packet drop among flows. The **random-detectflowaverage-depth-factor**command was used to configure a scaling factor of 8 for this interface. The scaling factor is used to scale the number of buffers available per flow and to determine the number of packets allowed in the output queue of each active flow before the queue is susceptible to packet drop. The maximum flow count for this interface was set to 16 by the **random-detectflowcount**command.

```
Router# show queueing random-detect
    Current random-detect configuration:
      Serial1
        Queueing strategy:random early detection (WRED)
        Exp-weight-constant:9 (1/512)
        Mean queue depth:29
        Max flow count:16       Average depth factor:8
        Flows (active/max active/max):39/40/16

        Class   Random       Tail    Minimum    Maximum     Mark
                  drop       drop  threshold  threshold  probability
          0         31          0         20         40     1/10
          1         33          0         22         40     1/10
          2         18          0         24         40     1/10
          3         14          0         26         40     1/10
          4         10          0         28         40     1/10
          5          0          0         31         40     1/10
          6          0          0         33         40     1/10
          7          0          0         35         40     1/10
         rsvp        0          0         37         40     1/10
```

**Examples** The following is sample output from the **showqueueingrandom-detect** command for DWRED:

```
    Current random-detect configuration:
      Serial1
        Queueing strategy:random early detection (WRED)
        Exp-weight-constant:9 (1/512)
        Mean queue depth:29
        Max flow count:16       Average depth factor:8
        Flows (active/max active/max):39/40/16

        Class   Random       Tail    Minimum    Maximum     Mark
                  drop       drop  threshold  threshold  probability
          0         31          0         20         40     1/10
          1         33          0         22         40     1/10
          2         18          0         24         40     1/10
          3         14          0         26         40     1/10
          4         10          0         28         40     1/10
```

```
          5          0          0         31         40     1/10
          6          0          0         33         40     1/10
          7          0          0         35         40     1/10
        rsvp         0          0         37         40     1/10
Current random-detect configuration:
  FastEthernet2/0/0
    Queueing strategy:fifo
    Packet drop strategy:VIP-based random early detection (DWRED)
    Exp-weight-constant:9 (1/512)
    Mean queue depth:0
    Queue size:0       Maximum available buffers:6308
    Output packets:5  WRED drops:0  No buffer:0
    Class    Random       Tail    Minimum    Maximum     Mark       Output
               drop       drop  threshold  threshold  probability  Packets
      0           0          0        109        218      1/10            5
      1           0          0        122        218      1/10            0
      2           0          0        135        218      1/10            0
      3           0          0        148        218      1/10            0
      4           0          0        161        218      1/10            0
      5           0          0        174        218      1/10            0
      6           0          0        187        218      1/10            0
      7           0          0        200        218      1/10            0
```

The table below describes the significant fields shown in the display.

***Table 247: show queueing Field Descriptions***

| Field | Description |
|---|---|
| Discard threshold | Number of messages allowed in each queue. |
| Dynamic queue count | Number of dynamic queues used for best-effort conversations. |
| Reserved queue count | Number of reservable queues used for reserved conversations. |
| High limit | High DLCI priority queue size in maximum number of packets. |
| Medium limit | Medium DLCI priority queue size, in maximum number of packets. |
| Normal limit | Normal DLCI priority queue size, in maximum number of packets. |
| Low limit | Low DLCI priority queue size, in maximum number of packets. |
| List | Custom queueing--Number of the queue list.<br>Priority queueing--Number of the priority list. |
| Queue | Custom queueing--Number of the queue.<br>Priority queueing--Priority queue level (**high**, **medium**, **normal**, or **low**keyword). |
| Args | Packet matching criteria for that queue. |

| Field | Description |
|---|---|
| Exp-weight-constant | Exponential weight factor. |
| Mean queue depth | Average queue depth. It is calculated based on the actual queue depth on the interface and the exponential weighting constant. It is a moving average. The minimum and maximum thresholds are compared against this value to determine drop decisions. |
| Class | IP Precedence value. |
| Random drop | Number of packets randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP Precedence value. |
| Tail drop | Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP Precedence value. |
| Minimum threshold | Minimum WRED threshold, in number of packets. |
| Maximum threshold | Maximum WRED threshold, in number of packets. |
| Mark probability | Fraction of packets dropped when the average queue depth is at the maximum threshold. |

## Related Commands

| Command | Description |
|---|---|
| **custom-queue-list** | Assigns a custom queue list to an interface. |
| **exponential-weighting-constant** | Configures the exponential weight factor for the average queue size calculation for a WRED parameter group. |
| **fair-queue (WFQ)** | Enables WFQ for an interface. |
| **frame-relay interface-queue priority** | Enables the FR PIPQ feature. |
| **precedence (WRED group)** | Configures a WRED group for a particular IP Precedence. |
| **priority-group** | Assigns the specified priority list to an interface. |
| **priority-list interface** | Establishes queueing priorities on packets entering from a given interface. |

| Command | Description |
|---|---|
| **priority-list queue-limit** | Specifies the maximum number of packets that can be waiting in each of the priority queues. |
| **queue-list interface** | Establishes queueing priorities on packets entering on an interface. |
| **queue-list queue byte-count** | Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle. |
| **random-detect (interface)** | Enables WRED or DWRED. |
| **random-detect flow average-depth-factor** | Sets the multiplier to be used in determining the average depth factor for a flow when flow-based WRED is enabled. |
| **random-detect flow count** | Sets the flow count for flow-based WRED. |
| **show interfaces** | Displays the statistical information specific to a serial interface. |
| **show queue** | Displays the contents of packets inside a queue for a particular interface or VC. |
| **show queueing interface** | Displays the queueing statistics of an interface or VC. |

# show queueing interface

To display the queueing statistics of an interface, use the **showqueueinginterface**command in user EXEC or privileged EXEC mode.

**show queueing interface** *type number* [**vc** [[ *vpi/* ] *vci*]]

### Catalyst 6500 Series Switches

**show queueing interface** {*type number*| **null 0**| **vlan** *vlan-id*} **[detailed]**

### Cisco 7600 Series Routers

**show queueing interface** {*type number*| **null 0**| **vlan** *vlan-id*}

## Syntax Description

| | |
|---|---|
| *type number* | Interface type and interface number.<br>For Cisco 7600 series routers, the valid interface types are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.<br>For Cisco 7600 series routers, the interface number is the module and port number. See the "Usage Guidelines" section for more information. |
| **vc** | (Optional) Shows the weighted fair queueing (WFQ) and Weighted Random Early Detection (WRED) parameters associated with a specific virtual circuit (VC). If desired, both the virtual path identifier (VPI) and virtual channel identifier (VCI) values, or just the VCI value, can be specified. |
| *vpi* / | (Optional) The VPI. If the *vpi* argument is omitted, 0 is used as the VPI value for locating the permanent virtual circuit (PVC). If the *vpi* argument is specified, the/separator is required. |
| *vci* | (Optional) The VCI. |
| **null 0** | Specifies the null interface number; the only valid value is 0. |
| **vlan** *vlan-id* | Specifies the VLAN identification number; valid values are from 1 to 4094. |
| **detailed** | (Optional) Displays the detailed statistics information per policy class. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

**Cisco 7600 Series Routers**

User EXEC (>)

## Command History

| Release | Modification |
|---|---|
| 11.1(22)CC | This command was introduced. |
| 12.2(14)SX | This command was implemented on the Supervisor Engine 720. |
| 12.2(17d)SXB | This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(33)SXI | The **detailed** keyword was added. |

## Usage Guidelines

**Cisco 7600 Series Routers**

The pos, atm, and ge-waninterfaces are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

The *typenumber*argument used with the **interface** keyword designates the module and port number. Valid values depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **showqueueinginterface** command does not display the absolute values that are programmed in the hardware. Use the **showqm-spport-data**command to verify the values that are programmed in the hardware.

**Catalyst 6500 Series Switches**

In Cisco IOS Release 12.2(33)SXI and later releases, the optional **detailed** keyword is available. The **showqueueinginterfacedetailed** command output includes the following information:

- Display of the last 30-second counters.
- Display of the peak 30-second counters over the last 5 minutes.
- Display of the 5-minute average and peak bps rates.
- The peak rates are monitored with 10-second resolution. Releases prior to Cisco IOS Release 12.2(33)SXI were monitored at 30-second resolution.

## Examples

The following is sample output from the **showqueueinginterface**command. In this example, WRED is the queueing strategy in use. The output varies according to queueing strategy in use.

```
Router# show queueing interface atm 2/0
```

```
Interface ATM2/0 VC 201/201
Queueing strategy:random early detection (WRED)
  Exp-weight-constant:9 (1/512)
  Mean queue depth:49
  Total output drops per VC:759
  Class    Random       Tail    Minimum    Maximum     Mark
             drop       drop  threshold  threshold  probability
    0         165         26         30         50     1/10
    1         167         12         32         50     1/10
    2         173         14         34         50     1/10
    3         177         25         36         50     1/10
    4           0          0         38         50     1/10
    5           0          0         40         50     1/10
    6           0          0         42         50     1/10
    7           0          0         44         50     1/10
 rsvp           0          0         46         50     1/10
```

The table below describes the significant fields shown in the display.

***Table 248: show queueing interface Field Descriptions***

| Field | Description |
|---|---|
| Queueing strategy | Name of the queueing strategy in use (for example, WRED). |
| Exp-weight-constant | Exponential weight constant. Exponent used in the average queue size calculation for a WRED parameter group. |
| Mean queue depth | Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a fluctuating average. The minimum and maximum thresholds are compared against this value to determine drop decisions. |
| Class | IP precedence level. |
| Random drop | Number of packets randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence level. |
| Tail drop | Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence level. |
| Minimum threshold | Minimum WRED threshold in packets. |
| Maximum threshold | Maximum WRED threshold in packets. |
| Mark probability | Fraction of packets dropped when the average queue depth is at the maximum threshold. |

The following is sample output from the **showqueueinginterface**command in Cisco IOS Release 12.2(33)SXI and later releases:

```
Router# show queueing interface gigabitethernet 3/27 detailed

.
.
.
  Packets dropped on Transmit:
    BPDU packets:  0
    queue  Total pkts   30-s pkts / peak   5 min average/peak pps   [cos-map]
 ------------------------------------------------------------------------------
    1      443340       55523 / 66671      3334 / 44455             [0 1 ]
    1      7778888      555555 / 666666    233333 / 340000          [2 3 ]
    2      0            0 / 0              0 / 0                    [4 5 ]
    2      0            0 / 0              0 / 0                    [6 7 ]
.
.
.
```

The table below describes the significant fields added when you enter the **detailed** keyword.

***Table 249: show queueing interface detailed Field Descriptions***

| Field | Description |
|---|---|
| Packets dropped on Transmit | Displays information regarding the packets dropped in transmission. |
| BPDU packets | Number of Bridge Protocol Data Unit (BPDU) packets. |
| queue | Queue number. |
| Total pkts | Display of the last 30-second counters. |
| 30-s pkts / peak | Display of the peak 30-second counters over the last 5 minutes. |
| 5 min average/peak pps | Display of the 5-minute average and peak rates in packets per second (pps). |
| cos-map | Class of service (CoS) mapping. |

## Related Commands

| | |
|---|---|
| **custom-queue-list** | Assigns a custom queue list to an interface. |
| **fair-queue (class-default)** | Specifies the number of dynamic queues to be reserved for use by the class-default class as part of the default class policy. |
| **fair-queue (WFQ)** | Enables WFQ for an interface. |
| **priority-group** | Assigns the specified priority list to an interface. |

| | |
|---|---|
| **random-detect flow** | Enables flow-based WRED. |
| **random-detect (interface)** | Enables WRED or DWRED. |
| **random-detect (per VC)** | Enables per-VC WRED or per-VC DWRED. |
| **show frame-relay pvc** | Displays information and statistics about WFQ for a VIP-based interface. |
| **show policy-map interface** | Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface. |
| **show qm-sp port-data** | Displays information about the QoS manager switch processor. |
| **show queueing** | Lists all or selected configured queueing strategies. |

# show random-detect-group

**Note** Effective with Cisco IOS Release 15.0(1)S and Cisco IOS Release 15.1(3)T, the **showrandom-detect-group** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* .

To display the Weighted Random Early Detection (WRED) or distributed WRED (DWRED) parameter group, use the **showrandom-detect-group**command in privileged EXEC mode.

**show random-detect-group** [ *group-name* ]

## Syntax Description

| | |
|---|---|
| *group-name* | (Optional) Name for the WRED or DWRED parameter group. |

## Command Default

No WRED or DWRED parameter group is displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(22)T | This command was introduced in a release earlier than Cisco IOS Release 12.4(22)T. |
| 12.2(33)SRC | This command was integrated in a release earlier than Cisco IOS Release 12.2(33)SRC. |
| 12.2(33)SXI | This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI. |
| 15.0(1)S | This command was modified. This command was hidden. |
| 15.1(3)T | This command was modified. This command was hidden. |

## Usage Guidelines

WRED is a congestion avoidance mechanism that slows traffic by randomly dropping packets when there is congestion. DWRED is similar to WRED but uses the Versatile Interface Processor (VIP) instead of the Route Switch Processor (RSP). WRED and DWRED are most useful when the traffic uses protocols such as TCP that respond to dropped packets by decreasing the transmission rate.

## Examples

The following example displays the current settings of the DWRED group called group-name:

```
Router# show random-detect-group group-name
exponential weight 9
class    min-threshold    max-threshold    mark-probablity
------------------------------------------------------------
0          -                -               1/10
1           1               2000            1/30
2           1               3000            1/40
3           1               4000            1/50
4           1               3000            1/60
5           1               3000            1/60
6           1               4000            1/60
7           1               4000            1/60
rsvp        1                1              1/10
```

The table below describes the significant fields shown in the display.

***Table 250: show random-detect group Field Descriptions***

| Field | Description |
|---|---|
| exponential weight | Exponential weight factor for the average queue size calculation for a WRED parameter group. |
| class | Policy map class name. |
| min-threshold | Minimum threshold in number of packets. The value range of this argument is from 1 to 4096. When the average queue length reaches the minimum threshold, WRED randomly drops some packets with the specified IP Precedence. |
| max-threshold | Maximum threshold in number of packets. The value range of this argument is from the value of the *min-threshold* argument to 4096. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified IP Precedence. |
| mark-probability | Denominator for the fraction of packets dropped when the average queue depth is at the minimum threshold. For example, if the denominator is 512, 1 out of every 512 packets is dropped when the average queue is at the minimum threshold. The value range is from 1 to 65536. The default is 10; 1 out of every 10 packets is dropped at the minimum threshold. |

| Field | Description |
|---|---|
| rsvp | Indicates Resource Reservation Protocol (RSVP) traffic. |

## Related Commands

| Command | Description |
|---|---|
| **dscp** | Changes the minimum and maximum packet thresholds for the DSCP value. |
| **exponential-weighting-constant** | Configures the exponential weight factor for the average queue size calculation for a WRED parameter group. |
| **precedence (WRED group)** | Configures a WRED group for a particular IP Precedence. |
| **random-detect-group** | Defines the WRED or DWRED parameter group. |
| **show queueing** | Lists all or selected configured queueing strategies. |
| **show queueing interface** | Displays the queueing statistics of an interface or VC. |

# show running-config service-group

To display the running configuration of one or all service groups, use the **showrunning-configservice-group**command in privileged EXEC mode.

**show running-config service-group** [ *service-group-identifier* ]

## Syntax Description

| | |
|---|---|
| *service-group-identifier* | (Optional) Service-group number. Enter the service-group number. |

## Command Default

If a service-group number is not specified, information about all service groups is displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRE | This command was introduced. |

## Examples

This example shows how to display information about all the running service groups:

```
Router# show running-config service-group
Building configuration...
Current configuration:
service-group 1
service-group 2
service-group 3
 service-policy output test
service-group 4
service-group 5
 service-policy output test
end
```

This example shows how to display information about a specific running service group. In the example below, service group 700 has been specified.

```
Router# show running-config service-group 700
Building configuration...
Current configuration:
service-group 700
 service-policy output test
end
```

The table below describes the significant fields shown in the display.

*Table 251: show running-config service-group Field Descriptions*

| Field | Description |
|---|---|
| **service-group** | Indicates the service-group number. |
| **service-policy output** | Indicates the output policy attached to the service group. |

# show service-group

To display service-group information for a specific service group or for all service groups, use the **showservice-group**command in privileged EXEC mode.

**show service-group** {*service-group-identifier*| **all**} **[detail]**

## Syntax Description

| | |
|---|---|
| *service-group-identifier* | Service-group number. Enter the number of the service group that you want to display. |
| **all** | Displays information for all service groups. |
| **detail** | (Optional) Displays detailed information. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRE | This command was introduced. |

## Usage Guidelines

Use the **showservice-group** command to display information such as statistics about memberships and interfaces, as well as information about policy maps and member identification numbers.

## Examples

The following is sample output from the **showservice-group**command. This example displays statistics for service group 1:

```
Router# show service-group 1

Service Group 1:
  Number of members:                    2
  State:                                Up
  Interface:                            GigabitEthernet2/0/0
    Number of members:                  2
```

The following is sample output of the **showservice-group**command with the **detail** keyword specified. This example displays detailed statistics for service group 1:

```
Router# show service-group 1 detail
Service Group 1:
  Description: Test service group.
  Number of members:                    2
      Service Instance                  2
  State:                                Up
  Features configured:                  QoS
  Input service policy:                 in1
  Output service policy:                out1
  Number of Interfaces:                 1
```

```
Interface:                                GigabitEthernet2/0/0
  Number of members:                      2
  Service Instance ID:
      1
      3
```

The table below describes the significant fields shown in the display.

***Table 252: show service-group Field Descriptions***

| Field | Description |
|---|---|
| Service Group 1 | Service group number. |
| Number of members | Number of members in the service group. Also includes service instance numbers. |
| State | Indicates the administrative state of the service group.<br>**Note** For Cisco IOS Release 12.2(33)SRE, the administrative state is always "Up" and cannot be modified. |
| Interface | Interface to which the service group is attached, along with the number of members, as applicable. |

The table below describes the significant fields shown in the display when the **detail** keyword is specified.

***Table 253: show service-group detail Field Descriptions***

| Field | Description |
|---|---|
| Service Group | Service-group number. |
| Description | Service-group description. |
| Number of members | Number of members in the service group. Also includes service instance numbers. |
| State | Indicates the administrative state of the service group.<br>**Note** For Cisco IOS Release 12.2(33)SRE, the administrative state is always "Up" and cannot be modified. |
| Features configured | Features configured in the service group.<br>**Note** For Cisco IOS Release 12.2(33)SRE, the only feature supported on the Cisco 7600 series router is Quality of Service (QoS). |
| Input service policy | Name of the input service policy. |
| Output service policy | Name of the output service policy. |

| Field | Description |
|---|---|
| Number of Interfaces | Number of interfaces. |
| Interface | Name of the interface, number of members in the service group, and service instance number(s), as applicable. |

# show service-group interface

To display service-group membership information by interface, use the **showservice-groupinterface**command in privileged EXEC mode.

**show service-group interface** *type number* [**group** *service-group-identifier*] **[detail]**

## Syntax Description

| | |
|---|---|
| *type* | Interface type. For more information, use the question mark (?) online help function. |
| number | Interface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function. |
| **group** | (Optional) Displays service-group information. |
| *service-group-identifier* | (Optional) Service-group number. Enter the number of the service group that you want to display. |
| **detail** | (Optional) Displays detailed statistics for all groups. |

## Command Default

If an interface is not specified, service-group information about all interfaces is displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRE | This command was introduced. |

## Examples

This example shows how to display service-group membership information for Gigabit Ethernet interface 3/1:

```
Router# show service-group interface gigabitethernet 3/1
Interface GigabitEthernet3/1:
  Number of groups:                     3
  Group
      1
      2
      3
This example shows how to display service-group detailed membership information for Gigabit
 Ethernet interface 3/1:
Router# show service-group interface gigabitethernet 3/1 detail
Interface GigabitEthernet3/1:
  Number of groups:                     3
Service Group 1:
```

```
  Number of members:                      3000
    Service Instance ID:
         1
         2
         3
         4
         5
         6
         7
         8
         9
        10
       . . .
This example shows how to display detailed membership information for Gigabit Ethernet
interface 3/1 service group 10:
Router# show service-group interface gigabitethernet 3/1 group 10 detail
Service Group 10:
 Number of members:                     3
  Service Instance ID:
   100
   101
   102
```

The table below describes the significant fields shown in the display.

***Table 254: show service-group interface service group Field Descriptions***

| Field | Description |
|---|---|
| Interface | Interface type and number. |
| Number of groups | Number of groups. |
| Service Group | Service-group number. |
| Number of members | Number of members in the service group. |
| Service Instance ID | Service-instance identifier. |

# show service-group state

To display state information about one or all service groups, use the **showservice-groupstate**command in privileged EXEC mode.

**show service-group state** [**group** *service-group-identifier*]

## Syntax Description

| | |
|---|---|
| **group** | (Optional) Displays service-group state statistics. |
| *service-group-identifier* | (Optional) Service-group number. Enter the number of the service group that you want to display. |

## Command Default

If a service-group number is not specified, information about all service groups is displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRE | This command was introduced. |

## Examples

The following is sample output from the **showservice-groupstate** command. In this example, state infomation about all the service groups is displayed. The fields are self-explanatory.

**Note** For Cisco IOS Release 12.2(33)SRE, the state is always “Up” and cannot be modified.

```
Router# show service-group state
    Group      State
      1         Up
      2         Up
      3         Up
     10         Up
     20         Up
```

# show service-group stats

To display service-group statistical information, use the **showservice-groupstats**command in privileged EXEC mode.

**show service-group stats** [**errors**| **group** *service-group-identifier*| **interface** *type number*| **module** *slot*]

## Syntax Description

| | |
|---|---|
| **errors** | (Optional) Displays service-group errors. |
| **group** | (Optional) Displays service-group statistics. |
| *service-group-identifier* | (Optional) Service-group number. Enter the number of the service group that you want to display. |
| **interface** | (Optional) Displays statistics for the specified interface. |
| *type* | (Optional) Interface type. For more information, use the question mark (?) online help function. |
| *number* | (Optional) Interface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function. |
| **module** | (Optional) Displays statistics for the configured module. |
| *slot* | (Optional) Module slot. The range of valid entries can vary by interface. For more information, use the question mark (?) online help function. |

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRE | This command was introduced. |

## Examples

The following section contains sample output from this command with the various keywords and arguments. The fields in the output are self-explanatory.

This example shows how to display all service-group statistics:

```
Router# show service-group stats
```

```
Service Group global statistics:
  Number of groups:                     5
  Number of members:                    8005
Service Group 1 statistics:
  Number of Interfaces:                 1
  Number of members:                    3000
    Service Instance                    3000
  Members joined:                       13000
  Members left:                         10000
Service Group 2 statistics:
  Number of Interfaces:                 1
  Number of members:                    2000
    Service Instance                    2000
  Members joined:                       10000
  Members left:                         8000
Service Group 3 statistics:
  Number of Interfaces:                 1
  Number of members:                    3000
    Service Instance                    3000
  Members joined:                       9000
  Members left:                         6000
Service Group 10 statistics:
  Number of Interfaces:                 1
  Number of members:                    3
    Service Instance                    3
  Members joined:                       8003
  Members left:                         8000
Service Group 20 statistics:
  Number of Interfaces:                 1
  Number of members:                    2
    Service Instance                    2
  Members joined:                       8002
  Members left:                         8000
This example shows how to display all error statistics for all service groups:
Router# show service-group stats errors
Service Group 1 errors:
  Members rejected to join:
    Capability limitation:              0
    Rejected by other software modules:  0
    Failed to install service policy:   0
    Database error:                     0
    Feature encountered error:          0
    Invalid member type:                0
    Invalid member id:                  0
Service Group 2 errors:
  Members rejected to join:
    Capability limitation:              0
    Rejected by other software modules:  0
    Failed to install service policy:   0
    Database error:                     0
    Feature encountered error:          0
    Invalid member type:                0
    Invalid member id:                  0
Service Group 3 errors:
  Members rejected to join:
    Capability limitation:              0
    Rejected by other software modules:  0
    Failed to install service policy:   0
    Database error:                     0
    Feature encountered error:          0
    Invalid member type:                0
    Invalid member id:                  0
This example shows how to display statistics for service group 20:
Router# show service-group stats group 20
Service Group 20 statistics:
  Number of Interfaces:                 1
  Number of members:                    2
    Service Instance:                   2
  Members joined:                       8002
  Members left:                         8000
This example shows how to display statistics for the service-groups on a specific interface:
Router# show service-group stats interface gigabitethernet2/0/0
```

```
Interface GigabitEthernet2/0/0:
  Number of groups:                     1
  Number of members:                    2
  Group  Members  Service Instances
      1        2                 2
This example shows how to display statistics for the service-groups on module 3:
Router# show service-group stats module 3
Module 3:
  Number of groups:                     3
  Number of members:                    8000
  Group               Interface  Members  Service Instances
      1       GigabitEthernet3/1     3000               3000
      2       GigabitEthernet3/1     2000               2000
      3       GigabitEthernet3/1     3000               3000
```

# show service-group traffic-stats

To display service-group traffic statistics, use the **showservice-grouptraffic-stats**command in privileged EXEC mode.

**show service-group traffic-stats** [**group** *service-group-identifier*]

## Syntax Description

| | |
|---|---|
| **group** | (Optional) Displays service-group statistics. |
| *service-group-identifier* | (Optional) Service-group identifier. Enter the number of an existing service group. |

## Command Default

If a service-group number is not specified, information about all service groups is displayed.

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRE | This command was introduced. |

## Usage Guidelines

The **showservice-grouptraffic-stats** command reports the combined total of the traffic statistics for all members of the service group.

**How Traffic Statistics Are Collected**

The traffic statistics for each member of a service group are accumulated and incremented periodically. Each time the statistics for the member are incremented, the group statistics are also incremented by the same amount. Note the following points:

- The service-group traffic statistics represent the grand total of the traffic statistics of all its members once they join the group. Traffic statistics collected prior to joining the group are not included. At any given time, therefore, it is possible that the total of the member traffic statistics may be larger than the group traffic statistics.
- The traffic statistics of a member can be cleared by using the **clearethernetserviceinstance**command. Clearing the traffic statistics of a member does not affect the group statistics in any way.
- Clearing the group traffic statistics does not clear the traffic statistics of the group member.

## Examples

The following section contains sample output from the **showservice-grouptraffic-stats**command. The fields in the output are self-explanatory.

This example shows how to display traffic statistics for all service groups.

```
Router# show service-group traffic-stats
Traffic Statistics of service groups:
  Group     Pks In   Bytes In   Pkts Out  Bytes Out
      1          0          0          0          0
      2          0          0          0          0
      3          0          0          0          0
     10          0          0          0          0
     20          0          0          0          0
This example shows how to display traffic statistics for service group 10:
Router# show service-group traffic-stats group 10
Traffic Statistics of service groups:
  Group     Pks In   Bytes In   Pkts Out  Bytes Out
     10          0          0          0          0
```

## Related Commands

| Command | Description |
|---|---|
| **clear ethernet service instance** | Clears Ethernet service instance attributes such as MAC addresses and statistics or purges Ethernet service instance errors. |

# show subscriber policy ppm-shim-db

To display the total number of dynamically created template service policy maps and Net Effect policy maps on the router, use the **showsubscriberpolicyppm-shim-db**command in user EXEC or privileged EXEC mode.

**show subscriber policy ppm-shim-db**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release XE 3.2S | This command was introduced on the ASR 1000 Series Aggregation Services Routers. |

## Examples

The following is sample output from the **showsubscriberpolicyppm-shim-db** command:

```
Router# show subscriber policy ppm-shim-db
Total number of dynamically created policy = 10
The output fields are self-explanatory.
```

# show table-map

To display the configuration of a specified table map or all table maps, use the **showtable-map**command in EXEC mode.

**show table-map** *table-map-name*

## Syntax Description

| | |
|---|---|
| *table-map-name* | Name of table map used to map one packet-marking value to another. The name can be a maximum of 64 alphanumeric characters. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |

## Examples

The sample output of the **showtable-map**command shows the contents of a table map called “map 1”. In “map1”, a “to-from” relationship has been established and a default value has been defined. The fields for establishing the “to-from” mappings are further defined by the policy map in which the table map will be configured. (Configuring a policy map is the next logical step after creating a table map.)

For instance, a precedence or differentiated services code point (DSCP) value of 0 could be mapped to a class of service (CoS) value of 1, or vice versa, depending on the how the values are defined in the table map. Any values not explicitly defined in a “to-from” relationship will be set to a default value.

The following sample output of the **showtable-map** command displays the contents of a table map called “map1”. In this table map, a packet-marking value of 0 is mapped to a packet-marking value of 1. All other packet-marking values are mapped to the default value 3.

```
Router# show table-map map1
 Table Map map1
 from 0 to 1
 default 3
```

The table below describes the fields shown in the display.

***Table 255: show table-map Field Descriptions***

| Field | Description |
|---|---|
| Table Map | The name of the table map being displayed. |

| Field | Description |
|---|---|
| from, to | The values of the “to-from” relationship established by the **table-map** (value mapping) command and further defined by the policy map in which the table map will be configured. |
| default | The default action to be used for any values not explicitly defined in a “to-from” relationship by the **table-map** (value mapping) command. If a default action is not specified in the table-map (value mapping) command, the default action is “copy”. |

## Related Commands

| Command | Description |
|---|---|
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map class** | Displays the configuration for the specified class of the specified policy map. |
| **table-map (value mapping)** | Creates and configures a mapping table for mapping and converting one packet-marking value to another. |

# show tech-support nbar platform

To display general information about Network-based Application Recognition (NBAR), use the show tech-support nbar platform command in privileged EXEC mode.

**show tech-support  nbar platform**

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Release XE 3.10S | This command was introduced. |

## Usage Guidelines

The **show tech-support nbar platform** command displays the output from the commands: **show ip nbar protocol activated**, **show ip nbar attribute-map**, **show ip nbar parameter extraction activated**, **show ip nbar parameter subclassification activated**, **show ip nbar protocol-attribute**, **show ip nbar protocol-discovery**, **show ip nbar protocol-pack active**, **show ip nbar resources**, **show ip nbar resources flow**, **show ip nbar statistics**, **show ip nbar version**, **show platform hardware qfp active feature nbar profiling**, **show platform software nbar statistics**, and **show policy-map interface**. The command also displays the output from the functions: st_sui_fia_show, st_sui_fia_ut_mean_func_show, st_sui_fe_show, st_sui_fv_stats_show, st_sui_mpe_chunk_utl_show, st_sui_mpe_dp_utl_show, st_sui_mtp_dp_dump_external_flags, st_sui_mtp_dp_show_cfg, st_sui_mtp_dp_show_prs_graph, st_sui_mtp_stats_general, st_sui_stile_is_ready, st_sui_stile_show_cls_err_cnt, and st_sui_stile_show_msc. These functions are used along with **show platform hardware qfp active feature nbar function** command, for example, **show platform hardware qfp active feature nbar function** *st_sui_fe_show*.

## Examples

This following example is an excerpt from the output of the **show  tech-support nbar platform** command that displays NBAR information:

```
Device# show tech-support nbar platform

------------------ show running-config ------------------


Building configuration...

Current configuration : 1600 bytes
!
! Last configuration change at 04:16:19 PST Thu Jul 25 2013
!
version 15.3
service timestamps debug uptime
service timestamps log uptime
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
```

```
!
no aaa new-model
!
!
!
clock timezone PST -8 0
!
!
!
!
!


!
!
!
ip cef
no ipv6 cef
!
!
!
!
!
!
!
multilink bundle-name authenticated
!
!
!
!
!
!
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface Tunnel21
 no ip address
 ip nbar protocol-discovery
!
interface Ethernet0/0
 no ip address
 shutdown
!
interface Ethernet0/1
 no ip address
 shutdown
!
interface Ethernet0/2
 no ip address
 shutdown
!
interface Ethernet0/3
 no ip address
 shutdown
!
interface Ethernet1/0
 no ip address
 shutdown
!
interface Ethernet1/1
 no ip address
 ip nbar protocol-discovery
 shutdown
!
interface Ethernet1/2
 no ip address
 shutdown
!
interface Ethernet1/3
 no ip address
 shutdown
```

```
!
interface Serial2/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial2/3
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/0
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial3/3
 no ip address
 shutdown
 serial restart-delay 0
!
ip forward-protocol nd
!
!
no ip http server
!
!
!
!
control-plane
!
!
line con 0
 logging synchronous
line aux 0
line vty 0 4
 login
!
!
!
end


------------------ show ip nbar statistics ------------------


Compiler statistics
Malloc failure = 0
Control-plane statistics
Malloc failure = 0
Invalid iterators = 0
Data-plane statistics
```

```
Malloc failure = 0
FO create failure = 0
CFT Age set failure = 0
L3 Classification Error = 0

------------------ show ip nbar resources ------------------

NBAR memory usage for tracking Stateful sessions
   System link age      : 30 secs
   Initial memory       : 4160 KBytes
   Max initial memory   : 13868 KBytes
   Memory expansion     : 128 KBytes
   Max memory expansion : 128 KBytes
   Memory in use        : 4160 KBytes
   Max memory allowed   : 27736 KBytes
   Active links         : 0
   Total links          : 32504
   Flow Object in Use   : 0


------------------ show ip nbar protocol activated ------------------



Following Protocol(s) is(are) enabled
 Feature:PD
       Hwidb:Tunnel21 MI:1 SI:0 FR:0 PVC:0
       Hwidb:Ethernet1/1 MI:1 SI:0 FR:0 PVC:0
All iana protocols



------------------ show ip nbar version ------------------



NBAR software version:  16
NBAR minimum backward compatible version:  13

1   base                              Mv: 6
2   ftp                               Mv: 7
      Iv:                               smtp - 2
      Iv:                            gridftp - 1
      Iv:                           ftp-data - 1
3   ftp-data                          Mv: 1
      Iv:                               ftp - 7
      Iv:                              smtp - 2
      Iv:                            gridftp - 1
4   http                              Mv: 20
      Iv:                            youtube - 6
      Iv:                      msn-messenger - 3
      Iv:                     yahoo-messenger - 3
      Iv:                         flash-video - 2
      Iv:                          flashyahoo - 2
      Iv:                        flashmyspace - 2
      Iv:                     audio-over-http - 2
      Iv:                    binary-over-http - 2
      Iv:                     video-over-http - 2
      Iv:                                 irc - 2
      Iv:                             babelgum - 1
      Iv:                               itunes - 1
      Iv:                                sling - 1
      Iv:                         google-earth - 1
      Iv:                          baidu-movie - 1
      Iv:                                pando - 1
      Iv:                              napster - 1
      Iv:                             songsari - 1
      Iv:                           webthunder - 1
      Iv:                              sopcast - 3
      Iv:                          tunnel-http - 1
      Iv:                             soribada - 2
      Iv:                                  icq - 1
```

```
      Iv:                          skype - 5
      Iv:                         edonkey - 7
      Iv:                    directconnect - 5
      Iv:                        gnutella - 7
      Iv:                       ms-update - 1
      Iv:                            rtsp - 9
      Iv:                         netflix - 1
      Iv:                       megavideo - 1
      Iv:                      bittorrent - 5
      Iv:                             tor - 1
      Iv:                           gmail - 1
      Iv:                           gtalk - 1
      Iv:                       gtalk-voip - 1
      Iv:                      gtalk-video - 1
      Iv:                       activesync - 1
      Iv:                         rhapsody - 1
      Iv:                            fring - 1
      Iv:                            rtmpt - 1
      Iv:                      livestation - 1
      Iv:                       secondlife - 1
      Iv:                         vnc-http - 1
      Iv:                      share-point - 1
      Iv:                    ms-office-365 - 1
      Iv:                           ms-sms - 1
      Iv:                        ghostsurf - 1
      Iv:                         gotomypc - 1
      Iv:                    adobe-connect - 1
      Iv:                        realmedia - 1
      Iv:                    windows-azure - 1
      Iv:                  ms-live-accounts - 1
      Iv:                     aol-messenger - 2
      Iv:               aol-messenger-video - 1
      Iv:                           mikogo - 1
      Iv:                          pandora - 1
      Iv:         oracle-ebsuite-unsecured - 1
      Iv:                          hotmail - 1
      Iv:                         facebook - 1
      Iv:                          twitter - 1
      Iv:                             hulu - 1
      Iv:                          blogger - 1
      Iv:                       yahoo-mail - 1
      Iv:                         linkedin - 1
      Iv:                          logmein - 1
      Iv:                          gbridge - 1
      Iv:                           citrix - 12
      Iv:                              ssl - 1
      Iv:                         showmypc - 1
      Iv:                    yahoo-accounts - 1
      Iv:                         exchange - 4
      Iv:                        salesforce - 1
      Iv:                         ppstream - 1
      Iv:                          ms-lync - 1
      Iv:                           qqlive - 1
      Iv:                             pptv - 1
      Iv:                           xunlei - 1
      Iv:           bittorrent-networking - 1
      Iv:                        shoutcast - 1
      Iv:                     xunlei-kankan - 1
5   static                           Mv: 6
6   socks                            Mv: 3
7   nntp                             Mv: 2
      Iv:                   yahoo-messenger - 3
8   tftp                             Mv: 2
9   ms-rpc                           Mv: 2
      Iv:                         exchange - 4
      Iv:                       ms-netlogon - 1
      Iv:                        ms-win-dns - 1
      Iv:                           ms-iis - 1
      Iv:                  active-directory - 1
10  exchange                         Mv: 4
      Iv:                           ms-rpc - 2
      Iv:                             http - 20
11  vdolive                          Mv: 1
```

```
12  sqlnet                              Mv: 2
13  oracle-sqlnet                       Mv: 2
14  netshow                             Mv: 3
15  sunrpc                              Mv: 3
      Iv:                                 nfs - 1
      Iv:                           clearcase - 1
16  nfs                                 Mv: 1
17  streamwork                          Mv: 2
18  citrix                              Mv: 12
      Iv:                                http - 20
19  fasttrack                           Mv: 3
20  gnutella                            Mv: 7
      Iv:                                http - 20
21  kazaa2                              Mv: 11
22  dhcp                                Mv: 1
23  rtsp                                Mv: 9
      Iv:                             youtube - 6
      Iv:                                http - 20
24  webex-meeting                       Mv: 1
      Iv:                                  ssl - 1
      Iv:                                 spdy - 1
      Iv:                                 http - 20
25  rtp                                 Mv: 8
      Iv:                             stun-nat - 1
      Iv:                           gtalk-voip - 1
      Iv:                          gtalk-video - 1
      Iv:                       ms-lync-media - 1
26  mgcp                                Mv: 2
27  skinny                              Mv: 3
      Iv:                           cisco-phone - 4
28  sip                                 Mv: 5
      Iv:                           cisco-phone - 4
      Iv:                 telepresence-control - 4
      Iv:                  yahoo-voip-over-sip - 1
      Iv:                           secondlife - 1
      Iv:                             stun-nat - 1
      Iv:                             facetime - 1
29  rtcp                                Mv: 5
      Iv:                 telepresence-control - 4
      Iv:                             stun-nat - 1
30  edonkey                             Mv: 7
      Iv:                                http - 20
31  winmx                               Mv: 5
32  bittorrent                          Mv: 5
      Iv:                              blizwow - 2
      Iv:                                socks - 3
      Iv:                                 http - 20
      Iv:                                  dht - 1
      Iv:                bittorrent-networking - 1
33  directconnect                       Mv: 5
      Iv:                                http - 20
34  hl7                                 Mv: 3
35  fix                                 Mv: 3
      Iv:                                  ssl - 1
      Iv:                                 spdy - 1
36  msn-messenger                       Mv: 3
      Iv:                                 http - 20
      Iv:                               ms-wbt - 1
      Iv:                                socks - 3
      Iv:                    msn-messenger-ft - 1
      Iv:                                  ssl - 1
37  ms-live-accounts                    Mv: 1
      Iv:                                 http - 20
      Iv:                                  ssl - 1
38  windows-azure                       Mv: 1
      Iv:                                 http - 20
      Iv:                                  ssl - 1
39  pandora                             Mv: 1
      Iv:                                 http - 20
      Iv:                                  ssl - 1
40  oracle-ebsuite-unsecured            Mv: 1
      Iv:                                 http - 20
41  hotmail                             Mv: 1
```

```
      Iv:                                http - 20
      Iv:                                 ssl - 1
42  dicom                               Mv: 4
43  yahoo-messenger                     Mv: 3
      Iv:                                http - 20
      Iv:                                nntp - 2
      Iv:                               socks - 3
      Iv:                                 ssl - 1
      Iv:                                spdy - 1
44  bgp                                 Mv: 1
45  l2tp                                Mv: 1
46  mapi                                Mv: 3
47  cifs                                Mv: 2
48  cisco-phone                         Mv: 4
      Iv:                                 sip - 5
      Iv:                              skinny - 3
      Iv:              telepresence-control - 4
49  youtube                             Mv: 6
      Iv:                                http - 20
      Iv:                                rtsp - 9
      Iv:                                 ssl - 1
50  realmedia                           Mv: 1
      Iv:                                http - 20
      Iv:                                rtsp - 9
      Iv:                                 ssl - 1
51  imap                                Mv: 1
52  pop3                                Mv: 1
53  irc                                 Mv: 2
      Iv:                                http - 20
54  skype                               Mv: 5
      Iv:                                http - 20
      Iv:                                 dns - 1
55  blizwow                             Mv: 2
      Iv:                             bittorrent - 5
56  telepresence-media                  Mv: 3
57  telepresence-control                Mv: 4
      Iv:                                rtcp - 5
      Iv:                            cisco-phone - 4
      Iv:                                 sip - 5
58  zattoo                              Mv: 3
59  sopcast                             Mv: 3
      Iv:                                http - 20
60  flash-video                         Mv: 2
      Iv:                                http - 20
61  flashyahoo                          Mv: 2
      Iv:                                http - 20
62  flashmyspace                        Mv: 2
      Iv:                                http - 20
63  audio-over-http                     Mv: 2
      Iv:                                http - 20
64  binary-over-http                    Mv: 2
      Iv:                                http - 20
65  video-over-http                     Mv: 2
      Iv:                                http - 20
66  my-jabber-ft                        Mv: 1
67  ayiya-ipv6-tunneled                 Mv: 1
68  filetopia                           Mv: 1
69  guruguru                            Mv: 1
70  manolito                            Mv: 1
71  radius                              Mv: 1
72  teamspeak                           Mv: 1
73  soribada                            Mv: 2
      Iv:                                http - 20
74  dht                                 Mv: 1
75  pptp                                Mv: 2
76  ntp                                 Mv: 1
77  poco                                Mv: 2
78  ventrilo                            Mv: 1
79  tomatopang                          Mv: 1
80  maplestory                          Mv: 1
81  itunes                              Mv: 1
      Iv:                                http - 20
82  napster                             Mv: 1
```

```
      Iv:                                http - 20
83  sling                               Mv: 1
      Iv:                                http - 20
84  google-earth                        Mv: 1
      Iv:                                http - 20
85  baidu-movie                         Mv: 1
      Iv:                                http - 20
86  pando                               Mv: 1
      Iv:                                http - 20
87  webthunder                          Mv: 1
      Iv:                                http - 20
      Iv:                               xunlei - 1
88  babelgum                            Mv: 1
      Iv:                                http - 20
89  songsari                            Mv: 1
      Iv:                                http - 20
90  tunnel-http                         Mv: 1
      Iv:                                http - 20
91  teredo-ipv6-tunneled                Mv: 1
92  sixtofour-ipv6-tunneled             Mv: 1
      Iv:                 isatap-ipv6-tunneled - 1
93  isatap-ipv6-tunneled                Mv: 1
      Iv:           sixtofour-ipv6-tunneled - 1
94  fring                               Mv: 1
      Iv:                                http - 20
95  fring-voip                          Mv: 1
      Iv:                          fring-video - 1
96  fring-video                         Mv: 1
      Iv:                           fring-voip - 1
97  waste                               Mv: 1
98  kuro                                Mv: 1
99  smtp                                Mv: 2
      Iv:                                  ftp - 7
100  icq                                 Mv: 1
      Iv:                                 http - 20
101  soulseek                            Mv: 1
102  yahoo-voip-messenger                Mv: 2
      Iv:                                  rtp - 8
103  yahoo-voip-over-sip                 Mv: 1
      Iv:                                  sip - 5
104  aol-protocol                        Mv: 1
      Iv:                         aol-messenger - 2
105  ipsec                               Mv: 1
106  isakmp                              Mv: 1
107  ppstream                            Mv: 1
      Iv:                                http - 20
108  rtmp                                Mv: 1
109  rtmpe                               Mv: 1
110  rtmpt                               Mv: 1
      Iv:                                http - 20
111  dns                                 Mv: 1
      Iv:                           tcpoverdns - 1
      Iv:                                skype - 5
112  windows-update                      Mv: 1
113  encrypted-emule                     Mv: 1
114  networking-gnutella                 Mv: 1
115  encrypted-bittorrent                Mv: 1
116  ms-wbt                              Mv: 1
      Iv:                         msn-messenger - 3
117  gmail                               Mv: 1
      Iv:                                http - 20
      Iv:                                 ssl - 1
118  openvpn                             Mv: 1
      Iv:                                  ssl - 1
      Iv:                                 spdy - 1
119  ssl                                 Mv: 1
      Iv:                                  fix - 3
      Iv:                         webex-meeting - 1
      Iv:                               netflix - 1
      Iv:                                 gmail - 1
      Iv:                           livemeeting - 1
      Iv:                           livestation - 1
      Iv:                                   dmp - 1
```

```
      Iv:                          rhapsody - 1
      Iv:                        secondlife - 1
      Iv:                  ms-live-accounts - 1
      Iv:                   google-accounts - 1
      Iv:                  active-directory - 1
      Iv:                           sip-tls - 1
      Iv:                     ms-office-365 - 1
      Iv:                             pcoip - 1
      Iv:                       vmware-view - 1
      Iv:                           openvpn - 1
      Iv:                         ms-update - 1
      Iv:                             mysql - 1
      Iv:                          gotomypc - 1
      Iv:                         ghostsurf - 1
      Iv:                      adobe-connect - 1
      Iv:                      aol-messenger - 2
      Iv:                        share-point - 1
      Iv:                          realmedia - 1
      Iv:            ms-dynamics-crm-online - 1
      Iv:                    windows-azure - 1
      Iv:                          twitter - 1
      Iv:                             hulu - 1
      Iv:                           logmein - 1
      Iv:                            mikogo - 1
      Iv:                           pandora - 1
      Iv:                           hotmail - 1
      Iv:                          facebook - 1
      Iv:                   google-services - 1
      Iv:                       google-plus - 1
      Iv:                       google-docs - 1
      Iv:                            picasa - 1
      Iv:                       yahoo-mail - 1
      Iv:                          youtube - 6
      Iv:                         linkedin - 1
      Iv:                            gtalk - 1
      Iv:                             http - 20
      Iv:                         facetime - 1
      Iv:                         showmypc - 1
      Iv:                    yahoo-accounts - 1
      Iv:                  msn-messenger-ft - 1
      Iv:                     msn-messenger - 3
      Iv:                msn-messenger-video - 1
      Iv:                          ms-lync - 1
      Iv:                             spdy - 1
120   aol-messenger                  Mv: 2
      Iv:                           socks - 3
      Iv:                             ssl - 1
      Iv:                            http - 20
      Iv:                            spdy - 1
121   ghostsurf                      Mv: 1
      Iv:                            http - 20
122   netflix                        Mv: 1
      Iv:                            http - 20
      Iv:                             ssl - 1
123   megavideo                      Mv: 1
      Iv:                            http - 20
124   stun-nat                       Mv: 1
      Iv:                             ssl - 1
      Iv:                            spdy - 1
      Iv:                    ms-lync-media - 1
125   viber                          Mv: 1
126   cisco-ip-camera                Mv: 1
      Iv:                            rtsp - 9
127   livestation                    Mv: 1
      Iv:                            http - 20
      Iv:                            rtmp - 1
      Iv:                             ssl - 1
128   gridftp                        Mv: 1
      Iv:                             ftp - 7
129   winny                          Mv: 1
130   livemeeting                    Mv: 1
      Iv:                             ssl - 1
      Iv:                        stun-nat - 1
```

```
      Iv:                                spdy - 1
131   tor                                Mv: 1
      Iv:                                http - 20
      Iv:                                 ssl - 1
132   xmpp-client                        Mv: 1
133   gtalk-chat                         Mv: 1
      Iv:                          xmpp-client - 1
134   gtalk                              Mv: 1
      Iv:                                http - 20
      Iv:                             stun-nat - 1
      Iv:                           gtalk-video - 1
      Iv:                            gtalk-voip - 1
      Iv:                              gtalk-ft - 1
      Iv:                                   ssl - 1
135   gtalk-voip                         Mv: 1
      Iv:                                http - 20
      Iv:                             stun-nat - 1
      Iv:                                gtalk - 1
      Iv:                                  rtp - 8
136   gtalk-ft                           Mv: 1
      Iv:                             stun-nat - 1
      Iv:                                gtalk - 1
137   gtalk-video                        Mv: 1
      Iv:                                http - 20
      Iv:                             stun-nat - 1
      Iv:                                gtalk - 1
138   steam                              Mv: 1
139   ping                               Mv: 1
140   exec                               Mv: 1
141   login                              Mv: 1
142   shell                              Mv: 1
143   netapp-snapmirror                  Mv: 1
144   ms-iis                             Mv: 1
      Iv:                              ms-rpc - 2
145   ms-win-dns                         Mv: 1
      Iv:                              ms-rpc - 2
146   ms-netlogon                        Mv: 1
      Iv:                              ms-rpc - 2
147   ms-sms                             Mv: 1
      Iv:                                http - 20
      Iv:                           ms-update - 1
148   perforce                           Mv: 1
149   vnc                                Mv: 1
      Iv:              apple-remote-desktop - 1
150   vnc-http                           Mv: 1
      Iv:                                http - 20
151   secondlife                         Mv: 1
      Iv:                                 ssl - 1
      Iv:                                http - 20
      Iv:                                 sip - 5
      Iv:                                spdy - 1
152   msn-messenger-ft                   Mv: 1
      Iv:                       msn-messenger - 3
      Iv:                                 ssl - 1
      Iv:                              socks - 3
      Iv:                                spdy - 1
153   icq-filetransfer                   Mv: 1
154   tcpoverdns                         Mv: 1
      Iv:                                 dns - 1
155   msn-messenger-video                Mv: 1
      Iv:                             stun-nat - 1
      Iv:                                  rtp - 8
      Iv:                       msn-messenger - 3
      Iv:                              socks - 3
      Iv:                                 ssl - 1
156   share-point                        Mv: 1
      Iv:                                http - 20
      Iv:                                 ssl - 1
157   sip-tls                            Mv: 1
      Iv:                                 ssl - 1
      Iv:                                spdy - 1
158   activesync                         Mv: 1
      Iv:                                http - 20
```

```
159  rhapsody                          Mv: 1
      Iv:                              http - 20
      Iv:                              rtmp - 1
      Iv:                               ssl - 1
160  ip-messenger                      Mv: 1
161  capwap-control                    Mv: 1
      Iv:                         capwap-data - 1
162  capwap-data                       Mv: 1
      Iv:                       capwap-control - 1
163  dmp                               Mv: 1
      Iv:                               ssl - 1
      Iv:                              spdy - 1
164  netbios-ns                        Mv: 1
165  ldap                              Mv: 1
166  active-directory                  Mv: 1
      Iv:                             ms-rpc - 2
      Iv:                               cifs - 2
      Iv:                               ldap - 1
      Iv:                               ssl - 1
167  google-accounts                   Mv: 1
      Iv:                               ssl - 1
      Iv:                              spdy - 1
168  ms-office-365                     Mv: 1
      Iv:                              http - 20
      Iv:                               ssl - 1
169  teamviewer                        Mv: 1
170  pcanywhere                        Mv: 1
171  snmp                              Mv: 1
172  vmware-vmotion                    Mv: 1
173  pcoip                             Mv: 1
      Iv:                               ssl - 1
      Iv:                              spdy - 1
174  vmware-view                       Mv: 1
      Iv:                               ssl - 1
      Iv:                              spdy - 1
175  gotomypc                          Mv: 1
      Iv:                              http - 20
      Iv:                               ssl - 1
176  ms-dynamics-crm-online            Mv: 1
      Iv:                               ssl - 1
      Iv:                              spdy - 1
177  kerberos                          Mv: 1
178  clearcase                         Mv: 1
179  ms-update                         Mv: 1
      Iv:                               ssl - 1
      Iv:                              http - 20
      Iv:                             ms-sms - 1
      Iv:                               spdy - 1
180  mysql                             Mv: 1
      Iv:                               ssl - 1
181  google-services                   Mv: 1
      Iv:                               ssl - 1
      Iv:                              spdy - 1
182  google-plus                       Mv: 1
      Iv:                               ssl - 1
      Iv:                              spdy - 1
183  google-docs                       Mv: 1
      Iv:                               ssl - 1
      Iv:                              spdy - 1
184  picasa                            Mv: 1
      Iv:                               ssl - 1
      Iv:                              spdy - 1
185  blogger                           Mv: 1
      Iv:                              http - 20
      Iv:                               ssl - 1
      Iv:                            gmail - 1
      Iv:                     google-services - 1
      Iv:                              spdy - 1
186  sqlserver                         Mv: 1
      Iv:                              cifs - 2
187  adobe-connect                     Mv: 1
      Iv:                              rtmp - 1
      Iv:                               ssl - 1
```

```
      Iv:                              http - 20
      Iv:                              spdy - 1
188   aol-messenger-audio              Mv: 1
      Iv:                               rtp - 8
189   aol-messenger-video              Mv: 1
      Iv:              aol-messenger-audio - 1
      Iv:                               rtp - 8
      Iv:                              http - 20
      Iv:                          stun-nat - 1
      Iv:                              rtmp - 1
190   aol-messenger-ft                 Mv: 1
      Iv:              aol-messenger-audio - 1
191   facebook                         Mv: 1
      Iv:                              http - 20
      Iv:                               ssl - 1
192   xunlei                           Mv: 1
      Iv:                              http - 20
      Iv:                    xunlei-kankan - 1
      Iv:                       webthunder - 1
193   xunlei-kankan                    Mv: 1
      Iv:                              http - 20
      Iv:                         xunlei - 1
194   ms-sql-m                         Mv: 1
195   ssh                              Mv: 1
196   hopopt                           Mv: 1
197   mikogo                           Mv: 1
      Iv:                              http - 20
      Iv:                               ssl - 1
198   ipv6-frag                        Mv: 1
199   ipv6-nonxt                       Mv: 1
200   ipv6-opts                        Mv: 1
201   ipv6-route                       Mv: 1
202   salesforce                       Mv: 1
      Iv:                              http - 20
      Iv:                               ssl - 1
203   twitter                          Mv: 1
      Iv:                              http - 20
      Iv:                               ssl - 1
204   hulu                             Mv: 1
      Iv:                              http - 20
      Iv:                               ssl - 1
205   oscar-filetransfer               Mv: 1
      Iv:              aol-messenger-audio - 1
206   logmein                          Mv: 1
      Iv:                               ssl - 1
      Iv:                              http - 20
      Iv:                              spdy - 1
207   iscsi                            Mv: 1
208   yahoo-mail                       Mv: 1
      Iv:                              http - 20
      Iv:                               ssl - 1
      Iv:                              spdy - 1
209   linkedin                         Mv: 1
      Iv:                              http - 20
      Iv:                               ssl - 1
210   showmypc                         Mv: 1
      Iv:                               ssl - 1
      Iv:                              http - 20
      Iv:                              rtmp - 1
      Iv:                              spdy - 1
211   gbridge                          Mv: 1
      Iv:                              http - 20
212   ms-lync                          Mv: 1
      Iv:                          stun-nat - 1
      Iv:                              http - 20
      Iv:                               ssl - 1
213   ms-lync-media                    Mv: 1
      Iv:                          stun-nat - 1
      Iv:                               rtp - 8
      Iv:                               ssl - 1
214   spdy                             Mv: 1
      Iv:                               ssl - 1
215   facetime                         Mv: 1
```

```
      Iv:                          stun-nat - 1
      Iv:                               sip - 5
      Iv:                               ssl - 1
216   yahoo-accounts                  Mv: 1
      Iv:                             http - 20
      Iv:                              ssl - 1
217   pptv                            Mv: 1
      Iv:                             http - 20
218   net-assistant                   Mv: 1
219   apple-remote-desktop            Mv: 1
      Iv:                              vnc - 1
220   lotus-notes                     Mv: 1
221   webex-media                     Mv: 1
      Iv:                             http - 20
222   webex-app-sharing               Mv: 1
      Iv:                             http - 20
223   notes                           Mv: 1
224   qqlive                          Mv: 1
      Iv:                             http - 20
225   bittorrent-networking           Mv: 1
      Iv:                        bittorrent - 5
      Iv:                             http - 20
      Iv:                              dht - 1
226   shoutcast                       Mv: 1
      Iv:                             http - 20
227   dameware-mrc                    Mv: 1
228   iana                            Mv: 1
229   custom-protocols                Mv: 1
230   attribute                       Mv: 1


{<No.>}<PDLM name> Mv: <PDLM Version>, {Nv: <NBAR Software Version>; <File name>}
            {Iv: <PDLM Interdependency Name>   - <PDLM Interdependency Version>}


------------------ show ip nbar protocol-pack active ------------------



Active Protocol Pack:

Name:                            Advanced Protocol Pack
Version:                         4.10001
Publisher:                       Cisco Systems Inc.
NBAR Engine Version:             16
State:                           Active


------------------ show ip nbar resources flow ------------------


------------------ show ip nbar attribute-map ------------------


% NBAR Error: No attribute-map configured

------------------ show ip nbar parameter extraction        activated ------------------


 Protocol        Parameter            ID
 --------        ---------            --

------------------ show ip nbar parameter subclassification        activated
------------------


 Protocol        Parameter          Parameter value        ID
```

```
--------        ---------          ---------------        --

------------------ show ip nbar protocol-discovery ------------------


Ethernet1/1

Last clearing of "show ip nbar protocol-discovery" counters 00:28:02

                           Input                     Output
                           -----                     ------
  Protocol                 Packet Count              Packet Count
                           Byte Count                Byte Count
                           5min Bit Rate (bps)       5min Bit Rate (bps)
                           5min Max Bit Rate (bps)   5min Max Bit Rate (bps)
  ------------------------ ------------------------- -------------------------
  Total                    0                         0
                           0                         0
                           0                         0
                           0                         0

Tunnel21

Last clearing of "show ip nbar protocol-discovery" counters 00:23:09

                           Input                     Output
                           -----                     ------
  Protocol                 Packet Count              Packet Count
                           Byte Count                Byte Count
                           5min Bit Rate (bps)       5min Bit Rate (bps)
                           5min Max Bit Rate (bps)   5min Max Bit Rate (bps)
  ------------------------ ------------------------- -------------------------
  Total                    0                         0
                           0                         0
                           0                         0
                           0                         0

------------------ show policy-map interface ------------------
```

# show tech-support rsvp

To generate a report of all Resource Reservation Protocol (RSVP)-related information, use the **showtech-supportrsvp**command in privileged EXEC mode.

**show tech-support rsvp**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command is not required for normal use of the operating system. This command is useful when you contact technical support personnel with questions regarding RSVP. The **showtech-supportrsvp**command generates a series of reports that can be useful to technical support personnel attempting to solve problems.

Any issues or caveats that apply to the **showtech-support** command also apply to this command. For example, the enable password, if configured, is not displayed in the output of the **showrunning-config** command.

## Examples

The **showtech-supportrsvp** command is equivalent to issuing the following commands:

- **show ip rsvp installed**
- **show ip rsvp interface**
- **show ip rsvp neighbor**
- **show ip rsvp policy cops**
- **show ip rsvp reservation**
- **show ip rsvp sender**
- **show running-config**
- **show version**

For the specific examples, refer to the displays and descriptions for the individual commands for more information.

# show traffic-shape

**Note** Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **showtraffic-shape**command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide* .

**Note** Effective with Cisco IOS XE Release 3.2S, the **showtraffic-shape**command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* .

To display the current traffic-shaping configuration, use the **showtraffic-shape** command in EXEC mode.

**show traffic-shape** [*interface-type interface-number*]

## Syntax Description

| | |
|---|---|
| *interface-type* | (Optional) The type of the interface. If no interface is specified, traffic-shaping details for all configured interfaces are shown. |
| *interface-number* | (Optional) The number of the interface. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.6 | This command was modified. This command was hidden. |
| 15.0(1)S | This command was modified. This command was hidden. |

| Release | Modification |
|---|---|
| 15.1(3)T | This command was modified. This command was hidden. |
| Cisco IOS XE Release 3.2S | This command was replaced by an MQC command (or sequence of MQC commands). |

## Usage Guidelines

You must have first enabled traffic shaping using the **traffic-shaperate**, **traffic-shapegroup**, or **frame-relaytraffic-shaping** command to display traffic-shaping information.

## Examples

The following is sample output from the **showtraffic-shape** command:

```
Router# show traffic-shape
Interface   Fa0/0
       Access Target    Byte   Sustain   Excess    Interval  Increment Adapt
VC     List   Rate      Limit  bits/int  bits/int  (ms)      (bytes)   Active
-             1000000   6250   25000     25000     25        3125      -
```

The table below describes the significant fields shown in the display.

***Table 256: show traffic-shape Field Descriptions***

| Field | Description |
|---|---|
| Interface | Interface type and number. |
| VC | Virtual circuit.<br>**Note** If you configure traffic shaping at a VC level instead of an interface level, a number appears in this field. |
| Access List | Number of the access list, if one is configured. |
| Target Rate | Rate that traffic is shaped to, in bits per second. |
| Byte Limit | Maximum number of bytes sent per internal interval. |
| Sustain bits/int | Configured sustained bits per interval. |
| Excess bits/int | Configured excess bits in the first interval. |
| Interval (ms) | Interval (in milliseconds) being used internally, which may be smaller than the committed burst divided by the committed information rate, if the router determines that traffic flow will be more stable with a smaller configured interval. |
| Increment (bytes) | Number of bytes that will be sustained per internal interval. |

| Field | Description |
|---|---|
| Adapt Active | Contains "BECN" if Frame Relay has backward explicit congestion notification (BECN) adaptation configured. |

## Related Commands

| Command | Description |
|---|---|
| **frame-relay cir** | Specifies the incoming or outgoing committed information rate (CIR) for a Frame Relay virtual circuit. |
| **frame-relay traffic-rate** | Configures all the traffic-shaping characteristics of a virtual circuit (VC) in a single command. |
| **frame-relay traffic-shaping** | Enables both traffic shaping and per-VC queueing for all PVCs and SVCs on a Frame Relay interface. |
| **show traffic-shape queue** | Displays information about the elements queued by traffic shaping at the interface level or the DLCI level. |
| **show traffic-shape statisitcs** | Displays the current traffic-shaping statistics. |
| **traffic-shape adaptive** | Configures a Frame Relay subinterface to estimate the available bandwidth when BECN signals are received. |
| **traffic-shape fecn-adap** | Replies to messages with the FECN bit (which are set with TEST RESPONSE messages with the BECN bit set). |
| **traffic-shape group** | Enables traffic shaping based on a specific access list for outbound traffic on an interface. |
| **traffic-shape rate** | Enables traffic shaping for outbound traffic on an interface. |

# show traffic-shape queue

**Note** Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **showtraffic-shapequeue**command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide* .

**Note** Effective with Cisco IOS XE Release 3.2S, the **showtraffic-shapequeue**command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* .

To display information about the elements queued by traffic shaping at the interface level or the data-link connection identifier (DLCI) level, use the **showtraffic-shapequeue**command in privileged EXEC mode.

**show traffic-shape queue** [*interface-number* [**dlci** *dlci-number*]]

## Syntax Description

| | |
|---|---|
| *interface-number* | (Optional) The number of the interface. |
| **dlci** | (Optional) The specific DLCI for which you wish to display information about queued elements. |
| *dlci-number* | (Optional) The number of the DLCI. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.0(3)XG | This command was integrated into Cisco IOS Release 12.0(3)XG. The *dlci* argument was added. |
| 12.0(4)T | This command was integrated into Cisco IOS Release 12.0(4)T. The *dlci* argument was added. |

| Release | Modification |
|---|---|
| 12.0(5)T | This command was modified to include information on the special voice queue that is created using the **queue** keyword of the **frame-relayvoicebandwidth** command. |
| 12.2(28)SB | This command was modified to support hierarchical queueing framework (HQF) on Frame Relay (FR) interfaces or permanent virtual circuits (PVCs). |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.6 | This command was modified. This command was hidden. |
| 15.0(1)S | This command was modified. This command was hidden. |
| 15.1(3)T | This command was modified. This command was hidden. |
| Cisco IOS XE Release 3.2S | This command was replaced by an MQC command (or sequence of MQC commands). |

## Usage Guidelines

When no parameters are specified with this command, the output displays information for all interfaces and DLCIs containing queued elements. When a specific interface and DLCI are specified, information is displayed about the queued elements for that DLCI only.

When you use this command with HQF, no output displays.

## Examples

The following is sample output for the **showtraffic-shapequeue**command when weighted fair queueing is configured on the map class associated with DLCI 16:

```
Router# show traffic-shape queue Serial1/1 dlci 16
Traffic queued in shaping queue on Serial1.1 dlci 16
  Queueing strategy: weighted fair
  Queueing Stats: 1/600/64/0 (size/max total/threshold/drops)
     Conversations  0/16 (active/max total)
     Reserved Conversations 0/2 (active/allocated)
  (depth/weight/discards) 1/4096/0
  Conversation 5, linktype: ip, length: 608

source: 172.21.59.21, destination: 255.255.255.255, id: 0x0006, ttl: 255,
  TOS: 0 prot: 17, source port 68, destination port 67
```

The following is sample output for the **showtraffic-shapequeue**command when priority queueing is configured on the map class associated with DLCI 16:

```
Router# show traffic-shape queue Serial1/1 dlci 16
Traffic queued in shaping queue on Serial1.1 dlci 16
  Queueing strategy: priority-group 4
  Queueing Stats: low/1/80/0 (queue/size/max total/drops)
Packet 1, linktype: cdp, length: 334, flags: 0x10000008
```

The following is sample output for the **showtraffic-shapequeue**command when first-come, first-serve queueing is configured on the map class associated with DLCI 16:

```
Router# show traffic-shape queue Serial1/1 dlci 16
Traffic queued in shaping queue on Serial1.1 dlci 16
  Queueing strategy: fcfs
  Queueing Stats: 1/60/0 (size/max total/drops)
Packet 1, linktype: cdp, length: 334, flags: 0x10000008
```

The following is sample output for the **showtraffic-shapequeue** command displaying statistics for the special queue for voice traffic that is created automatically when the **frame-relayvoicebandwidth**command is entered:

```
Router# show traffic-shape queue Serial1/1 dlci 45

 Voice queue attached to traffic shaping queue on Serial1 dlci 45
 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    Voice Queueing Stats: 0/100/0 (size/max/dropped)
    ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
 Traffic queued in shaping queue on Serial1 dlci 45
   Queueing strategy: weighted fair
   Queueing Stats: 0/600/64/0 (size/max total/threshold/drops)
      Conversations  0/16 (active/max total)
      Reserved Conversations 0/2 (active/allocated)
```

The table below describes the significant fields shown in the display.

***Table 257: show traffic-shape queue Field Descriptions***

| Field | Description |
|---|---|
| Queueing strategy | When Frame Relay Traffic Shaping (FRTS) is configured, the queueing type can be weighted fair, custom-queue, priority-group, or fcfs (first-come, first-serve), depending on what is configured on the Frame Relay map class for this DLCI. The default is fcfs for FRTS. When generic traffic shaping is configured, the only queueing type available is weighted fair queueing (WFQ). |
| Queueing Stats | Statistics for the configured queueing strategy, as follows:<br>• size--Current size of the queue.<br>• max total--Maximum number of packets of all types that can be queued in all queues.<br>• threshold--For WFQ, the number of packets in the queue after which new packets for high-bandwidth conversations will be dropped.<br>• drops--Number of packets discarded during this interval. |
| Conversations active | Number of currently active conversations. |
| Conversations max total | Maximum allowed number of concurrent conversations. |

| Field | Description |
|---|---|
| Reserved Conversations active | Number of currently active conversations reserved for voice. |
| Reserved Conversations allocated | Maximum configured number of conversations reserved. |
| depth | Number of packets currently queued. |
| weight | Number used to classify and prioritize the packet. |
| discards | Number of packets discarded from queues. |
| Packet | Number of queued packet. |
| linktype | Protocol type of the queued packet. (cdp = Cisco Discovery Protocol) |
| length | Number of bytes in the queued packet. |
| flags | Number of flag characters in the queued packet. |
| source | Source IP address. |
| destination | Destination IP address. |
| id | Packet ID. |
| ttl | Time to live count. |
| TOS | IP type of service. |
| prot | Layer 4 protocol number. Refer to RFC 943 for a list of protocol numbers. (17 = User Datagram Protocol (UDP)) |
| source port | Port number of source port. |
| destination port | Port number of destination port. |

## Related Commands

| Command | Description |
|---|---|
| **show frame-relay fragment** | Displays Frame Relay fragmentation details. |
| **show frame-relay pvc** | Displays statistics about PVCs for Frame Relay interfaces. |

| Command | Description |
|---|---|
| **show frame-relay vofr** | Displays details about FRF.11 subchannels being used on VoFR DLCIs. |
| **show traffic-shape** | Displays the current traffic-shaping configuration. |
| **show traffic-shape statistics** | Displays the current traffic-shaping statistics. |

# show traffic-shape statistics

**Note** Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **showtraffic-shapestatistics**command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide* .

**Note** Effective with Cisco IOS XE Release 3.2S, the **showtraffic-shapestatistics**command is replaced by a modular QoS CLI (MQC) command (or sequence of MQC commands). For the appropriate replacement command (or sequence of commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* .

To display the current traffic-shaping statistics, use the **showtraffic-shapestatistics**command in EXEC mode.

**show traffic-shape statistics** [*interface-type interface-number*]

## Syntax Description

| | |
|---|---|
| *interface-type* | (Optional) The type of the interface. If no interface is specified, traffic-shaping statistics for all configured interfaces are shown. |
| *interface-number* | (Optional) The number of the interface. |

## Command Modes

EXEC

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.6 | This command was modified. This command was hidden. |

| Release | Modification |
|---|---|
| 15.0(1)S | This command was modified. This command was hidden. |
| 15.1(3)T | This command was modified. This command was hidden. |
| Cisco IOS XE Release 3.2S | This command was replaced by an MQC command (or sequence of MQC commands). |

## Usage Guidelines

You must have first enabled traffic shaping using the **traffic-shaperate**, **traffic-shapegroup**, or **frame-relaytraffic-shaping** command to display traffic-shaping information.

## Examples

The following is sample output from the **showtraffic-shapestatistics** command:

```
Router# show traffic-shape statistics
          Access Queue     Packets   Bytes     Packets   Bytes     Shaping
I/F       List   Depth                        Delayed   Delayed   Active
Et0       101    0         2         180       0         0         no
Et1              0         0         0         0         0         no
```

The table below describes the significant fields shown in the display.

***Table 258: show traffic-shape statistics Field Descriptions***

| Field | Description |
|---|---|
| I/F | Interface. |
| Access List | Number of the access list. |
| Queue Depth | Number of messages in the queue. |
| Packets | Number of packets sent through the interface. |
| Bytes | Number of bytes sent through the interface. |
| Packets Delayed | Number of packets sent through the interface that were delayed in the traffic-shaping queue. |
| Bytes Delayed | Number of bytes sent through the interface that were delayed in the traffic-shaping queue. |
| Shaping Active | Contains “yes” when timers indicate that traffic shaping is occurring and “no” if traffic shaping is not occurring. |

## Related Commands

| Command | Description |
|---|---|
| **frame-relay traffic-shaping** | Enables both traffic shaping and per-VC queueing for all PVCs and SVCs on a Frame Relay interface. |
| **show interfaces** | Displays statistics for all interfaces configured on the router or access server. |
| **show ip rsvp neighbor** | Displays RSVP-related interface information. |
| **traffic-shape adaptive** | Configures a Frame Relay subinterface to estimate the available bandwidth when BECN signals are received. |
| **traffic-shape group** | Enables traffic shaping based on a specific access list for outbound traffic on an interface. |
| **traffic-shape rate** | Enables traffic shaping for outbound traffic on an interface. |

# show vrf

To display the defined Virtual Private Network (VPN) routing and forwarding (VRF) instances, use the **showvrf**command in user EXEC or privileged EXEC mode.

**show vrf** [**ipv4**| **ipv6**] [**interface**| **brief**| **detail**| **id**| **select**| **lock**] [ *vrf-name* ]

## Syntax Description

| | |
|---|---|
| **ipv4** | (Optional) Displays IPv4 address family-type VRF instances. |
| **ipv6** | (Optional) Displays IPv6 address family-type VRF instances. |
| **interface** | (Optional) Displays the interface associated with the specified VRF instances. |
| **brief** | (Optional) Displays brief information about the specified VRF instances. |
| **detail** | (Optional) Displays detailed information about the specified VRF instances. |
| **id** | (Optional) Displays VPN-ID information for the specified VRF instances. |
| **select** | (Optional) Displays selection information for the specified VRF instances. |
| **lock** | (Optional) Displays VPN lock information for the specified VRF instances. |
| *vrf-name* | (Optional) Name assigned to a VRF. |

## Command Default

If you do not specify any arguments or keywords, the command displays concise information about all configured VRFs.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.2(33)SRB | This command was introduced. |
| 12.2(33)SXH | This command was integrated into Cisco IOS Release 12.2(33)SXH. |

| Release | Modification |
|---|---|
| 12.2(33)SB | This command was integrated into Cisco IOS Release 12.2(33)SB. |
| 12.4(20)T | This command was integrated into Cisco IOS Release 12.4(20)T. |
| Cisco IOS XE Release 2.1 | This command was integrated into Cisco IOS XE Release 2.1. |
| 12.2(33)SRE | This command was modified. When backup paths have been created either through the Prefix Independent Convergence or Best External feature, the output of the **showvrfdetail** command displays the following line:<br>Prefix protection with additional path enabled |
| 15.0(1)S | This command was integrated into Cisco IOS Release 15.0(1)S. |

## Usage Guidelines

Use the **showvrf** command to display information about specified VRF instances or all VRF instances. Specify no arguments or keywords to display information on all VRF instances.

## Examples

The following sample output from the**showvrf**command displays brief information about all configured VRF instances:

```
Router# show vrf
  Name                              Default RD          Protocols   Interfaces
  N1                                100:0               ipv4,ipv6
  V1                                1:1                 ipv4        Lo1
  V2                                2:2                 ipv4,ipv6   Et0/1.1
                                                                    Et0/1.2
                                                                    Et0/1.3
  V3                                3:3                 ipv4        Lo3
                                                                    Et0/1.4
```

The table below describes the significant fields shown in the display.

***Table 259: show vrf Field Descriptions***

| Field | Description |
|---|---|
| Name | Name of the VRF instance. |
| Default RD | The default route distinguisher (RD) for the specified VRF instances. |
| Protocols | The address family protocol type for the specified VRF instance. |
| Interfaces | The network interface associated with the VRF instance. |

The following sample output from the **showvrf** command with the **detail** keyword displays information for a VRF named cisco:.

```
Router# show vrf detail
VRF cisco1; default RD 100:1; default VPNID <not set>
  Interfaces:
    Ethernet0/0                 Loopback10
Address family ipv4 (Table ID = 0x1):
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
Address family ipv6 (Table ID = 0xE000001):
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
```

The table below describes the significant fields shown in the display.

***Table 260: show vrf detail Field Descriptions***

| Field | Description |
|---|---|
| default RD 100:1 | The RD given to this VRF. |
| Interfaces: | Interfaces to which the VRF is attached. |
| Export VPN route-target communities<br>RT:100:1 | Route-target VPN extended communities to be exported. |
| Import VPN route-target communities<br>RT:100:1 | Route-target VPN extended communities to be imported. |

The following example displays output from the **showvrfdetail** command when backup paths have been created either through the Prefix Independent Convergence or Best External feature. The output of the **showvrfdetail** command displays the following line:

Prefix protection with additional path enabled

```
Router# show vrf detail
VRF vpn1 (VRF Id = 1); default RD 1:1; default VPNID <not set>
  Interfaces:
    Et1/1
Address family ipv4 (Table ID = 1 (0x1)):
  Export VPN route-target communities
    RT:1:1
  Import VPN route-target communities
    RT:1:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
```

```
Prefix protection with additional path enabled
Address family ipv6 not active.
```

The following sample output from the **showvrflock** command displays VPN lock information:

```
Router# show vrf lock
VRF Name: Mgmt-intf; VRF id = 4085 (0xFF5)
VRF lock count: 3
         Lock user: RTMGR, lock user ID: 2, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :108
         Lock user: CEF, lock user ID: 4, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :10C
         Lock user: VRFMGR, lock user ID: 1, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+21EAD18 :10C
VRF Name: vpn1; VRF id = 1 (0x1)
VRF lock count: 3
         Lock user: RTMGR, lock user ID: 2, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :10C
         Lock user: CEF, lock user ID: 4, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+45A9F04 :100
         Lock user: VRFMGR, lock user ID: 1, lock count per user: 1
         Caller PC tracebacks:
         Trace backs: :10000000+44DAEB4 :10000000+21E83AC :10000000+21EAD18 :10C
```

## Related Commands

| Command | Description |
|---|---|
| **vrf definition** | Configures a VRF routing table instance and enters VRF configuration mode. |
| **vrf forwarding** | Associates a VRF instance with an interface or subinterface. |

# show wrr-queue

To display the queue information that is serviced on a weighted round-robin (WRR) scheduling basis, use the **showwrr-queue**command in user EXEC or privileged EXEC mode.

**show wrr-queue** {**bandwidth**| **cos-map**}

## Syntax Description

| | |
|---|---|
| **bandwidth** | Displays the bandwidth information. |
| **cos-map** | Displays the class of service (CoS) map information. |

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| 12.4(24)T | This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T. |

## Usage Guidelines

Use this command to display the queue information that is scheduled for servicing on WRR basis. WRR is a type of scheduling that prevents low-priority queues from being completely neglected during periods of high-priority traffic. The WRR scheduler transmits some packets from each queue in turn. The number of packets that the scheduler transmits corresponds to the relative importance of the queue.

## Examples

The following is sample output from the **showwrr-queue**command. The fields are self-explanatory.

```
Router# show wrr-queue bandwidth
wrr-queue bandwidth for Etherswitch HWIC is:
WRR Queue  :   1   2   3   4
Bandwidth  :   1   2   4   8


Router# show wrr-queue cos-map
wrr-queue cos_map for Etherswitch HWIC is:
CoS Value      :  0  1  2  3  4  5  6  7
Priority Queue :  1  1  2  2  3  3  4  4
```

# subscriber accounting accuracy

To guarantee Input/Ouput Packet/Byte statistics in the accounting Stop record are accurate within 1 second, use the **subscriberaccountingaccuracy** command in privileged EXEC mode. To disable this statistics setting, use the **no** form of this command.

**subscriber accounting accuracy** *value*

**no subscriber accounting accuracy**

## Syntax Description

| | |
|---|---|
| *value* | Value for the Subscriber Accounting Accuracy feature in milliseconds. The range is 1,000 to 10,000. |

## Command Default

The default value is 1000 milliseconds.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release XE 3.2S | This command was introduced on the ASR 1000 Series Routers. |

## Examples

This section shows an example of the **subscriberaccountingaccuracy**command set to its default value:

```
Router# subscriber accounting accuracy 1000
```

# svc-bundle

To create or modify a member of a switched virtual circuit (SVC) bundle, use the **svc-bundle** command in SVC-bundle configuration mode. To remove an SVC bundle member from the bundle, use the **no** form of this command.

**svc-bundle** *svc-handle*

**no svc-bundle** *svc-handle*

## Syntax Description

| | |
|---|---|
| *svc-handle* | Unique name for the SVC in the router. |

## Command Default

No SVCs are members of an SVC bundle.

## Command Modes

SVC-bundle configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(4)T | This command was introduced. |

## Usage Guidelines

Using this command will cause the system to enter SVC-bundle member configuration mode, in which you can configure characteristics of the member such as precedence, variable bit rate (VBR) traffic shaping, unspecified bit rate (UBR) traffic shaping, UBR+ traffic shaping, an idle timeout, and bumping conditions.

## Examples

The following example creates a member of an SVC bundle named “five”:

```
svc-bundle five
```

# table-map (value mapping)

To create and configure a mapping table for mapping and converting one packet-marking value to another, use the **table-map** (value mapping) command in global configuration mode. To disable the use of this table map, use the **no** form of this command.

**table-map** *table-map-name* **map from** *from-value* **to** *to-value* [**default** *default-value-or-action*]

**no table-map** *table-map-name* **map from** *from-value* **to** *to-value* [**default** *default-value-or-action*]

## Syntax Description

| | |
|---|---|
| *table-map-name* | Name of table map to be created. The name can be a maximum of 64 alphanumeric characters. |
| **map from** | Indicates that a “map from” value will be used. |
| *from-value* | The “map from” value of the packet-marking category. The value range varies according to the packet-marking category from which you want to map and convert. For more information, see the “Usage Guidelines” section below. |
| **to** | Indicates that a “map to” value will be used. |
| *to-value* | The “map to” value of the packet-marking category. The value range varies according to the packet-marking category to which you want to map and convert. For more information, see the “Usage Guidelines” section below. |
| **default** | (Optional) Indicates that a default value or action will be used. |
| *default-value-or-action* | (Optional) The default value or action to be used if a “to-from” relationship has not been explicitly configured. Default actions are “ignore” and “copy”. If neither action is specified, “copy” is used. |

## Command Default

The **default** keyword and *default-value-or-action* argument sets the default value (or action) to be used if a value if not explicitly designated.

If you configure a table map but you do not specify a *default-value-or-action* argument for the **default**keyword, the default action is “copy”.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(13)T | This command was introduced. |

## Usage Guidelines

This command allows you to create a mapping table. The mapping table, a type of conversion chart, is used for establishing a "to-from" relationship between packet-marking types or categories. For example, a mapping table can be used to establish a "to-from" relationship between the following packet-marking categories:

- Class of service (CoS)
- Precedence
- Differentiated services code point (DSCP)
- Quality of service (QoS) group
- Multiprotocol Label Switching (MPLS) experimental (EXP) imposition
- MPLS EXP topmost

When configuring the table map, you must specify the packet-marking values to be used in the conversion. The values you can enter vary by packet-marking category.

The table below lists the valid value ranges you can enter for each packet-marking category.

***Table 261: Valid Value Ranges***

| Packet-Marking Category | Value Ranges |
|---|---|
| CoS | Specific IEEE 802.1Q number in the range from 0 to 7. |
| Precedence | Number in the range from 0 to 7. |
| DSCP | Number in the range from 0 to 63. |
| QoS Group | Number in the range from 0 to 99. |
| MPLS EXP imposition | Number in the range from 0 to 7. |
| MPLS EXP topmost | Number in the range from 0 to 7. |

## Examples

In the following example, the **table-map**(value mapping)command has been configured to create a table map called "map1". In "map1", two "to-from" relationships have been established and a default value has been defined. The fields for establishing the "to-from" mappings are further defined by the policy map in which the table map will be configured. (Configuring a policy map is the next logical step after creating a table map.)

For instance, a precedence or DSCP value of 0 could be mapped to a CoS value of 0, or vice versa, depending on the how the table map is configured. Any values not explicitly defined in a “to-from” relationship will be set to a default value.

```
Router(config)# table-map map1
Router(config-tablemap)# map from 0 to 0
Router(config-tablemap)# map from 2 to 1
Router(config-tablemap)# default 3
Router(config-tablemap)# end
```

## Related Commands

| Command | Description |
|---|---|
| **policy-map** | Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. |
| **show policy-map** | Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps. |
| **show policy-map class** | Displays the configuration for the specified class of the specified policy map. |
| **show policy-map interface** | Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface. |
| **show table-map** | Displays the configuration of a specified table map or all table maps. |

# tcp

To enable Transmission Control Protocol (TCP) header compression within an IP Header Compression (IPHC) profile, use the **tcp** command in IPHC-profile configuration mode. To disable TCP header compression, use the **no** form of this command.

**tcp**

**no tcp**

## Syntax Description

This command has no arguments or keywords.

## Command Default

TCP header compression is enabled.

## Command Modes

IPHC-profile configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

### Intended for Use with IPHC Profiles

The **tcp**command is intended for use as part of an IPHC profile. An IPHC profile is used to enable and configure header compression on your network. For more information about using IPHC profiles to configure header compression, see the "Header Compression" module and the "Configuring Header Compression Using IPHC Profiles" module of the *Cisco IOS Quality of Service Solutions Configuration Guide* , Release 12.4T.

## Examples

The following is an example of an IPHC profile called profile1. In this example, TCP header compression has been enabled.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile1 van-jacobson
Router(config-iphcp)# tcp
Router(config-iphcp)# end
```

## Related Commands

| Command | Description |
|---|---|
| **iphc-profile** | Creates an IPHC profile. |

# tcp contexts

To set the number of contexts available for Transmission Control Protocol (TCP) header compression, use the **tcpcontexts** command in IPHC-profile configuration mode. To remove the number of previously configured contexts, use the **no** form of this command.

**tcp contexts** {**absolute** *number-of-contexts*| **kbps-per-context** *kbps*}

**no tcp contexts**

## Syntax Description

| | |
|---|---|
| **absolute** | Indicates that the maximum number of compressed TCP contexts will be based on a fixed (absolute) number. |
| *number-of-contexts* | Number of TCP contexts. Range is from 1 to 256. |
| **kbps-per-context** | Indicates that the maximum number of compressed TCP contexts will be based on available bandwidth. |
| *kbps* | Number of kbps to allow for each context. Range is from 1 to 100. |

## Command Default

The **tcpcontexts** command calculates the number of contexts on the basis of bandwidth and allocates 4 kbps per context.

## Command Modes

IPHC-profile configuration

## Command History

| Release | Modification |
|---|---|
| 12.4(9)T | This command was introduced. |

## Usage Guidelines

Use the **tcpcontexts** command to set the number of contexts available for TCP header compression. A context is the state that the compressor uses to compress a header and that the decompressor uses to decompress a header. The context is the uncompressed version of the last header sent and includes information used to compress and decompress the packet.

**Intended for Use with IPHC Profiles**

The **tcpcontexts**command is intended for use as part of an IPHC profile. An IPHC profile is used to enable and configure header compression on your network. For more information about using IPHC profiles to configure header compression, see the "Header Compression" module and the "Configuring Header Compression Using IPHC Profiles" module of the *Cisco IOS Quality of Service Solutions Configuration Guide* , Release 12.4T.

### Setting the Number of Contexts as an Absolute Number

The **tcpcontexts**command allows you to set the number of contexts as an absolute number. To set the number of contexts as an absolute number, enter a number between 1 and 256.

### Calculating the Number of Contexts on the Basis of Bandwidth

The **tcpcontexts**command can calculate the number of contexts on the basis of the bandwidth available on the network link to which the IPHC profile is applied.

To have the number of contexts calculated on the basis of the available bandwidth, enter the **kbps-per-context**keyword followed by a value for the *kbps* argument The command divides the available bandwidth by the kbps specified. For example, if the bandwidth of the network link is 2000 kbps, and you enter 10 for the *kbps* argument, the command calculates 200 contexts.

## Examples

The following is an example of an IPHC profile called profile2. In this example, the number of TCP contexts has been set to 75.

```
Router> enable
Router# configure terminal
Router(config)# iphc-profile profile2 van-jacobson
Router(config-iphcp)# tcp contexts absolute 75
Router(config-iphcp)# end
```

## Related Commands

| Command | Description |
|---|---|
| **iphc-profile** | Creates an IPHC profile. |

# traffic-shape adaptive

To configure a Frame Relay subinterface to estimate the available bandwidth when backward explicit congestion notification (BECN) signals are received, use the **traffic-shapeadaptive** interface configuration command in interface configuration mode. To disregard the BECN signals and not estimate the available bandwidth, use the **no**form of this command.

**traffic-shape adaptive** *bit-rate*

**no traffic-shape adaptive**

## Syntax Description

| | |
|---|---|
| *bit-rate* | Lowest bit rate that traffic is shaped to, in bits per second. The default *bitrate* value is 0. |

## Command Default

Bandwidth is not estimated when BECN signals are received.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command specifies the boundaries in which traffic will be shaped when BECN signals are received. You must enable traffic shaping on the interface with the **traffic-shaperate**or**traffic-shapegroup**command before you can use the **traffic-shapeadaptive** command.

The bit rate specified for the **traffic-shaperate** command is the upper limit, and the bit rate specified for the **traffic-shapeadaptive** command is the lower limit to which traffic is shaped when BECN signals are received on the interface. The rate actually shaped to will be between these two bit rates.

You should configure this command and the **traffic-shapefecn-adapt** command on both ends of the connection to ensure adaptive traffic shaping over the connection, even when traffic is flowing primarily in one direction. The **traffic-shapefecn-adapt** command configures the router to reflect forward explicit congestion notification (FECN) signals as BECN signals.

## Examples

The following example configures traffic shaping on serial interface 0.1 with an upper limit of 128 kbps and a lower limit of 64 kbps. This configuration allows the link to run from 64 to 128 kbps, depending on the congestion level.

```
interface serial 0
 encapsulation-frame-relay
interface serial 0.1
 traffic-shape rate 128000
 traffic-shape adaptive 64000
 traffic-shape fecn-adapt
```

## Related Commands

| Command | Description |
|---|---|
| **show traffic-shape** | Displays the current traffic-shaping configuration. |
| **show traffic-shape statistics** | Displays the current traffic-shaping statistics. |
| **traffic-shape fecn-adapt** | Replies to messages with the FECN bit (which are set with TEST RESPONSE messages with the BECN bit set). |
| **traffic-shape group** | Enables traffic shaping based on a specific access list for outbound traffic on an interface. |
| **traffic-shape rate** | Enables traffic shaping for outbound traffic on an interface. |

# traffic-shape fecn-adapt

To reply to messages with the forward explicit congestion notification (FECN) bit (which are sent with TEST RESPONSE messages with the BECN bit set), use the **traffic-shapefecn-adapt** command in interface configuration mode. To stop backward explicit congestion notification (BECN) signal generation, use the **no**form of this command.

**traffic-shape fecn-adapt**

**no traffic-shape fecn-adapt**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Traffic shaping is disabled.

## Command Modes

Interface configuration (config-if)

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Enable traffic shaping on the interface with the **traffic-shaperate**or **traffic-shapegroup** command. FECN is available only when traffic shaping is configured.

Use this command to reflect FECN bits as BECN bits. Reflecting FECN bits as BECN bits notifies the sending DTE that it is transmitting at a rate too fast for the DTE to handle. Use the **traffic-shapeadaptive** command to configure the router to adapt its transmission rate when it receives BECN signals.

You should configure this command and the **traffic-shapeadaptive** command on both ends of the connection to ensure adaptive traffic shaping over the connection, even when traffic is flowing primarily in one direction.

## Examples

The following example configures traffic shaping on serial interface 0.1 with an upper limit of 128 kbps and a lower limit of 64 kbps. This configuration allows the link to run from 64 to 128 kbps, depending on the congestion level. The router reflects FECN signals as BECN signals.

```
interface serial 0
 encapsulation-frame-relay
interface serial 0.1
 traffic-shape rate 128000
```

```
traffic-shape adaptive 64000
traffic-shape fecn-adapt
```

## Related Commands

| Command | Description |
|---|---|
| **show traffic-shape** | Displays the current traffic-shaping configuration. |
| **show traffic-shape statistics** | Displays the current traffic-shaping statistics. |
| **traffic-shape adaptive** | Configures a Frame Relay subinterface to estimate the available bandwidth when BECN signals are received. |
| **traffic-shape group** | Enables traffic shaping based on a specific access list for outbound traffic on an interface. |
| **traffic-shape rate** | Enables traffic shaping for outbound traffic on an interface. |

# traffic-shape group

To enable traffic shaping based on a specific access list for outbound traffic on an interface, use the **traffic-shapegroup** command in interface configuration mode. To disable traffic shaping on the interface for the access list, use the **no**form of this command.

**traffic-shape group** *access-list bit-rate* [*burst-size* [ *excess-burst-size* ]]

**no traffic-shape group** *access-list*

## Syntax Description

| | |
|---|---|
| *access-list* | Number of the access list that controls the packets that traffic shaping is applied to on the interface. Access list numbers can be numbers from 1 to 2699. |
| *bit-rate* | Bit rate that traffic is shaped to, in bits per second. This is the access bit rate that you contract with your service provider, or the service levels you intend to maintain. Bit rates can be numbers in the range of 8000 to 100000000 bps. |
| *burst-size* | (Optional) Sustained number of bits that can be sent per interval. On Frame Relay interfaces, this is the Committed Burst size contracted with your service provider. Valid entries are numbers in the range of 0 to 100000000. |
| *excess-burst-size* | (Optional) Maximum number of bits that can exceed the burst size in the first interval in a congestion event. On Frame Relay interfaces, this is the Excess Burst size contracted with your service provider. Valid entries are numbers in the range of 0 to 100000000. The default is equal to the *burst-size*argument. |

## Command Default

Disabled

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |

| Release | Modification |
|---|---|
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

Generic traffic shaping is not supported on ISDN and dialup interfaces. It is also not supported on nongeneric routing encapsulation tunnel interfaces. Traffic shaping is not supported with flow switching.

Traffic shaping uses queues to limit surges that can congest a network. Data is buffered and then sent into the network in regulated amounts to ensure that traffic will fit within the promised traffic envelope for the particular connection.

The**traffic-shapegroup** command allows you to specify one or more previously defined access list to shape traffic on the interface. You must specify one **traffic-shapegroup** command for each access list on the interface.

The **traffic-shapegroup** command supports both standard and extended access lists.

Use traffic shaping if you have a network with differing access rates or if you are offering a subrate service. You can configure the values according to your contract with your service provider or the service levels you intend to maintain.

An interval is calculated as follows:

- If the *burst-size* is not equal to zero, the interval is the *burst-size* divided by the *bit-rate* .
- If the *burst-size* is zero, the interval is the *excess-burst-size* divided by the *bit-rate* .

Traffic shaping is supported on all media and encapsulation types on the router. To perform traffic shaping on Frame Relay virtual circuits, you can also use the **frame-relaytraffic-shaping** command. For more information on Frame Relay Traffic Shaping, refer to the "Configuring Frame Relay" chapter in the *Cisco IOS Wide-Area Networking Configuration Guide* .

If traffic shaping is performed on a Frame Relay network with the **traffic-shaperate**command, you can also use the **traffic-shapeadaptive** command to specify the minimum bit rate to which the traffic is shaped.

## Examples

The following example enables traffic that matches access list 101 to be shaped to a certain rate and traffic matching access list 102 to be shaped to another rate on the interface:

```
interface serial 1
 traffic-shape group 101 128000 16000 8000
 traffic-shape group 102 130000 10000 1000
```

## Related Commands

| Command | Description |
|---|---|
| **access-list (IP Standard)** | Defines a standard IP access list. |
| **show traffic-shape** | Displays the current traffic-shaping configuration. |
| **show traffic-shape statistics** | Displays the current traffic-shaping statistics. |

| Command | Description |
|---|---|
| **traffic-shape adaptive** | Configures a Frame Relay subinterface to estimate the available bandwidth when BECN signals are received. |
| **traffic-shape fecn-adapt** | Replies to messages with the FECN bit (which are set with TEST RESPONSE messages with the BECN bit set). |
| **traffic-shape rate** | Enables traffic shaping for outbound traffic on an interface. |

# traffic-shape rate

To enable traffic shaping for outbound traffic on an interface, use the **traffic-shaperate** command in interface configuration mode. To disable traffic shaping on the interface, use the **no**form of this command.

**traffic-shape rate** *bit-rate* [*burst-size* [ *excess-burst-size* ]] [ *buffer-limit* ]

**no traffic-shape rate**

## Syntax Description

| | |
|---|---|
| *bit-rate* | Bit rate that traffic is shaped to, in bits per second. This is the access bit rate that you contract with your service provider, or the service levels you intend to maintain. Bit rates can be in the range of 8000 to 100000000 bps. |
| *burst-size* | (Optional) Sustained number of bits that can be sent per interval. On Frame Relay interfaces, this is the Committed Burst size contracted with your service provider. Valid entries are numbers in the range of 0 to 100000000. |
| *excess-burst-size* | (Optional) Maximum number of bits that can exceed the burst size in the first interval in a congestion event. On Frame Relay interfaces, this is the Excess Burst size contracted with your service provider. Valid entries are numbers in the range of 0 to 100000000. The default is equal to the *burst-size*argument. |
| *buffer-limit* | (Optional) Maximum buffer limit in bps. Valid entries are numbers in the range of 0 to 4096. |

## Command Default

Traffic shaping for outbound traffic is not enabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 11.2 | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

| Release | Modification |
|---|---|
| 12.4(18e) | This command was modified to prevent simultaneous configuration of legacy traffic-shaping and MQC shaping on the same interface. |

## Usage Guidelines

Generic traffic shaping is not supported on ISDN and dialup interfaces. Is is also not supported on nongeneric routing encapsulation tunnel interfaces. Traffic shaping is not supported with flow switching.

Traffic shaping uses queues to limit surges that can congest a network. Data is buffered and then sent into the network in regulated amounts to ensure that traffic will fit within the promised traffic envelope for the particular connection.

Use traffic shaping if you have a network with differing access rates or if you are offering a subrate service. You can configure the values according to your contract with your service provider or the service levels you intend to maintain.

An interval is calculated as follows:

- If the *burst-size* is not equal to zero, the interval is the *burst-size* divided by the *bit-rate*.
- If the *burst-size* is zero, the interval is the *excess-burst-size* divided by the *bit-rate* .

Traffic shaping is supported on all media and encapsulation types on the router. To perform traffic shaping on Frame Relay virtual circuits, you can also use the **frame-relaytraffic-shaping** command. For more information on Frame Relay Traffic Shaping, refer to the "Configuring Frame Relay" chapter in the *Cisco IOS Wide-Area Networking Configuration Guide* .

If traffic shaping is performed on a Frame Relay network with the **traffic-shaperate**command, you can also use the **traffic-shapeadaptive** command to specify the minimum bit rate to which the traffic is shaped.

**Note** Beginning in Cisco IOS Release 12.4(18e), you cannot configure the traffic-shape rate and MQC shaping on the same interface at the same time. You must remove the traffic-shape rate configured on the interface before you attach the service policy. For example, if you try to enter the **service-policy** {**input** | **output**} *policy-map-name* command when the **traffic-shaperate** command is already in effect, this message is displayed: Remove traffic-shape rate configured on the interface before attaching the service-policy. If the MQC shaper is attached first, and you enter the legacy **traffic-shaperate**command on the same interface, the command is rejected and an error message is displayed.

## Examples

The following example enables traffic shaping on serial interface 0 using the bandwidth required by the service provider:

```
interface serial 0
 traffic-shape rate 128000 16000 8000
```

## Related Commands

| Command | Description |
|---|---|
| **show traffic-shape** | Displays the current traffic-shaping configuration. |

| Command | Description |
|---|---|
| **show traffic-shape statistics** | Displays the current traffic-shaping statistics. |
| **traffic-shape adaptive** | Configures a Frame Relay subinterface to estimate the available bandwidth when BECN signals are received. |
| **traffic-shape fecn-adapt** | Replies to messages with the FECN bit (which are set with TEST RESPONSE messages with the BECN bit set). |
| **traffic-shape group** | Enables traffic shaping based on a specific access list for outbound traffic on an interface. |

# trust

To define a trust state for traffic that is classified through the **class** policy-map configuration command, use the **trust** command in policy-map class configuration mode. To return to the default setting, use the **no** form of this command.

**trust** [**cos**| **dscp**| **precedence**]

**no trust** [**cos**| **dscp**| **precedence**]

## Syntax Description

| | |
|---|---|
| **cos** | (Optional) Classifies an ingress packet by using the packet class of service (CoS) value. For an untagged packet, the port default CoS value is used. |
| **dscp** | (Optional) Classifies an ingress packet by using the packet differentiated services code point (DSCP) values (most significant 6 bits of the 8-bit service-type field). For a non-IP packet, the packet CoS value is used if the packet is tagged. If the packet is untagged, the default port CoS value is used to map CoS to DSCP. |
| **precedence** | (Optional) Classifies the precedence of the ingress packet. |

## Command Default

The action is not trusted.

## Command Modes

Policy-map class configuration (config-pmap-c)

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | This command was introduced on the Catalyst 6500 series. |
| 12.2(33)SRA | This command was implemented on the Catalyst 7600 series. |

## Usage Guidelines

Use this command to distinguish the quality of service (QoS) trust behavior for certain traffic from other traffic. For example, inbound traffic with certain DSCP values can be trusted. You can configure a class map to match and trust the DSCP values in the inbound traffic.

Trust values set with this command supersede trust values set with the **qostrust** interface configuration command.

If you specify the **trustcos** command, QoS uses the received or default port CoS value and the CoS-to-DSCP map to generate a DSCP value for the packet.

If you specify the **trustdscp** command, QoS uses the DSCP value from the ingress packet. For non-IP packets that are tagged, QoS uses the received CoS value; for non-IP packets that are untagged, QoS uses the default port CoS value. In either case, the DSCP value for the packet is derived from the CoS-to-DSCP map.

## Examples

The following example shows how to define a port trust state to trust inbound DSCP values for traffic classified with “class1” :

```
Router# configure terminal
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# trust dscp
Router(config-pmap-c)# police 1000000 20000 exceed-action policed-dscp-transmit
Router(config-pmap-c)# end
Router#
```

You can verify your settings by entering the **showpolicy-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class** | Specifies the name of the class whose traffic policy you want to create or change. |
| **police** | Configures the Traffic Policing feature. |
| **policy-map** | Creates a policy map that can be attached to multiple ports to specify a service policy and enters policy-map configuration mode. |
| **set** | Marks IP traffic by setting a CoS, DSCP, or IP-precedence in the packet. |
| **show policy-map** | Displays information about the policy map. |

# tx-ring-limit

To limit the number of packets that can be used on a transmission ring on the digital subscriber line (DSL) WAN interface card (WIC) or interface, use the **tx-ring-limit** command in ATM VC configuration mode. To not limit the number of packets that can be used on a transmission ring on a DSL WIC or interface, use the **no** form of this command.

**tx-ring-limit** *ring-limit*

**no tx-ring-limit** *ring-limit*

## Syntax Description

| | |
|---|---|
| *ring-limit* | Specifies the maximum number of allowable packets that can be placed on the transmission ring. Valid entries can be numbers from 1 to 32767. The default value is 60. On Cisco 1700 series routers, possible values are 2 through 60. On Cisco 2600 and 3600 series routers, possible values are 3 through 60. |

## Command Default

The default value of the *ring-limit* argument is 60.

## Command Modes

ATM VC configuration

## Command History

| Release | Modification |
|---|---|
| 12.0(7)XE1 | This command was introduced. |
| 12.0(9)S | This command was incorporated into Cisco IOS Release 12.0(9)S. |
| 12.1(5)T | This command was integrated into Cisco IOS Release 12.1(5)T. |
| 12.2(2)XK | Support was added for asymmetric digital subscriber line (ADSL), and a transmission (tx) ring setting of 3 was added for latency-critical traffic for ADSL on Cisco 2600 and Cisco 3600 routers. |
| 12.2(4)XL | Support was added for G.SHDSL. |
| 12.2(8)YN | Enhanced quality of service (QoS) features were added for Cisco 1720, Cisco 1750, Cisco 1751, Cisco 1760, Cisco 2610XM-2651XM, Cisco 3640, Cisco 3640A, and Cisco 3660. |
| 12.3(2)T | Support was added for the following platforms: Cisco 1721, Cisco 2610-2651, Cisco 2610XM-2651XM, Cisco 2691, Cisco 3620, and Cisco 3660. |

| Release | Modification |
|---|---|
| 12.3(3a) | Support was added for Packet over SONET (POS) interfaces on Cisco 7200 Series routers. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Examples

The following example configures the transmission ring limit to three packets on an ATM permanent virtual circuit (PVC) subinterface:

```
Router(config)# interface atm1/0.1 point-to-point
Router(config-subif)#

pvc 2/200
Router(config-if-atm-vc)#

tx-ring-limit 3
```

## Related Commands

| Command | Description |
|---|---|
| **show atm vc** | Displays all ATM PVCs and traffic information. |

# vbr-nrt

To configure the variable bit rate-nonreal time (VBR-NRT) quality of service (QoS) and specify output peak cell rate (PCR), output sustainable cell rate (SCR), and output maximum burst cell size for an ATM permanent virtual circuit (PVC), PVC range, switched virtual circuit (SVC), VC class, or VC bundle member, use the **vbr-nrt**command in the appropriate command mode. To remove the VBR-NRT parameters, use the **no** form of this command.

**vbr-nrt** *output-pcr output-scr output-maxburstsize* [ *input-pcr* ] [ *input-scr* ] [ *input-maxburstsize* ]

**no vbr-nrt** *output-pcr output-scr output-maxburstsize* [ *input-pcr* ] [ *input-scr* ] [ *input-maxburstsize* ]

### Cisco 10000 Series Router

**vbr-nrt** *output-pcr output-scr output-maxburstsize*

**no vbr-nrt** *output-pcr output-scr output-maxburstsize*

## Syntax Description

| | |
|---|---|
| *output-pcr* | The output PCR, in kilobytes per second (kbps). |
| *output-scr* | The output SCR, in kbps. |
| *output-maxburstsize* | The output maximum burst cell size, expressed in number of cells. |
| *input-pcr* | (Optional for SVCs only) The input PCR, in kbps. |
| *input-scr* | (Optional for SVCs only) The input SCR, in kbps. |
| *input-maxburstsize* | (Optional for SVCs only) The input maximum burst cell size, expressed in number of cells. |

## Command Default

Unspecified bit rate (UBR) QoS at the maximum line rate of the physical interface is the default.

## Command Modes

ATM PVC-in-range configuration (for an individual PVC within a PVC range) ATM PVC range configuration (for an ATM PVC range) ATM PVP configuration Bundle-vc configuration (for ATM VC bundle members) Interface-ATM-VC configuration (for an ATM PVC or SVC) VC-class configuration (for a VC class)

## Command History

| Release | Modification |
|---|---|
| 11.3T | This command was introduced. |
| 12.0(3)T | This command was enhanced to support configuration of VBR-NRT QoS and specification of output PCR, output SCR, and output maximum burst cell size for ATM bundles and VC bundle members. |

| Release | Modification |
|---|---|
| 12.0(25)SX | This command was integrated into Cisco IOS Release 12.0(25)SX and implemented on the Cisco 10000 series router. |
| 12.1(5)T | This command was made available in PVC range and PVC-in-range configuration modes. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(31)SB2 | This command was integrated into Cisco IOS Release 12.2(31)SB2. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |
| Cisco IOS XE Release 2.3 | This command was made available in ATM PVP configuration mode. |

## Usage Guidelines

Configure QoS parameters using the **ubr**, **ubr+**, or **vbr-nrt** command. The last command you enter will apply to the PVC or SVC you are configuring.

If the **vbr-nrt**command is not explicitly configured on an ATM PVC or SVC, the VC inherits the following default configuration (listed in order of precedence):

- Configuration of any QoS command (**ubr**, **ubr+**, or **vbr-nrt**) in a VC class assigned to the PVC or SVC itself.
- Configuration of any QoS command (**ubr**, **ubr+**, or **vbr-nrt**) in a VC class assigned to the PVC's or SVC's ATM subinterface.
- Configuration of any QoS command (**ubr**, **ubr+**, or **vbr-nrt**) in a VC class assigned to the PVC's or SVC's ATM main interface.
- Global default: UBR QoS at the maximum line rate of the PVC or SVC.

To use this command in VC-class configuration mode, enter the **vc-classatm** global configuration command before you enter the **vbr-nrt**command. This command has no effect if the VC class that contains the command is attached to a standalone VC, that is, if the VC is not a bundle member.

To use this command in bundle-vc configuration mode, enter the **pvc-bundle**configuration command and add the VC as a bundle member.

VCs in a VC bundle are subject to the following configuration inheritance rules (listed in order of precedence):

- VC configuration in bundle-vc mode
- Bundle configuration in bundle mode (with the effect of assigned VC-class configuration)
- Subinterface configuration in subinterface mode

### Cisco 10000 Series Router

Input PCR, input SCR, and input maximum burst size (MBS) are not supported.

For Cisco IOS Release 12.2(31)SB2 and later releases, if you set the output PCR and SCR to the same value, the Cisco IOS software allows a maximum burst cell size of 1. For example:

Prior to Cisco IOS Release 12.2(31)SB2

```
interface ATM2/0/0.81801 point-to-point
 bandwidth 11760
 pvc 81/801
  vbr-nrt 11760 11760 32
  encapsulation aal5snap
  protocol pppoe
```

Cisco IOS Release 12.2(31)SB2 and Later Releases

```
interface ATM2/0/0.81801 point-to-point
 bandwidth 11760
 pvc 81/801
  vbr-nrt 11760 11760 1
  encapsulation aal5snap
  protocol pppoe
```

## Examples

The following example specifies the output PCR for an ATM PVC to be 100,000 kbps, the output SCR to be 50,000 kbps, and the output MBS to be 64:

```
pvc 1/32
 vbr-nrt 100000 50000 64
```

The following example specifies the VBR-NRT output and input parameters for an ATM SVC:

```
svc atm-svc1 nsap 47.0091.81.000000.0040.0B0A.2501.ABC1.3333.3333.05
 vbr-nrt 10000 5000 32 20000 10000 64
```

## Related Commands

| Command | Description |
|---|---|
| **abr** | Selects ABR QoS and configures output peak cell rate and output minimum guaranteed cell rate for an ATM PVC or virtual circuit class. |
| **broadcast** | Configures broadcast packet duplication and transmission for an ATM VC class, PVC, SVC, or VC bundle. |
| **bump** | Configures the bumping rules for a virtual circuit class that can be assigned to a virtual circuit bundle. |
| **bundle** | Creates a bundle or modifies an existing bundle to enter bundle configuration mode. |
| **class-int** | Assigns a VC class to an ATM main interface or subinterface. |
| **class-vc** | Assigns a VC class to an ATM PVC, SVC, or VC bundle member. |
| **encapsulation** | Sets the encapsulation method used by the interface. |

| Command | Description |
|---|---|
| **inarp** | Configures the Inverse ARP time period for an ATM PVC, VC class, or VC bundle. |
| **oam-bundle** | Enables end-to-end F5 OAM loopback cell generation and OAM management for a virtual circuit class that can be applied to a virtual circuit bundle. |
| **oam retry** | Configures parameters related to OAM management for an ATM PVC, SVC, VC class, or VC bundle. |
| **precedence** | Configures precedence levels for a virtual circuit class that can be assigned to a virtual circuit bundle and thus applied to all virtual circuit members of that bundle. |
| **protect** | Configures a virtual circuit class with protected group or protected virtual circuit status for application to a virtual circuit bundle member. |
| **protocol (ATM)** | Configures a static map for an ATM PVC, SVC, VC class, or VC bundle, and enables Inverse ARP or Inverse ARP broadcasts on an ATM PVC by either configuring Inverse ARP directly on the PVC, on the VC bundle, or in a VC class (applies to IP and IPX protocols only). |
| **pvc-bundle** | Adds a PVC to a bundle as a member of the bundle and enters bundle-vc configuration mode in order to configure that PVC bundle member. |
| **ubr** | Configures UBR QoS and specifies the output peak cell rate for an ATM PVC, SVC, VC class, or VC bundle member. |
| **ubr+** | Configures UBR QoS and specifies the output peak cell rate and output minimum guaranteed cell rate for an ATM PVC, SVC, VC class, or VC bundle member. |
| **vc-class atm** | Creates a VC class for an ATM PVC, SVC, or ATM interface, and enters vc-class configuration mode. |

# vc-hold-queue

To configure the per-virtual circuit (VC) hold queue on an ATM adapter, use the **vc-hold-queue** command in interface configuration mode. To return to the default value of the per-VC hold queue, use the **no** form of this command.

**vc-hold-queue** *number-of-packets*

**no vc-hold-queue** *number-of-packets*

## Syntax Description

| | |
|---|---|
| *number-of-packets* | Specifies number of packets that can be configured for the per-VC hold queue. Number of packets can be a minimum of 5 to a maximum of 1024. |

## Command Default

The default value of the hold queue is set by the queueing mechanism in use.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.1(5)T | This command was introduced. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2SX | This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware. |

## Usage Guidelines

This command can only be used on Cisco 7200 series routers and on Cisco 2600 and 3600 adapters that support per-VC queueing.

This command is configurable at the VC level only.

## Examples

The following example sets the per-VC hold queue to 55:

```
interface atm2/0.1
 pvc 1/101
  vc-hold-queue 55
```

## Related Commands

| Command | Description |
|---|---|
| **hold-queue** | Specifies the hold-queue limit of an interface. |
| **show interfaces** | Displays statistics for all interfaces configured on the router or access server. |
| **show queueing interface** | Displays the queueing statistics of an interface or VC. |

# wrr-queue bandwidth

To allocate the bandwidth between the standard transmit queues, use the **wrr-queuebandwidth** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

**wrr-queue bandwidth** *weight-1 ... weight-n*

**no wrr-queue bandwidth**

## Syntax Description

| | |
|---|---|
| *weight-1 ... weight-n* | WRR weights; valid values are fr om 1 to 255. |

## Command Default

The defaults are as follows:

- QoS enabled--4:255
- QoS disabled--255:1

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17a)SX | This command was changed to support seven queue weights. |
| 12.2(17d)SXB | Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB . |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(50)SY | Support for this command was introduced. |

## Usage Guidelin

**Note** In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

You can configure up to seven queue weights on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

You can configure up to three queue weights on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

WRR allows bandwidth sharing at the egress port. This command defines the bandwidths for egress WRR through scheduling weights. Four queues participate in the WRR unless you enable the egress-expedite queue. The expedite queue is a strict-priority queue that is used until it is empty before using one of the WRR queues.

There is no order of dependencies for the **wrr-queuebandwidth** command. If you enable the egress priority, the weight ratio is calculated with the first two and the last parameters; otherwise, all four parameters are used.

The WRR weights are used to partition the bandwidth between the queues if all queues are nonempty. For example, entering weights of 1:3 means that one queue gets 25 percent of the bandwidth and the other queue gets 75 percent as long as both queues have data.

## Examples

This example shows how to allocate a three-to-one bandwidth ratio:

```
Router(config-if)# wrr-queue bandwidth 3 1
```

## Related Commands

| Command | Description |
|---|---|
| **show queueing interface** | Displays queueing information. |
| **wrr-queue queue-limit** | Sets the transmit-queue size ratio on an interface. |

# wrr-queue cos-map

To map CoS values to drop thresholds for a queue, use the **wrr-queuecos-map** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

**wrr-queue cos-map** *queue-id threshold-id cos-1 ... cos-n*

**no wrr-queue cos-map**

## Syntax Description

| | |
|---|---|
| *queue-id* | Queue number; the valid values are from 1 to 2. |
| *threshold-id* | Threshold ID; valid values are from 1 to 2. |
| *cos-1 ... cos-n* | CoS value; valid values are from 0 to 7. |

## Command Default

The defaults are as follows:

- Receive queue 1/drop threshold 1 and transmit queue 1/drop threshold 1: CoS 0 and 1.
- Receive queue 1/drop threshold 2 and transmit queue 1/drop threshold 2: CoS 2 and 3.
- Receive queue 2/drop threshold 3 and transmit queue 2/drop threshold 1: CoS 4 and 6.
- Receive queue 2/drop threshold 4 and transmit queue 2/drop threshold 2: CoS 7.
- On 1p1q4t, 1p2q2t, and 1p3q1t interfaces, CoS 5 is mapped to the strict-priority queues.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(50)SY | Support for this command was introduced. |

## Usage Guidelines

**Note** In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

Enter up to eight CoS values to map to the threshold.

The threshold for 1p3q1t is always 1.

## Examples

This example shows how to map the CoS values 0 and 1 to standard transmit queue 1/threshold 1:

```
Router(config-if)# wrr-queue cos-map 1 1 0 1
```

# awrr-queue dscp-map

To map the hardware Differentiated Services Code Point (DSCP) values to the drop threshold values for a queue, use the **wrr-queuedscp-map** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

**wrr-queue dscp-map** *queue-id threshold-id dscp-1 ... dscp-n*

**no wrr-queue dscp-map** *queue-id*

## Syntax Description

| | |
|---|---|
| *queue-id* | Queue number; valid values are from 1 to 8. |
| *threshold-id* | Threshold ID; valid values are from 1 to 4. |
| *dscp-1 ... dscp-n* | DSCP value; valid values are from 0 to 7. |

## Command Default

The interface is in Class of Service (CoS) mode.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(18)SXF5 | This command was introduced. |
| 12.2(50)SY | Support for this command was introduced. |

## Usage Guidelin

**Note** In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

**Note** To enter the**wrr-queuedscp-map**command, the interface must be in DSCP-queuing mode. Use the **mlsqosqueue-modemode-dscp** command to set the mode to DSCP.

This command is supported on 10-Gigabit Ethernet ports only.

When mapping DSCP values, follow these guidelines:

- You can enter up to eight DSCP values that map to a queue and threshold.
- You can enter multiple commands to map additional DSCP values to the queue and threshold.

- You must enter a separate command for each queue and threshold.

## Examples

This example shows how to map the hardware DSCP values to the drop threshold values for a queue:

```
wrr-queue dscp-map 8 1 0 1 2 3
```

## Related Commands

| | |
|---|---|
| **show queueing interface** | Displays queueing information. |

# wrr-queue queue-limit

To set the transmit-queue size ratio on an interface, use the **wrr-queuequeue-limit** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

**wrr-queue queue-limit** *queue1-weight* [ *queue2-weight* ] *queue3-weight*

**no wrr-queue queue-limit**

## Syntax Description

| | |
|---|---|
| *queue1-weight* | Ratio of the low-priority queue weight; valid values are from 1 and 100 percent. |
| *queue2-weight* | (Optional) Ratio of the medium-priority queue weight; valid values are from 1 and 100 percent. |
| *queue3-weight* | Ratio of the high-priority queue weight; see the "Usage Guidelines" section for valid values. |

## Command Default

The defaults are as follows:

- 90 percent for low priority
- 10 percent for high priority

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(50)SY | Support for this command was introduced. |

## Usage Guidelin

**Note** In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

Valid high-priority weight values are fr om 1 to 100 percent, ex cept on 1p2q1t egress LAN ports, where valid values for the high-priority queue ar e from 5 to 100 percent.

On 1p2q2t interfaces, QoS sets the strict-priority queue size equal to the high-priority queue size.

Estimate the mix of low priority-to-high priority traffic on your network (for example, 80 percent low-priority traffic and 20 percent high-priority traffic). Use the estimated percentages as queue weights.

Due to the granularity of programming the hardware, the values that are set in the hardware are close approximations of the provided values. For example, if you specify 0 percent, the actual value that is programmed is not necessarily 0.

## Examples

This example shows how to configure the transmit-queue size ratio:

```
Router(config-if)# wrr-queue queue-limit 75 25
```

## Related Commands

| Command | Description |
|---|---|
| **show queueing interface** | Displays queueing information. |
| **wrr-queue bandwidth** | Allocates the bandwidth between the standard transmit queues. |

# wrr-queue random-detect

To enable WRED or specify the minimum and maximum WRED threshold for the specified queues on 1p2q2t and 1p3q1t interfaces, use the **wrr-queuerandom-detect** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

**wrr-queue random-detect** *queue-id*

**wrr-queue random-detect** {**max-threshold| min-threshold**} *queue-id threshold-percent-1 ... threshold-percent-n*

**no wrr-queue random-detect** *queue-id*

**no wrr-queue random-detect** {**max-threshold| min-threshold**} *queue-id*

## Syntax Description

| | |
|---|---|
| *queue-id* | Queue number; valid values are 1, 2, or 3. |
| **max-threshold** | Specifies the maximum WRED-drop threshold. |
| **min-threshold** | Specifies the minimum WRED-drop threshold. |
| *threshold-percent-1 threshold-percent-n* | Threshold weights; valid values are from 1 to 100 percent. |

## Command Default

The default is that WRED is disabled. When WRED is enabled, the defaults are as follows:

- The maximum threshold is (low) 40 percent and (high) 100 percent.
- The minimum thresholds are both set to zero.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(50)SY | Support for this command was introduced. |

## Usage Guidelin

**Note** In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

1p2q1t and 1p3q1t interfaces have WRED-drop thresholds in their standard transmit queues. You can configure 1p3q1t transmit queues to use a WRED-drop threshold or a tail-drop threshold.

To enable WRED-drop thresholds on 1p2p1t interfaces, enter the **wrr-queuerandom-detect***queue-id* command. Use the **no** form of this command to disable WRED.

To enable WRED-drop thresholds on 1p3q1t interfaces, enter the **wrr-queuerandom-detect***queue-id* command. To return to the tail-drop threshold, enter the **nowrr-queuerandom-detect***queue-id* command.

The *queue-id* argument is 1 for the standard low-priority queue, 2 for the standard high-priority queue, and 3 for strict priority.

The threshold in the strict-priority queue is not configurable.

Each queue on a 1p2q2t interface has two thresholds; 1p3q1t interfaces have one threshold.

Each threshold has a low and a high WRED value.

WRED values are a percentage of the queue capacity.

For additional information on configuring WRED thresholds, refer to the QoS chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide* .

## Examples

This example shows how to configure the low-priority transmit-queue high-WRED drop thresholds:

```
Router(config-if)# wrr-queue random-detect max-threshold 1 60 100
```

## Related Commands

| Command | Description |
|---|---|
| **show queueing interface** | Displays queueing information. |
| **wrr-queue queue-limit** | Sets the transmit-queue size ratio on an interface. |

# wrr-queue threshold

To configure the drop-threshold percentages for the standard receive and transmit queues on 1q4t and 2q2t interfaces, use the **wrr-queuethreshold** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

**wrr-queue threshold** *queue-id threshold-percent-1 ... threshold-percent-n*

**no wrr-queue threshold** *queue-id*

## Syntax Description

| | |
|---|---|
| *queue-id* | Queue number; valid values are 1 and 2. |
| *threshold-percent-1 threshold-percent-n* | Number of weights for queues 1 and 2; valid valu es are from 1 to 100 percent. |

## Command Default

When you enable QoS, the default values are as follows:

- **100** percent for threshold 1
- **60** percent for threshold 2

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(14)SX | Support for this command was introduced on the Supervisor Engine 720. |
| 12.2(17d)SXB | Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB. |
| 12.2(33)SRA | This command was integrated into Cisco IOS Release 12.2(33)SRA. |
| 12.2(50)SY | Support for this command was introduced. |

## Usage Guidelin

**Note** In Cisco IOS Release 12.2(50)SY and later releases, you can enable this command only if either the **platform qos queueing-only** command or the **auto qos default** command is configured.

Use the transmit queue and threshold numbers.

The *queue-id* argument is 1 for the standard low-priority queue and 2 for the standard high-priority queue.

Always set threshold 2 to 100 percent.

Receive-queue drop thresholds are supported only on Gigabit Ethernet interfaces that are configured to trust CoS.

## Examples

This example shows how to configure receive queue 1/threshold 1 and transmit queue 1/threshold 1:

```
Router(config-if)# wrr-queue threshold 1 60 100
```

## Related Commands

| Command | Description |
|---|---|
| **show queueing interface** | Displays queueing information. |
| **wrr-queue queue-limit** | Sets the transmit-queue size ratio on an interface. |