



Cisco IOS IP Routing: BGP Command Reference

First Published: November 21, 2012

Last Modified: March 22, 2013

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



CONTENTS

CHAPTER 1

BGP Commands: A through B 1

activate (bmp)	4
additional-paths	6
address (bmp)	8
address-family ipv4 (BGP)	10
address-family l2vpn	14
address-family mvpn	17
address-family nsap	19
address-family rtfilter unicast	21
address-family vpnv4	23
advertise additional-paths	25
aggregate-address	27
autodiscovery (MPLS)	31
auto-summary (BGP)	33
bgp additional-paths	36
bgp additional-paths install	39
bgp additional-paths select (additional paths)	41
bgp additional-paths select (diverse path)	44
bgp advertise-best-external	46
bgp aggregate-timer	48
bgp always-compare-med	50
bgp asnotation dot	52
bgp bestpath as-path ignore	56
bgp bestpath compare-routerid	57
bgp bestpath cost-community ignore	59
bgp bestpath igp-metric ignore	61
bgp bestpath med confed	63
bgp bestpath med missing-as-worst	65

bgp bestpath prefix-validate	66
bgp client-to-client reflection	68
bgp client-to-client reflection intra-cluster	71
bgp cluster-id	74
bgp confederation identifier	76
bgp confederation peers	80
bgp consistency-checker	84
bgp dampening	86
bgp default ipv4-unicast	89
bgp default local-preference	91
bgp deterministic-med	93
bgp dmzlink-bw	95
bgp enforce-first-as	97
bgp enhanced-error	99
bgp fast-external-fallover	101
bgp graceful-restart	103
bgp graceful-shutdown all	106
bgp inject-map	109
bgp listen	112
bgp log-neighbor-changes	115
bgp maxas-limit	117
bgp mpls-local-label	119
bgp nexthop	121
bgp nexthop trigger delay	124
bgp nexthop trigger enable	125
bgp nopeerup-delay	126
bgp recursion host	128
bgp redistribute-internal	133
bgp refresh max-eor-time	135
bgp refresh stalepath-time	137
bgp regexp deterministic	139
bgp route-map priority	141
bgp router-id	142
bgp rpki server	144
bgp rr-group	146

bgp scan-time 148
bgp slow-peer detection 151
bgp slow-peer split-update-group dynamic 153
bgp soft-reconfig-backup 155
bgp sso route-refresh-enable 157
bgp suppress-inactive 158
bgp transport 160
bgp update-delay 162
bgp update-group split as-override 164
bgp upgrade-cli 167
bgp-policy 169
bmp 173

CHAPTER 2

BGP Commands: C through I 177

clear bgp l2vpn evpn 180
clear bgp nsap 183
clear bgp nsap dampening 185
clear bgp nsap external 187
clear bgp nsap flap-statistics 188
clear bgp nsap peer-group 190
clear ip bgp 191
clear ip bgp dampening 196
clear ip bgp external 198
clear ip bgp flap-statistics 201
clear ip bgp in prefix-filter 204
clear ip bgp ipv4 205
clear ip bgp ipv6 210
clear ip bgp l2vpn 214
clear ip bgp mvpn 217
clear ip bgp peer-group 219
clear ip bgp rpki server 223
clear ip bgp table-map 225
clear ip bgp update-group 228
clear ip bgp vpnv4 231
clear ip bgp vpnv4 unicast dampening 235

clear ip bgp vpnv6 237

clear ip bgp vpnv6 unicast dampening 241

clear ip prefix-list 243

continue 245

debug ip bgp event rpki 251

debug ip bgp igp-metric ignore 253

debug ip bgp import 254

debug ip bgp route-server 257

default (bmp) 259

default-information originate (BGP) 262

default-metric (BGP) 264

description (bmp) 267

description (route server context) 269

distance bgp 271

distribute-list in (BGP) 273

distribute-list out (BGP) 276

exit-bmp-server-mode (bmp) 279

exit-peer-policy 281

exit-peer-session 282

exit-route-server-context 283

export map (VRF table to global table) 284

failure-retry-delay (bmp) 287

flapping-delay (bmp) 289

ha-mode graceful-restart 291

import ipv4 293

import map 296

import path limit 299

import path selection 301

import-map 304

inherit peer-policy 306

inherit peer-session 308

initial-delay (bmp) 310

ip as-path access-list 312

ip bgp fast-external-fallover 316

ip bgp-community new-format 318

- [ip community-list 320](#)
- [ip extcommunity-list 326](#)
- [ip policy-list 333](#)
- [ip prefix-list 335](#)
- [ip prefix-list description 339](#)
- [ip prefix-list sequence-number 341](#)
- [ip verify unicast vrf 343](#)

CHAPTER 3**BGP Commands: M through N 345**

- [match additional-paths advertise-set 348](#)
- [match as-path 352](#)
- [match community 355](#)
- [match extcommunity 358](#)
- [match local-preference 360](#)
- [match policy-list 362](#)
- [match rpki 364](#)
- [match source-protocol 366](#)
- [maximum-paths eibgp 369](#)
- [maximum-paths ibgp 372](#)
- [mvpn single-forwarder-selection highest-ip-address 376](#)
- [neighbor accept-route-legacy-rt 377](#)
- [neighbor activate 379](#)
- [neighbor additional-paths 383](#)
- [neighbor advertise additional-paths 386](#)
- [neighbor advertise best-external 389](#)
- [neighbor advertise diverse-path 392](#)
- [neighbor advertise-map 395](#)
- [neighbor advertisement-interval 399](#)
- [neighbor allow-policy 401](#)
- [neighbor announce rpki state 403](#)
- [neighbor bmp-activate 406](#)
- [neighbor capability orf prefix-list 408](#)
- [neighbor cluster-id 410](#)
- [neighbor default-originate 412](#)
- [neighbor description 414](#)

neighbor disable-connected-check	416
neighbor distribute-list	418
neighbor dmzlink-bw	422
neighbor ebgp-multihop	424
neighbor fall-over	426
neighbor filter-list	430
neighbor ha-mode graceful-restart	433
neighbor ha-mode sso	435
neighbor inherit peer-policy	437
neighbor inherit peer-session	439
neighbor internal-vpn-client	441
neighbor local-as	443
neighbor maximum-prefix (BGP)	450
neighbor next-hop-self	453
neighbor next-hop-unchanged	455
neighbor password	458
neighbor path-attribute discard	461
neighbor path-attribute treat-as-withdraw	463
neighbor peer-group (assigning members)	465
neighbor peer-group (creating)	467
neighbor prefix-list	470
neighbor remote-as	474
neighbor remove-private-as	480
neighbor route-map	484
neighbor route-reflector-client	487
neighbor route-server-client	490
neighbor send-community	492
neighbor shutdown	495
neighbor slow-peer detection	498
neighbor slow-peer split-update-group dynamic	501
neighbor slow-peer split-update-group static	504
neighbor soft-reconfiguration	506
neighbor soo	508
neighbor suppress-signaling-protocol	511
neighbor timers	513

- neighbor translate-update 515
- neighbor transport 518
- neighbor ttl-security 522
- neighbor unsuppress-map 524
- neighbor update-source 526
- neighbor version 529
- neighbor weight 531
- network (BGP and multiprotocol BGP) 533
- network backdoor 536

CHAPTER 4

BGP Commands: O through show bgp 539

- redistribute (BGP to ISO IS-IS) 541
- redistribute (IP) 544
- redistribute (ISO IS-IS to BGP) 554
- redistribute dvmrp 557
- router bgp 559
- route-server-context 565
- scope 567
- set as-path 569
- set comm-list delete 573
- set community 576
- set dampening 578
- set extcomm-list delete 581
- set extcommunity cost 583
- set extcommunity rt 587
- set extcommunity soo 592
- set extcommunity vpn-distinguisher 596
- set ip dscp (bmp) 599
- set ip next-hop self (BGP) 601
- set ip next-hop (BGP) 602
- set ipv6 next-hop (BGP) 605
- set metric (BGP-OSPF-RIP) 608
- set metric-type internal 611
- set origin (BGP) 613
- set traffic-index 615

[set weight](#) 617
[show bgp all community](#) 620
[show bgp all neighbors](#) 624
[show bgp ipv6](#) 630
[show bgp l2vpn evpn](#) 635
[show bgp l2vpn vpls](#) 639
[show bgp mvpn](#) 643
[show bgp nsap](#) 645
[show bgp nsap community](#) 648
[show bgp nsap community-list](#) 652
[show bgp nsap dampened-paths](#) 655
[show bgp nsap dampening](#) 657
[show bgp nsap filter-list](#) 661
[show bgp nsap flap-statistics](#) 664
[show bgp nsap inconsistent-as](#) 667
[show bgp nsap neighbors](#) 670
[show bgp nsap paths](#) 679
[show bgp nsap quote-regexp](#) 681
[show bgp nsap regexp](#) 684
[show bgp nsap summary](#) 687
[show bgp vpnv6 multicast](#) 690
[show bgp vpnv6 unicast](#) 692

CHAPTER 5

BGP Commands: show ip through Z 695

[show ip as-path-access-list](#) 698
[show ip bgp](#) 700
[show ip bgp bmp](#) 713
[show ip bgp all dampening](#) 716
[show ip bgp cidr-only](#) 719
[show ip bgp cluster-ids](#) 722
[show ip bgp community](#) 725
[show ip bgp community-list](#) 729
[show ip bgp dampened-paths](#) 732
[show ip bgp dampening dampened-paths](#) 734
[show ip bgp dampening flap-statistics](#) 736

[show ip bgp dampening parameters](#) 740

[show ip bgp extcommunity-list](#) 742

[show ip bgp filter-list](#) 744

[show ip bgp flap-statistics](#) 747

[show ip bgp inconsistent-as](#) 749

[show ip bgp injected-paths](#) 750

[show ip bgp ipv4](#) 753

[show ip bgp ipv4 multicast](#) 757

[show ip bgp ipv4 multicast summary](#) 760

[show ip bgp ipv6 multicast](#) 762

[show ip bgp ipv6 unicast](#) 763

[show ip bgp l2vpn](#) 766

[show ip bgp neighbors](#) 773

[show ip bgp path-attribute discard](#) 794

[show ip bgp path-attribute unknown](#) 796

[show ip bgp paths](#) 797

[show ip bgp peer-group](#) 799

[show ip bgp quote-regexp](#) 801

[show ip bgp regexp](#) 805

[show ip bgp replication](#) 809

[show ip bgp rib-failure](#) 811

[show ip bgp rpki servers](#) 813

[show ip bgp rpki table](#) 815

[show ip bgp rtfilter](#) 817

[show ip bgp summary](#) 820

[show ip bgp template peer-policy](#) 828

[show ip bgp template peer-session](#) 831

[show ip bgp unicast route-server](#) 834

[show ip bgp update-group](#) 837

[show ip bgp vpnv4](#) 841

[show ip bgp vpnv4 all dampening](#) 855

[show ip bgp vpnv4 all sso summary](#) 857

[show ip bgp vpnv6 unicast all dampening](#) 859

[show ip community-list](#) 861

[show ip extcommunity-list](#) 863

show ip policy-list 867
show ip prefix-list 868
show ip route 870
show ip route vrf 882
show tcp ha connections 889
slow-peer detection 891
slow-peer split-update-group dynamic 893
slow-peer split-update-group static 895
soo 896
stats-reporting-period (bmp) 899
synchronization 901
table-map 903
template peer-policy 906
template peer-session 910
timers bgp 914
update-source (bmp) 916
ve 918



BGP Commands: A through B

- [activate \(bmp\), page 4](#)
- [additional-paths, page 6](#)
- [address \(bmp\), page 8](#)
- [address-family ipv4 \(BGP\), page 10](#)
- [address-family l2vpn, page 14](#)
- [address-family mvpn, page 17](#)
- [address-family nsap, page 19](#)
- [address-family rtfilter unicast, page 21](#)
- [address-family vpnv4, page 23](#)
- [advertise additional-paths, page 25](#)
- [aggregate-address, page 27](#)
- [autodiscovery \(MPLS\), page 31](#)
- [auto-summary \(BGP\), page 33](#)
- [bgp additional-paths, page 36](#)
- [bgp additional-paths install, page 39](#)
- [bgp additional-paths select \(additional paths\), page 41](#)
- [bgp additional-paths select \(diverse path\), page 44](#)
- [bgp advertise-best-external, page 46](#)
- [bgp aggregate-timer, page 48](#)
- [bgp always-compare-med, page 50](#)
- [bgp asnotation dot, page 52](#)
- [bgp bestpath as-path ignore, page 56](#)
- [bgp bestpath compare-routerid, page 57](#)
- [bgp bestpath cost-community ignore, page 59](#)

- [bgp bestpath igp-metric ignore](#), page 61
- [bgp bestpath med confed](#), page 63
- [bgp bestpath med missing-as-worst](#), page 65
- [bgp bestpath prefix-validate](#), page 66
- [bgp client-to-client reflection](#), page 68
- [bgp client-to-client reflection intra-cluster](#), page 71
- [bgp cluster-id](#), page 74
- [bgp confederation identifier](#), page 76
- [bgp confederation peers](#), page 80
- [bgp consistency-checker](#), page 84
- [bgp dampening](#), page 86
- [bgp default ipv4-unicast](#), page 89
- [bgp default local-preference](#), page 91
- [bgp deterministic-med](#), page 93
- [bgp dmzlink-bw](#), page 95
- [bgp enforce-first-as](#), page 97
- [bgp enhanced-error](#), page 99
- [bgp fast-external-fallover](#), page 101
- [bgp graceful-restart](#), page 103
- [bgp graceful-shutdown all](#), page 106
- [bgp inject-map](#), page 109
- [bgp listen](#), page 112
- [bgp log-neighbor-changes](#), page 115
- [bgp maxas-limit](#), page 117
- [bgp mpls-local-label](#), page 119
- [bgp nexthop](#), page 121
- [bgp nexthop trigger delay](#), page 124
- [bgp nexthop trigger enable](#), page 125
- [bgp nopeerup-delay](#), page 126
- [bgp recursion host](#), page 128
- [bgp redistribute-internal](#), page 133
- [bgp refresh max-eor-time](#), page 135
- [bgp refresh stalepath-time](#), page 137

- [bgp regexp deterministic, page 139](#)
- [bgp route-map priority, page 141](#)
- [bgp router-id, page 142](#)
- [bgp rpki server, page 144](#)
- [bgp rr-group, page 146](#)
- [bgp scan-time, page 148](#)
- [bgp slow-peer detection, page 151](#)
- [bgp slow-peer split-update-group dynamic, page 153](#)
- [bgp soft-reconfig-backup, page 155](#)
- [bgp sso route-refresh-enable, page 157](#)
- [bgp suppress-inactive, page 158](#)
- [bgp transport, page 160](#)
- [bgp update-delay, page 162](#)
- [bgp update-group split as-override, page 164](#)
- [bgp upgrade-cli, page 167](#)
- [bgp-policy, page 169](#)
- [bmp, page 173](#)

activate (bmp)

To initiate a connection between BGP monitoring protocol (BMP) server and BGP neighbors, use the **activate** command in BMP server configuration mode. To stop the connection, use the **no** form of the command.

activate

no activate

Command Default

No connectivity is established between BMP servers and BGP BMP neighbors.

Command Modes

BMP server configuration (config-router-bmpsrvr)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use the **bmp server** command to enter BMP server configuration mode and configure a specific BMP server. To configure BGP BMP neighbors to which the BMP servers establish a connection, use the **neighbor bmp-activate** command in router configuration mode. Use the **show ip bgp bmp** command to verify whether the connection is established or not.

Examples

The following example show how to enter BMP server configuration mode and initiate connection between a specific BMP server with the BGP BMP neighbors. In this example, connection is initiated to BMP server 1 and BMP server 2:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp server 1
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# exit-bmp-server-mode
Device(config-router)# bmp server 2
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# end
```

The following is sample output from the **show ip bgp bmp server** command for BMP server number 1 and 2. The output displays “activated” which indicates that the connection between the two servers has been established with the BGP BM neighbors:

```
Device# show ip bgp bmp server 1

Print detailed info for 1 server number 1.

bmp server 1
address: 10.1.1.1    port 8000
```



```
description SERVER1
up time 00:06:22
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
activated
```

Device# **show ip bgp bmp server 2**

Print detailed info for 1 server number 2.

```
bmp server 2
address: 20.1.1.1    port 9000
description SERVER2
up time 00:06:23
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
activated
```

Related Commands

Command	Description
bmp server	Enters BMP server configuration mode to configure specific BMP servers.
neighbor bmp-activate	Activates BMP monitoring for BGP neighbors.
show ip bgp bmp	Displays information about BMP servers and neighbors.

additional-paths

To use a policy template to configure BGP to send or receive additional paths, use the **additional-paths** command in policy template configuration mode. To remove the policy from the current template, use the **no** form of this command.

additional-paths {send [receive]| receive| disable}

no additional-paths

Syntax Description

send	(Optional) Enables BGP to send additional paths.
receive	(Optional) Enables BGP to receive additional paths.
disable	(Optional) Overrides any address family configuration that enable the sending or receiving of additional paths. The disable keyword cannot be used with the send or receive keyword.

Command Default

No additional paths are sent or received using a policy template.

Command Modes

Policy template configuration (config-router-ptmp)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines

The **additional-paths** command is part of a template; the syntax differs from the global **bgp additional-paths** command. The ability to send and receive additional paths is negotiated between two BGP neighbors during session establishment.

Keep in mind that in order to advertise this path, you also need to:

- Select the path (other than best-path)
- Advertise that advertise-set (other than best-path) by using the **advertise additional-paths** command.

The **no additional-paths** command removes the policy from the current template. A peer applying this policy might still be subject to the address-family-wide **bgp additional-paths** command.

Use the **show ip bgp neighbors** command to display whether neighbors are capable of sending or receiving additional paths. Use the **show ip bgp** command with a network address to display the path selections and path IDs.

Examples

In the following example, the template is configured to allow additional path sending and receiving.

```
router bgp 45000
address-family ipv4 unicast
  bgp additional-paths send receive
  bgp additional-paths select group-best best 3
  template peer-policy rr-client-pt1
    additional-paths send receive
    advertise additional-paths best 3
  exit
address-family ipv4 unicast
  neighbor 192.168.1.1 remote-as 45000
  neighbor 192.168.1.1 inherit peer-policy rr-client-pt1
end
```

Related Commands

Command	Description
advertise additional-paths	Advertises BGP additional paths based on selection.
bgp additional-paths	Configures BGP to send or receive additional paths for all neighbors in the address family.
neighbor additional-paths	Configures the local router with the ability to send and receive additional path information for a neighbor or peer group.
neighbor inherit peer-policy	Sends a peer policy template to a neighbor so that the neighbor can inherit the configuration.
show ip bgp	Displays information about BGP networks, including path selections and path IDs.
show ip bgp neighbors	Displays information about the TCP and BGP connections of neighbors.
template peer-policy	Creates a peer policy template and enters policy template configuration mode.

address (bmp)

To configure IP address and port number to a specific BGP Monitoring Protocol (BMP) server, use the **address** command in BMP server configuration mode. To remove the IP address and the port number, use the **no** form of the command.

address *{ipv4-addr | ipv6-addr}* **port-number** *port-number*

no address *{ipv4-addr | ipv6-addr}* **port-number** *port-number*

Syntax Description

<i>ipv4-addr</i>	Configures an IPv4 address on the BMP server.
<i>ipv6-addr</i>	Configures an IPv6 address on the BMP server.
port-number <i>port-number</i>	Configures the listening port of the BMP server. The port-number of the listening BMP server ranges from 1 to 65535.

Command Default

IP address and port number is not configured for the BMP server.

Command Modes

BMP server configuration (config-router-bmpsrvr)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use the **bmp server** command to enter BMP server configuration mode and configure a specific BMP server. To configure BGP BMP neighbors to which the BMP servers establish a connection, use the **neighbor bmp-activate** command in router configuration mode. Use the **show ip bgp bmp** command to verify that IP address and port number have been configured.

Examples

The following example show how to enter BMP server configuration mode and assign IP address and port number for BMP server 1 and 2:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp server 1
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 10.1.1.1 port-number 8000
```

```

Device(config-router-bmpsrvr)# exit-bmp-server-mode
Device(config-router)# bmp server 2
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 20.1.1.1 port-number 9000
Device(config-router-bmpsrvr)# end

```

The following is sample output from the **show ip bgp bmp server** command for BMP server number 1 and 2. The “address” and the “port” field in the output display the IP address and the port number of the listening BMP servers 1 and 2:

```
Device# show ip bgp bmp server 1
```

Print detailed info for 1 server number 1.

```

bmp server 1
address: 10.1.1.1    port 8000
description SERVER1
up time 00:06:22
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
activated

```

```
Device# show ip bgp bmp server 2
```

Print detailed info for 1 server number 2.

```

bmp server 2
address: 20.1.1.1    port 9000
description SERVER2
up time 00:06:23
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
activated

```

Related Commands

Command	Description
bmp server	Enters BMP server configuration mode to configure specific BMP servers.
neighbor bmp-activate	Activates BMP monitoring for BGP neighbors.
show ip bgp bmp	Displays information about BMP servers and neighbors.

address-family ipv4 (BGP)

To enter address family or router scope address family configuration mode to configure a routing session using standard IP Version 4 (IPv4) address prefixes, use the **address-family ipv4** command in router configuration or router scope configuration mode. To exit address family configuration mode and remove the IPv4 address family configuration from the running configuration, use the **no** form of this command.

Syntax Available Under Router Configuration Mode

address-family ipv4 [**mdt** | **tunnel** | {**multicast** | **unicast**} [**vrf vrf-name**] | **vrf vrf-name**]

no address-family ipv4 [**mdt** | **tunnel** | {**multicast** | **unicast**} [**vrf vrf-name**] | **vrf vrf-name**]

Syntax Available Under Router Scope Configuration Mode

address-family ipv4 [**mdt** | **multicast** | **unicast**]

no address-family ipv4 [**mdt** | **multicast** | **unicast**]

Syntax Description

mdt	(Optional) Specifies an IPv4 multicast distribution tree (MDT) address family session.
tunnel	(Optional) Specifies an IPv4 routing session for multipoint tunneling.
multicast	(Optional) Specifies IPv4 multicast address prefixes.
unicast	(Optional) Specifies IPv4 unicast address prefixes. This is the default.
vrf vrf-name	(Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with subsequent IPv4 address family configuration mode commands.

Command Default

IPv4 address prefixes are not enabled.

Command Modes

Router configuration (config-router)

Router scope configuration (config-router-scope)

Command History

Release	Modification
12.0(5)T	This command was introduced. This command replaced the match nlri and set nlri commands.

Release	Modification
12.0(28)S	This command was modified. The tunnel keyword was added.
12.0(29)S	This command was modified. The mdt keyword was added.
12.0(30)S	This command was modified. Support for the Cisco 12000 series Internet router was added.
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	This command was modified. Support for router scope configuration mode was added. The tunnel keyword was deprecated.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Aggregation Services Routers.
12.4(20)T	This command was modified. The mdt keyword was added. The tunnel keyword was deprecated.
Cisco IOS XE Release 3.6S	This command was modified. VRF-based multicast support was added.
15.2(4)S	This command was implemented on the Cisco 7200 series router.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The **address-family ipv4** command replaces the **match nlri** and **set nlri** commands. The **address-family ipv4** command places the device in address family configuration mode (prompt: config-router-af), from which you can configure routing sessions that use standard IPv4 address prefixes. To leave address family configuration mode and return to router configuration mode, type **exit**.



Note

Routing information for address family IPv4 is advertised by default for each Border Gateway Protocol (BGP) routing session configured with the **neighbor remote-as** command unless you enter the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

The **tunnel** keyword is used to enable the tunnel subaddress family identifier (SAFI) under the IPv4 address family identifier. This SAFI is used to advertise the tunnel endpoints and the SAFI-specific attributes (which contain the tunnel type and tunnel capabilities). Redistribution of tunnel endpoints into the BGP IPv4 tunnel SAFI table occurs automatically when the tunnel address family is configured. However, peers need to be activated under the tunnel address family before the sessions can exchange tunnel information.

The **mdt** keyword is used to enable the MDT SAFI under the IPv4 address family identifier. This SAFI is used to advertise tunnel endpoints for inter-AS multicast VPN peering sessions.

If you specify the **address-family ipv4 multicast** command, you will then specify the **network** *network-number* [**mask** *network-mask*] command. The **network** command advertises (injects) the specified network number and mask into the multicast BGP database. This route must exist in the forwarding table installed by an Interior Gateway Protocol (IGP) (that is, by EIGRP, OSPF, RIP, IGRP, static, or IS-IS), but not BGP.

In Cisco IOS Release 12.2(33)SRB and later releases, the ability to use address family configuration under the router scope configuration mode was introduced. The scope hierarchy can be defined for BGP routing sessions and is required to support Multitopology Routing (MTR). To enter the router scope configuration mode, use the **scope** command, which can apply globally or for a specific VRF. When using the scope for a specific VRF, only the **unicast** keyword is available.

Examples

The following example places the device in address family configuration mode for the IPv4 address family:

```
Device(config)# router bgp 50000
Device(config-router)# address-family ipv4
Device(config-router-af)#
```

The following example places the device in address family configuration mode and specifies only multicast address prefixes for the IPv4 address family:

```
Device(config)# router bgp 50000
Device(config-router)# address-family ipv4 multicast
Device(config-router-af)#
```

The following example places the device in address family configuration mode and specifies unicast address prefixes for the IPv4 address family:

```
Device(config)# router bgp 50000
Device(config-router)# address-family ipv4 unicast
Device(config-router-af)#
```

The following example places the device in address family configuration mode and specifies **cisco** as the name of the VRF instance to associate with subsequent IPv4 address family configuration mode commands:

```
Device(config)# router bgp 50000
Device(config-router)# address-family ipv4 vrf cisco
Device(config-router-af)#
```



Note

Use this form of the command, which specifies a VRF, only to configure routing exchanges between provider edge (PE) and customer edge (CE) devices.

The following example places the device in tunnel address family configuration mode:

```
Device(config)# router bgp 100
Device(config-router)# address-family ipv4 tunnel
Device(config-router-af)#
```

The following example shows how to configure a device to support an IPv4 MDT address-family session:

```
Device(config)# router bgp 45000
Device(config-router)# address-family ipv4 mdt
Device(config-router-af)#
```


The following example shows how to configure the IPv4 address family under router scope configuration mode. In this example, the scope hierarchy is enabled globally. The device enters router scope address family configuration mode, and only multicast address prefixes for the IPv4 address family are specified:

```
Device(config)# router bgp 50000
Device(config-router)# scope global
Device(config-router-scope)# address-family ipv4 multicast
Device(config-router-scope-af)#
```

Related Commands

Command	Description
address-family ipv6	Places the device in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
address-family vpn4	Places the device in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
bgp default ipv4-unicast	Enables the IPv4 unicast address family on all neighbors.
neighbor activate	Enables the exchange of information with a BGP neighboring device.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
scope	Defines the scope for a BGP routing session and enters router scope configuration mode.

address-family l2vpn

To enter address family configuration mode to configure a routing session using Layer 2 Virtual Private Network (L2VPN) endpoint provisioning address information, use the **address-family l2vpn** command in router configuration mode. To remove the L2VPN address family configuration from the running configuration, use the **no** form of this command.

address-family l2vpn [evpn | vpls]

no address-family l2vpn [evpn | vpls]

Syntax Description

evpn	(Optional) Specifies L2VPN Ethernet Virtual Private Network (EVPN) endpoint provisioning address information.
vpls	(Optional) Specifies L2VPN Virtual Private LAN Service (VPLS) endpoint provisioning address information.

Command Default

No L2VPN endpoint provisioning support is enabled.

Command Modes

Router configuration (config-router)

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.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.
Cisco IOS XE Release 3.11S	This command was modified. The evpn keyword was added.

Usage Guidelines

The **address-family l2vpn** command places the router in address family configuration mode (prompt: config-router-af), from which you can configure routing sessions that support L2VPN endpoint provisioning.

BGP support for the L2VPN address family introduces a BGP-based autodiscovery mechanism to distribute L2VPN endpoint provisioning information. BGP uses a separate L2VPN routing information base (RIB) to store endpoint provisioning information, which is updated each time any Layer 2 (L2) virtual forwarding instance (VFI) is configured. Prefix and path information is stored in the L2VPN database, allowing BGP to make best-path decisions. When BGP distributes the endpoint provisioning information in an update message

to all its BGP neighbors, the endpoint information is used to set up a pseudowire mesh to support L2VPN-based services.

The BGP autodiscovery mechanism facilitates the setting up of L2VPN services, which are an integral part of the Cisco IOS Virtual Private LAN Service (VPLS) feature. VPLS enables flexibility in deploying services by connecting geographically dispersed sites as a large LAN over high-speed Ethernet in a robust and scalable IP MPLS network.

The multiprotocol capability for address family L2VPN EVPN is advertised when the Address Family Identifier (AFI) is enabled under the internal BGP (iBGP) and external BGP (eBGP) neighbors for both IPv4 and IPv6 neighbors.


Note

Routing information for address family IPv4 is advertised by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

Examples

In this example, two provider edge (PE) routers are configured with VPLS endpoint provisioning information that includes L2 VFI, VPN, and VPLS IDs. BGP neighbors are configured and activated under L2VPN address family to ensure that the VPLS endpoint provisioning information is saved to a separate L2VPN RIB and then distributed to other BGP peers in BGP update messages. When the endpoint information is received by the BGP peers, a pseudowire mesh is set up to support L2VPN-based services.

Examples

```
enable
configure terminal
l2 vfi customerA autodiscovery
  vpn id 100
  vpls-id 45000:100
exit
l2 vfi customerB autodiscovery
  vpn id 200
  vpls-id 45000:200
exit
router bgp 45000
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  neighbor 172.16.1.2 remote-as 45000
  neighbor 172.21.1.2 remote-as 45000
  address-family l2vpn vpls
  neighbor 172.16.1.2 activate
  neighbor 172.16.1.2 send-community extended
  neighbor 172.21.1.2 activate
  neighbor 172.21.1.2 send-community extended
end
```

Examples

```
enable
configure terminal
l2 vfi customerA autodiscovery
  vpn id 100
  vpls-id 45000:100
exit
l2 vfi customerB autodiscovery
  vpn id 200
  vpls-id 45000:200
exit
router bgp 45000
  no bgp default ipv4-unicast
```

```
bgp log-neighbor-changes
neighbor 172.16.1.1 remote-as 45000
neighbor 172.22.1.1 remote-as 45000
address-family l2vpn vpls
neighbor 172.16.1.1 activate
neighbor 172.16.1.1 send-community extended
neighbor 172.22.1.1 activate
neighbor 172.22.1.1 send-community extended
end
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a BGP neighboring router.
show ip bgp l2vpn	Displays L2VPN address family information.

address-family mvpn

To enter address family configuration mode to configure a routing session using multicast VPN (MVPN) address information, use the **address-family mvpn** command in router configuration mode. To exit address family configuration mode and remove the MVPN address family configuration from the running configuration, use the **no** form of this command.

address-family {ipv4 | ipv6} **mvpn** [**vrf** *vrf-name*]

no address-family {ipv4 | ipv6} **mvpn** [**vrf** *vrf-name*]

Syntax Description

ipv4	Specifies IPv4 MVPN address prefixes.
ipv6	Specifies IPv6 MVPN address prefixes.
vrf <i>vrf-name</i>	(Optional) Specifies the name of the VPN routing and forwarding (VRF) instance to associate with subsequent address family configuration mode commands.

Command Default

MVPN address prefixes are not configured

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

The **address-family mvpn** command places the router in address family configuration mode (prompt: config-router-af), from which you can configure routing sessions that use MVPN address information. To leave address family configuration mode and return to router configuration mode, type **exit**.

Configure **address-family ipv4 mvpn** to enable IPv4 multicast customer-route (c-route) exchange.

Configure **address-family ipv6 mvpn** to enable IPv6 multicast c-route exchange.

Examples

The following example places the device in address family configuration mode for IPv4 MVPN address prefixes:

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 mvpn
Router(config-router-af)#
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Configures a routing session using standard IPv4 address prefixes.

address-family nsap

To enter address family configuration mode to configure Connectionless Network Service (CLNS)-specific parameters for Border Gateway Protocol (BGP) routing sessions, use the **address-family nsap** command in router configuration mode. To exit address family configuration mode and remove the CLNS address family configuration from the running configuration, use the **no** form of this command.

address-family nsap [unicast]

no address-family nsap [unicast]

Syntax Description

unicast	(Optional) Specifies network service access point (NSAP) unicast address prefixes.

Command Default

NSAP prefix support is not enabled.



Note

Routing information for address family IPv4 is advertised by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **address-family nsap** command enters address family configuration mode (prompt: config-router-af)#, from which you can configure routing sessions that use standard NSAP address prefixes; you must enter NSAP address family configuration mode to configure BGP for CLNS prefixes.

To leave address family configuration mode and return to router configuration mode without removing the existing configuration, enter the **exit-address-family** command.

Examples

The following example enters NSAP address family configuration mode under BGP:

```
Router(config)# router bgp 50000
Router(config-router)# address-family nsap
Router(config-router-af)#
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
bgp default ipv4-unicast	Enables the IPv4 unicast address family on all neighbors.
neighbor activate	Enables the exchange of information with a BGP neighboring router.

address-family rtfilter unicast

To enter address family configuration mode and to enable Route Target Constrain (RTC) with a Border Gateway Protocol (BGP) peer, use the **address-family rtfilter unicast** command in router configuration mode. To remove RTC, use the **no** form of the command.

address-family rtfilter unicast

no address-family rtfilter unicast

Syntax Description This command has no arguments or keywords.

Command Default No RTC support is enabled for BGP.

Command Modes Router configuration (config-router)

Command History	Release	Modification
	15.1(1)S	This command was introduced.
	Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
	15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
	15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines Use this command when you are configuring the BGP: RT Constrained Route Distribution feature. The **address-family rtfilter unicast** command is configured on the provider edge (PE) and route reflector (RR). The command enables the PE to send RTC Network Layer Reachability Information (NLRI) to an RR. As soon as you configure a peer as a RR client, the default filter and default route are sent out also.

Examples In the following example, the local PE is configured to send RTC NLRI to the neighboring RR at 10.2.2.2:

```
router bgp 65000
 address-family rtfilter unicast
 neighbor 10.2.2.2 activate
 neighbor 10.0.0.2 send-community extended
 exit-address-family
```

In the following example, the local PE is configured with the RTC default filter, which indicates that the PE wants all of the VPN routes (regardless of the RT values):

```
router bgp 65000
 address-family rtfilter unicast
 neighbor 10.2.2.2 activate
```

```
neighbor 10.0.0.2 send-community extended
neighbor 10.2.2.2 default-originate
exit-address-family
```

In the following example, the RR is configured with the RTC default filter, which indicates that the RR is requesting the PE to advertise all of its routes to the RR:

```
router bgp 65000
 address-family rtfilter unicast
 neighbor 10.1.1.1 activate
 neighbor 10.1.1.1 route-reflector-client
 neighbor 10.1.1.1 default-originate
 exit-address-family
```

Related Commands

Command	Description
neighbor default-originate	Allows a BGP speaker (the local router) to send the default route 0:0:0:0 to a neighbor for use as a default route.
router bgp	Configures the BGP routing process.
show ip bgp rtfilter	Displays information about BGP RT filtering.

address-family vpnv4

To enter address family configuration mode to configure a routing session using Virtual Private Network (VPN) Version 4 address prefixes, use the **address-family vpnv4** command in router configuration mode. To exit address family configuration mode and remove the VPNv4 address family configuration from the running configuration, use the **no** form of this command.

address-family vpnv4 [**multicast** | **unicast**]

no address-family vpnv4 [**multicast** | **unicast**]

Syntax Description

multicast	(Optional) Specifies VPN Version 4 multicast address prefixes.
unicast	(Optional) Specifies VPN Version 4 unicast address prefixes.

Command Default

Unicast prefix support is enabled by default when this command is entered without any optional keywords.



Note

Routing information for address family IPv4 is advertised by default for each Border Gateway Protocol (BGP) routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

Command Modes

Router configuration (config-router)

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.
Cisco IOS XE Release 3.6S	This command was modified. Support for multicast VPN Version 4 was added.
15.2(4)S	This command was implemented on the Cisco 7200 series router.

Usage Guidelines

The **address-family vpnv4** command replaces the **match nlri** and **set nlri** commands.

The **address-family vpnv4** command places the router in address family configuration mode (prompt: config-router-af), from which you can configure routing sessions that use VPN Version 4 address prefixes.

To leave address family configuration mode and return to router configuration mode without removing the existing configuration, enter the **exit-address-family** command.

Examples

The following example places the router in address family configuration mode for the VPN Version 4 address family:

```
Router(config)# router bgp 50000
Router(config-router)# address-family vpnv4
Router(config-router-af)#
```

The following example places the router in address family configuration mode for the unicast VPN Version 4 address family:

```
Router(config)# router bgp 50000
Router(config-router)# address-family vpnv4 unicast
Router(config-router-af)#
```

The following example places the router in address family configuration mode for the multicast VPN Version 4 address family:

```
Router(config)# router bgp 50000
Router(config-router)# address-family vpnv4 multicast
Router(config-router-af)#
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
address-family nsap	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use CLNS prefixes.
exit-address-family	Exits the address family configuration mode and returns to router configuration mode without removing the existing configuration
neighbor activate	Enables the exchange of information with a BGP neighboring router.

advertise additional-paths

To advertise additional paths for a BGP peer policy template based on selection, use the **advertise additional-paths** command in peer policy template configuration mode. To prevent the advertisement of additional paths for a peer policy template, use the **no** form of the command.

advertise additional-paths [*best number*] [*group-best*] [*all*]

no advertise additional-paths [*best number*] [*group-best*] [*all*]

Syntax Description

best number	(Optional) Advertises the paths tagged with the best 2 or best 3 tag.
group-best	(Optional) Advertises the set of paths tagged with the group-best tag.
all	(Optional) Advertises paths tagged with the all tag.

Command Default

This command has no default behavior.

Command Modes

Peer policy template (config-router-ptmp)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines

Use this command to specify for the peer policy template which additional paths are advertised. You can advertise additional paths based on any combination of the selection methods, but you must choose at least one selection method if you use this command.

Keep in mind that in order to advertise additional-paths, you also need to:

- Configure the additional-path send capability, and that send capability must be negotiated (other than best-path).
- Select paths (other than best-path) with the **bgp additional-paths select** command, which sets the tags.

Examples

In the following example, a peer policy template named rr-client-pt1 is configured with the additional path sending and receiving capability. The group-best and best 3 selection policies are configured, and paths tagged with the best 3 tag are advertised.

```
router bgp 45000
address-family ipv4 unicast
  bgp additional-paths send receive
  bgp additional-paths select group-best best 3
template peer-policy rr-client-pt1
  additional-paths send receive
  advertise additional-paths best 3
exit
address-family ipv4 unicast
neighbor 192.168.1.1 remote-as 45000
neighbor 192.168.1.1 inherit peer-policy rr-client-pt1
end
```

Related Commands

Command	Description
additional-paths	Configures the send and receive capabilities of additional path information for a peer template.
bgp additional-paths select	Causes the system to calculate BGP additional paths that can be candidates for advertisement in addition to a bestpath.
neighbor advertise additional-paths	Advertises additional paths for a neighbor based on selection.
neighbor inherit peer-policy	Sends a peer policy template to a neighbor so that the neighbor can inherit the configuration.
show ip bgp	Displays information about BGP neighbors, including path selections and path IDs.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.
template peer-policy	Creates a peer policy template.

aggregate-address

To create an aggregate entry in a Border Gateway Protocol (BGP) database, use the **aggregate-address** command in address family or router configuration mode. To disable this function, use the **no** form of this command.

aggregate-address *address mask* [**as-set**] [**as-confed-set**] [**summary-only**] [**suppress-map** *map-name*] [**advertise-map** *map-name*] [**attribute-map** *map-name*]

no aggregate-address *address mask* [**as-set**] [**as-confed-set**] [**summary-only**] [**suppress-map** *map-name*] [**advertise-map** *map-name*] [**attribute-map** *map-name*]

Syntax Description

<i>address</i>	Aggregate address.
<i>mask</i>	Aggregate mask.
as-set	(Optional) Generates autonomous system set path information.
as-confed-set	(Optional) Generates autonomous confederation set path information.
summary-only	(Optional) Filters all more-specific routes from updates.
suppress-map <i>map-name</i>	(Optional) Specifies the name of the route map used to select the routes to be suppressed.
advertise-map <i>map-name</i>	(Optional) Specifies the name of the route map used to select the routes to create AS_SET origin communities.
attribute-map <i>map-name</i>	(Optional) Specifies the name of the route map used to set the attribute of the aggregate route.

Command Default

The atomic aggregate attribute is set automatically when an aggregate route is created with this command unless the **as-set** keyword is specified.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
11.1(20)CC	The nlri unicast , nlri multicast , and nlri unicast multicast keywords were added.
12.0(2)S	The nlri unicast , nlri multicast , and nlri unicast multicast keywords were added.
12.0(7)T	The nlri unicast , nlri multicast , and nlri unicast multicast keywords were removed. Address family configuration mode support was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(33)SRE	The as-confed-set keyword was added.
Cisco IOS XE Release 3.1S	This command was introduced on Cisco ASR 1000 series routers.

Usage Guidelines

You can implement aggregate routing in BGP and Multiprotocol BGP (mBGP) either by redistributing an aggregate route into BGP or mBGP, or by using the conditional aggregate routing feature.

Using the **aggregate-address** command with no keywords will create an aggregate entry in the BGP or mBGP routing table if any more-specific BGP or mBGP routes are available that fall within the specified range. (A longer prefix that matches the aggregate must exist in the Routing Information Base (RIB).) The aggregate route will be advertised as coming from your autonomous system and will have the atomic aggregate attribute set to show that information might be missing. (By default, the atomic aggregate attribute is set unless you specify the **as-set** keyword.)

Using the **as-set** keyword creates an aggregate entry using the same rules that the command follows without this keyword, but the path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized. Do not use this form of the **aggregate-address** command when aggregating many paths, because this route must be continually withdrawn and updated as autonomous system path reachability information for the summarized routes changes.

Using the **as-confed-set** keyword creates an aggregate entry using the same rules that the command follows without this keyword. This keyword performs the same function as the **as-set** keyword, except that it generates autonomous confed set path information.

Using the **summary-only** keyword not only creates the aggregate route (for example, 192.*.*) but also suppresses advertisements of more-specific routes to all neighbors. If you want to suppress only advertisements to certain neighbors, you may use the **neighbor distribute-list** command, with caution. If a more-specific

route leaks out, all BGP or mBGP routers will prefer that route over the less-specific aggregate you are generating (using longest-match routing).

Using the **suppress-map** keyword creates the aggregate route but suppresses advertisement of specified routes. You can use the **match** clauses of route maps to selectively suppress some more-specific routes of the aggregate and leave others unsuppressed. IP access lists and autonomous system path access lists match clauses are supported.

Using the **advertise-map** keyword selects specific routes that will be used to build different components of the aggregate route, such as AS_SET or community. This form of the **aggregate-address** command is useful when the components of an aggregate are in separate autonomous systems and you want to create an aggregate with AS_SET, and advertise it back to some of the same autonomous systems. You must remember to omit the specific autonomous system numbers from the AS_SET to prevent the aggregate from being dropped by the BGP loop detection mechanism at the receiving router. IP access lists and autonomous system path access lists **match** clauses are supported.

Using the **attribute-map** keyword allows attributes of the aggregate route to be changed. This form of the **aggregate-address** command is useful when one of the routes forming the AS_SET is configured with an attribute such as the community no-export attribute, which would prevent the aggregate route from being exported. An attribute map route map can be created to change the aggregate attributes.

Examples

Examples

In the following example, an aggregate BGP address is created in router configuration mode. The path advertised for this route will be an AS_SET consisting of all elements contained in all paths that are being summarized.

```
Router(config)# router bgp 50000
Router(config-router)# aggregate-address 10.0.0.0 255.0.0.0 as-set
```

Examples

In the following example, an aggregate BGP address is created in address family configuration mode and applied to the multicast database under the IP Version 4 address family. Because the **summary-only** keyword is configured, more-specific routes are filtered from updates.

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 multicast
Router(config-router-af)# aggregate-address 10.0.0.0 255.0.0.0 summary-only
```

Examples

In the following example, a route map called MAP-ONE is created to match on an AS-path access list. The path advertised for this route will be an AS_SET consisting of elements contained in paths that are matched in the route map.

```
Router(config)# ip as-path access-list 1 deny ^1234_
Router(config)# ip as-path access-list 1 permit .*
Router(config)# !
Router(config)# route-map MAP-ONE
Router(config-route-map)# match ip as-path 1
Router(config-route-map)# exit
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4
Router(config-router-af)# aggregate-address 10.0.0.0 255.0.0.0 as-set advertise-map
MAP-ONE
Router(config-router-af)# end
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
ip as-path access-list	Defines a BGP autonomous system path access list.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
neighbor distribute-list	Distributes BGP neighbor information in an access list.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

autodiscovery (MPLS)

To designate a Layer 2 virtual forwarding interface (VFI) as having Border Gateway Protocol (BGP) or Label Distribution Protocol (LDP) autodiscovered pseudowire members, use the **autodiscovery** command in L2 VFI configuration mode. To disable autodiscovery, use the **no** form of this command.

autodiscovery bgp signaling {**bgp** | **ldp**}[**template** *template-name*]

no autodiscovery bgp signaling {**bgp** | **ldp**}[**template** *template-name*]

Syntax Description

bgp	Specifies that BGP should be used for signaling and autodiscovery.
ldp	Specifies that LDP should be used for signaling.
template <i>template-name</i>	Specifies the template to be used for autodiscovered pseudowires.

Command Default

Layer 2 VFI autodiscovery is disabled.

Command Modes

L2 VFI configuration (config-vfi)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support.. This command will replace the l2 vfi autodiscovery command in future releases.
Cisco IOS XE Release 3.8S	This command was modified. The bgp keyword was added.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

This command was introduced as part of the Multiprotocol Label Switching (MPLS)-based L2VPN command modifications for cross-OS support. This command will replace the **l2 vfi autodiscovery** command in future releases.

Layer 2 VFI autodiscovery enables each VPLS PE router to discover other PE routers that are part of the same VPLS domain. VPLS autodiscovery also automatically detects when PE routers are added to or removed from the VPLS domain

The **bgp** keyword specifies that BGP should be used for signaling and autodiscovery, accordance with RFC 4761.

The **ldp** keyword specifies that LDP should be used for signaling. BGP will be used for autodiscovery.

Use of the **autodiscovery** command places the device into L2VPN VFI autodiscovery configuration mode (config-vfi-autodiscovery).

Examples

The following example shows how to enable Layer 2 VFI as having BGP autodiscovered pseudowire members and specify that LDP signaling should be used for autodiscovery:

```
Device(config)# l2vpn vfi context vfi1
Device(config-vfi)# vpn id 100
Device(config-vfi)# autodiscovery bgp signaling ldp
Device(config-vfi-autodiscovery)#
```

Related Commands

Command	Description
l2 vfi autodiscovery	Enables the VPLS PE router to automatically discover other PE routers that are part of the same VPLS domain.
vpn id	Sets or updates a VPN ID on a VPLS instance.

auto-summary (BGP)

To configure automatic summarization of subnet routes into network-level routes, use the **auto-summary** command in address family or router configuration mode. To disable automatic summarization and send subprefix routing information across classful network boundaries, use the **no** form of this command.

auto-summary

no auto-summary

Syntax Description This command has no arguments or keywords.

Command Default Automatic summarization is disabled by default (the software sends subprefix routing information across classful network boundaries).

Command Modes Address family configuration (config-router-af)
Router configuration (config-router)

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(7)T	Address family configuration mode support was added.
	12.2(8)T	The command default behavior was changed to disabled.
	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.
	15.0M, 12.2SRE	This command was modified. When an interface addressed with an address falling within the summarized range is shut down, that route no longer appears in the BGP routing table.

Usage Guidelines BGP automatically summarizes routes to classful network boundaries when this command is enabled. Route summarization is used to reduce the amount of routing information in routing tables. Automatic summarization applies to connected, static, and redistributed routes.



Note

The MPLS VPN Per VRF Label feature does not support auto-summary.

By default, automatic summarization is disabled and BGP accepts subnets redistributed from an Interior Gateway Protocol (IGP). To block subnets and create summary subprefixes to the classful network boundary when crossing classful network boundaries, use the **auto-summary** command.

To advertise and carry subnet routes in BGP when automatic summarization is enabled, use an explicit **network** command to advertise the subnet. The **auto-summary** command does not apply to routes injected into BGP via the **network** command or through iBGP or eBGP.

Why auto-summary for BGP Is Disabled By Default

When **auto-summary** is enabled, routes injected into BGP via redistribution are summarized on a classful boundary. Remember that a 32-bit IP address consists of a network address and a host address. The subnet mask determines the number of bits used for the network address and the number of bits used for the host address. The IP address classes have a natural or standard subnet mask, as shown in the table below.

Table 1: IP Address Classes

Class	Address Range	Standard Mask
A	1.0.0.0 to 126.0.0.0	255.0.0.0 or /8
B	128.1.0.0 to 191.254.0.0	255.255.0.0 or /16
C	192.0.1.0 to 223.255.254.0	255.255.255.0 or /24

Reserved addresses include 128.0.0.0, 191.255.0.0, 192.0.0.0, and 223.255.255.0.

When using the standard subnet mask, Class A addresses have one octet for the network, Class B addresses have two octets for the network, and Class C addresses have three octets for the network.

Consider the Class B address 156.26.32.1 with a 24-bit subnet mask, for example. The 24-bit subnet mask selects three octets, 156.26.32, for the network. The last octet is the host address. If the network 156.26.32.1/24 is learned via an IGP and is then redistributed into BGP, if **auto-summary** were enabled, the network would be automatically summarized to the natural mask for a Class B network. The network that BGP would advertise is 156.26.0.0/16. BGP would be advertising that it can reach the entire Class B address space from 156.26.0.0 to 156.26.255.255. If the only network that can be reached via the BGP router is 156.26.32.0/24, BGP would be advertising 254 networks that cannot be reached via this router. This is why the **auto-summary** (BGP) command is disabled by default.

Examples

In the following example, automatic summarization is enabled for IPv4 address family prefixes:

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 unicast
Router(config-router-af)# auto-summary
```

```
Router(config-router-af)# network 7.7.7.7 255.255.255.255
```

In the example, there are different subnets, such as 7.7.7.6 and 7.7.7.7 on Loopback interface 6 and Loopback interface 7, respectively. Both **auto-summary** and a **network** command are configured.

```
Router# show ip interface brief
Interface      IP-Address      OK? Method Status      Protocol
Ethernet0/0    100.0.1.7       YES NVRAM   up          up
Ethernet0/1    unassigned      YES NVRAM   administratively down down
```

```

Ethernet0/2      unassigned      YES NVRAM      administratively down down
Ethernet0/3      unassigned      YES NVRAM      administratively down down
Ethernet1/0      108.7.9.7       YES NVRAM      up              up
Ethernet1/1      unassigned      YES NVRAM      administratively down down
Ethernet1/2      unassigned      YES NVRAM      administratively down down
Ethernet1/3      unassigned      YES NVRAM      administratively down down
Loopback6       7.7.7.6         YES NVRAM      up              up
Loopback7       7.7.7.7         YES NVRAM      up              up

```

Note that in the output below, because of the **auto-summary** command, the BGP routing table displays the summarized route 7.0.0.0 instead of 7.7.7.6. The 7.7.7.7/32 network is displayed because it was configured with the **network** command, which is not affected by the **auto-summary** command.

```

Router# show ip bgp
BGP table version is 10, local router ID is 7.7.7.7
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
*> 6.6.6.6/32     100.0.1.6        0           0 6 i
*> 7.0.0.0        0.0.0.0          0          32768 ?   <-- summarization
*> 7.7.7.7/32     0.0.0.0          0          32768 i   <-- network command
r>i9.9.9.9/32     108.7.9.9        0         100      0 i
*> 100.0.0.0      0.0.0.0          0          32768 ?
r> 100.0.1.0/24   100.0.1.6        0           0 6 ?
*> 108.0.0.0      0.0.0.0          0          32768 ?
r>i108.7.9.0/24   108.7.9.9        0         100      0 ?
*>i200.0.1.0     108.7.9.9

```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
network (BGP and multiprotocol BGP)	Specifies the networks to be advertised by BGP and multiprotocol BGP.

bgp additional-paths

To configure BGP to send or receive additional paths (for all neighbors in the address family), use the **bgp additional-paths** command in address family configuration mode. To disable the sending or receiving of additional-path capability for the address family, use the **no** form of this command.

bgp additional-paths {send [receive]| receive| disable}

no bgp additional-paths {send [receive]| receive}

Syntax Description

send	(Optional) Enables BGP to send additional paths to all neighbors in the address family.
receive	(Optional) Enables BGP to receive additional paths from all neighbors in the address family.
disable	(Optional) Overrides and disables the address family-wide command for the current template. Note that the disable keyword is mutually exclusive with the send and receive keywords.

Command Default

No additional paths are sent or received per address family.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines

Using this command will enable the sending and receiving of additional path capability for an address family, after successful negotiation with a neighbor. The ability to send and receive additional paths is negotiated between two BGP neighbors during session establishment. The following address families are supported: IPv4 unicast, IPv4 multicast, IPv4 unicast + label, IPv6 unicast, IPv6 multicast, and IPv6 multicast + label.

The **bgp additional-paths** command controls whether the local device can send or receive additional paths to and from all neighbors within an address family. If the **neighbor additional-paths** command is configured, its send and receive configurations for that neighbor or peer group override the configuration for the address family.

When the additional paths feature is used with IPv4+label or IPv6+label, only one label is allocated.

Use the **show ip bgp neighbors** command to display whether neighbors are capable of sending or receiving additional paths. Use the **show ip bgp** command with a network address to display the path selections, path IDs, and the capabilities for advertising and receiving additional paths.

When **bgp additional-paths** is configured, that configuration is applied to all neighbors in that address family.

- If you want to disable additional paths for the address family, use the **no bgp additional-paths {send [receive] | receive}** command.
- If you want to disable additional paths for one of the neighbors, use the **neighbor additional-paths disable** command.

Examples

In the following example, BGP negotiates with each neighbor in the IPv6 multicast address family that it can send and receive additional paths:

```
router bgp 65000
 address-family ipv6 multicast
  bgp additional-paths send receive
```

In the following example, BGP negotiates with each neighbor in the IPv4 unicast address family that it can send additional paths:

```
router bgp 65000
 address-family ipv4 unicast
  bgp additional-paths send
```

In the following example, BGP negotiates with all neighbors in the IPv6 multicast address family that it can receive additional paths:

```
router bgp 65000
 address-family ipv6 multicast
  bgp additional-paths receive
```

In the following example, the send and receive capability of the neighbor overrides the receive-only capability of the address family:

```
router bgp 65000
 address-family ipv6 multicast
  bgp additional-paths receive
  bgp additional-paths select group-best
  neighbor 2001:DB8::1037 activate
  neighbor 2001:DB8::1037 additional-paths send receive
  neighbor 2001:DB8::1037 advertise additional-paths group-best
  neighbor 2001:DB8::1037 route-map add_path4 out
!
route-map add_path4 permit 10
 match additional-paths advertise-set group-best
 set metric 565
!
```

In the following example, BGP is prevented from sending additional paths to or receiving additional paths from all neighbors in the IPv6 unicast address family. Note that the **no bgp additional-paths send receive** command will not actually appear in the configuration file; this example shows the CLI commands entered by the user.

```
Device(config)# router bgp 65000
Device(config-router)# address-family ipv6 unicast
Device(config-router-af)# no bgp additional-paths send receive
```

Related Commands

Command	Description
additional-paths	Uses a policy template to configure BGP to send or receive additional paths.

Command	Description
advertise additional-paths	Advertise additional paths for a BGP peer policy template based on selection.
bgp additional-paths select	Causes the system to calculate BGP additional paths that can be candidates for advertisement in addition to a bestpath.
neighbor additional-paths	Configures the local device with the ability to send and receive additional path information to and from a neighbor or peer group.
neighbor advertise additional-paths	Advertises additional paths for a neighbor based on selection.
show ip bgp	Displays information about BGP networks, including path selections and path IDs.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

bgp additional-paths install

To enable Border Gateway Protocol (BGP) to calculate a backup path for a given address family and to install it into the Routing Information Base (RIB) and Cisco Express Forwarding, use the **bgp additional-paths install** command in address family configuration or router configuration mode. To remove the backup paths, use the **no** form of this command.

bgp additional-paths install

no bgp additional-paths install

Syntax Description This command has no arguments or keywords.

Command Default A backup path is not created.

Command Modes Address family configuration (config-router-af)
Router configuration (config-router)

Command History	Release	Modification
	12.2(33)SRE	This command was introduced.
	12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
	Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
	15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
	Cisco IOS XE Release 3.3S	Support for IPv6 address family configuration mode was added.
	15.1(2)S	Support for IPv6 address family configuration mode was added.
	15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
	15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines You can issue the **bgp additional-paths install** command in different modes, each of which protects VRFs in its own way:

- VPNv4 address family configuration mode protects all VRFs.
- IPv4 address family configuration mode protects only IPv4 VRFs.

- IPv6 address family configuration mode protects only IPv6 VRFs.
- Router configuration mode protects VRFs in the global routing table.

Examples

The following example shows how to calculate a backup path and install it into the RIB and Cisco Express Forwarding:

```
Router(config-router-af) # bgp additional-paths install
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
bgp advertise-best-external	Enables BGP to use an external route as the backup path after a link or node failure.

bgp additional-paths select (additional paths)

To have the system calculate BGP additional paths that can be candidates for advertisement in addition to a bestpath, use the **bgp additional-paths select** command in address family configuration mode. To remove this mechanism for calculating additional paths and diverse path, use the **no** form of the command.

bgp additional-paths select [*best number*] [*group-best*] [*all*]

no bgp additional-paths select [*best number*] [*group-best*] [*all*]

Syntax Description

best number	(Optional) Calculates 2 or 3 bestpaths. • The value of <i>number</i> can be 2 or 3. • The bestpath is included as one of the 2 or 3 additional paths. • Paths with a unique next hop are selected; paths with a duplicate next hop are not considered.
group-best	(Optional) Selects the set of paths that are the best paths from the paths of the same AS. • For example, suppose there are three autonomous systems: AS 100, 200, and 300. Paths p101, p102, and p103 are from AS 100; p201, p202, and p203 are from AS200; and p301, p302, and p303 are from AS300. If the BGP bestpath algorithm is run on the paths from each AS, the algorithm will select one bestpath from each set of paths from that AS. Assume p101 is the best from AS100, p201 is the best from AS200, and p301 is the best from AS300; then the group-best is the set of p101, p201, and p301. • Paths with a unique next hop are selected; paths with a duplicate next hop are not considered.
all	(Optional) Selects all paths. • Paths with a unique next hop are selected; paths with a duplicate next hop are not considered.

Command Default

No additional paths are selected to be advertised.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines

This command configures part of the BGP Additional Paths feature. This feature allows you to calculate multiple paths for the same prefix without the new paths implicitly replacing any previous paths. Use this command to select which paths are candidates as additional paths to be advertised to BGP peers.

You can specify any combination of the keywords in the same instance of the **bgp additional-paths select** command; you must specify at least one keyword.

In order to enable the BGP Additional Paths feature and have a reason for selecting which paths will be advertised, you must have the additional path Send capability specified and it must be negotiated (other than best-path).

After you have selected which additional paths are candidates for advertisement, you typically use the **neighbor advertise additional-paths** command to advertise the additional paths to a specific neighbor. Alternatively, you could use the **advertise additional-paths** command under the **template peer-policy** command to advertise the additional paths to BGP peers in the peer policy template.

**Note**

The **bgp additional-paths select backup** and **bgp additional-paths select best-external** commands are for the diverse path feature, not the Additional Paths feature. If the diverse path feature is also configured, it will apply only to neighbors where additional path capability is not negotiated.

You can remove every selection option configured by issuing the **no bgp additional-paths select** command.

**Note**

The **no bgp additional-paths select** command will remove anything configured after the **select** keyword, which means that it will remove diverse path configurations: **bgp additional-paths select backup** and **bgp additional-paths select best-external**, and additional path configurations: **bgp additional-paths select best number**, **bgp additional-paths select group-best**, and **bgp additional-paths select all**.

Examples

In the following example, there are one or more eBGP neighbors not shown in the configuration. The eBGP routes learned from these neighbors are advertised for the neighbors shown in the configuration, and their attributes are changed. The route map called `add_path3` specifies that any path that is tagged with the **group-best** tag will have its metric set to 825 and will be advertised toward neighbor 2001:DB8::1045.

```
router bgp 1
 neighbor 2001:DB8::1045 remote-as 1
```

```

neighbor 2001:DB8::1037 remote-as 1
!
address-family ipv6 unicast
  bgp additional-paths send receive
  bgp additional-paths select group-best
  neighbor 2001:DB8::1045 activate
  neighbor 2001:DB8::1045 route-map add_path3 out
  neighbor 2001:DB8::1045 advertise additional-paths group-best
exit-address-family
!
route-map add_path3 permit 10
match additional-paths advertise-set group-best
set metric 825

```

Related Commands

Command	Description
additional-paths	Uses a policy template to configure BGP to send or receive additional paths.
advertise additional-paths	Advertises additional paths for a BGP peer policy template based on selection.
bgp additional-paths	Configures BGP to send or receive additional paths per address family.
bgp additional-paths select (diverse path)	Calculates a second BGP bestpath.
neighbor additional-paths	Configures BGP to send or receive additional paths per neighbor.
neighbor advertise additional-paths	Configures BGP to advertise additional paths to the neighbor.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.

bgp additional-paths select (diverse path)

To have the system calculate a second Border Gateway Protocol (BGP) best path, use the **bgp additional-paths select** command in address family configuration mode. To remove this mechanism for calculating a second best path, use the **no** form of this command.

bgp additional-paths select {**best-external**[**backup**]| **backup**}

no bgp additional-paths select

Syntax Description

best-external	(Optional) Calculates a second best path from among those received from external neighbors. Configure this keyword on a provider edge (PE) or route reflector. This keyword enables the BGP Best External feature on a route reflector.
backup	(Optional) Calculates a second best path as a backup path.

Command Default

A second BGP best path is not calculated.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

The BGP Diverse Path feature can be enabled on a route reflector to calculate a best path and an additional path per address family.

Computation of a diverse path per address family is triggered by any of the following commands:

- **bgp additional-paths install**
- **bgp additional-paths select**
- **maximum-paths ebgp**
- **maximum-paths ibgp**

The **bgp additional-paths install** command will install the type of path that is specified in the **bgp additional-paths select** command. Either the **best-external** keyword or the **backup** keyword is required;

both keywords can be specified. If both keywords (**best-external** and **backup**) are specified, the system will install a backup path.

**Note**

The **bgp additional-paths select backup** and **bgp additional-paths select best-external** commands are for the Diverse Path feature, not the BGP Additional Paths feature. If the Diverse Path feature and the Additional Paths feature are configured, the Diverse Path feature will apply only to neighbors where additional path capability is not negotiated.

You can remove every selection option configured by issuing the **no bgp additional-paths select** command.

**Note**

The **no bgp additional-paths select** command will remove anything configured after the **select** keyword, which means that it will remove diverse path configurations: **bgp additional-paths select backup** and **bgp additional-paths select best-external**, and additional path configurations: **bgp additional-paths select best number**, **bgp additional-paths select group-best**, and **bgp additional-paths select all**.

Examples

In the following example, the system computes a second best path from among those received from external neighbors:

```
router bgp 1
 neighbor 10.1.1.1 remote-as 1
 address-family ipv4 unicast
 neighbor 10.1.1.1 activate
 maximum-paths ibgp 4
 bgp bestpath igp-metric ignore
 bgp additional-paths select best-external
 bgp additional-paths install
 neighbor 10.1.1.1 advertise diverse-path backup
```

Related Commands

Command	Description
bgp additional-paths install	Enables BGP to calculate a backup path for a given address and to install it into the RIB and CEF.
bgp bestpath igp-metric ignore	Specifies that the system ignore the IGP metric during best path selection.
maximum-paths ebgp	Configures multipath load sharing for EBGp and IBGP routes.
maximum-paths ibgp	Controls the maximum number of parallel IBGP routes that can be installed in a routing table.

bgp advertise-best-external

To enable Border Gateway Protocol (BGP) to calculate an external route as the best backup path for a given address family and to install it into the Routing Information base (RIB) and Cisco Express Forwarding, and to advertise the best external path to its neighbors, use the **bgp advertise-best-external** command in address family or router configuration mode. To remove the external backup path, use the **no** form of this command.

bgp advertise-best-external

no bgp advertise-best-external

Syntax Description This command has no arguments or keywords.

Command Default An external backup path is not created.

Command Modes Router configuration (config-router)
Address family configuration (config-router-af)

Command History	Release	Modification
	12.2(33)SRE	This command was introduced.
	12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
	Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
	Cisco IOS XE Release 3.3S	Support for IPv6 address family configuration mode was added.
	15.1(2)S	Support for IPv6 address family configuration mode was added.
	15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
	15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines When you configure the Best External feature with the **bgp advertise-best-external** command, you need not enable the Prefix Independent Convergence (PIC) feature with the **bgp additional-paths install** command. The Best External feature automatically installs a backup path. If you try to configure the PIC feature after configuring the Best External feature, you receive an error. This behavior applies to both BGP and MPLS.

When you configure the MPLS VPN: Best External feature with the **bgp advertise-best-external** command, it will override the functionality of the MPLS VPN--BGP Local Convergence feature. You need not remove the **protection local-prefixes** command from the configuration.

You can issue the **bgp advertise-best-external** command in different modes, each of which protects VRFs in its own way:

- VPNv4 address-family configuration mode protects all VRFs.
- IPv4 address-family configuration mode protects only IPv4 VRFs.
- IPv6 address family configuration mode protects only IPv6 VRFs.
- Router configuration mode protects VRFs in the global routing table.

Examples

The following example calculates an external backup path and installs it into the RIB and Cisco Express Forwarding:

```
Router(config-router-af)# bgp advertise-best-external
```

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
bgp additional-paths install	Enables BGP to use an additional path as the backup path.
protection local-prefixes	Enables PE-CE link protection by preserving the local label.

bgp aggregate-timer

To set the interval at which BGP routes will be aggregated or to disable timer-based route aggregation, use the **bgp aggregate-timer** command in address-family or router configuration mode. To restore the default value, use the **no** form of this command.

bgp aggregate-timer *seconds*

no bgp aggregate-timer

Syntax Description

<i>seconds</i>	Interval (in seconds) at which the system will aggregate BGP routes. • The range is from 6 to 60 or else 0 (zero). The default is 30. • A value of 0 (zero) disables timer-based aggregation and starts aggregation immediately.

Command Default

30 seconds

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.2SX	This command was introduced.
12.2M	This command was integrated into Cisco IOS Release 12.2 Mainline.
12.2SR	This command was integrated into Cisco IOS Release 12.2 SR.
XE 2.0	This command was integrated into Cisco IOS XE Release 2.0.
12.2(33)SRD4	The zero (0) timer was added.

Usage Guidelines

Use this command to change the default interval at which BGP routes are aggregated.

In very large configurations, even if the **aggregate-address summary-only** command is configured, more specific routes are advertised and later withdrawn. To avoid this behavior, configure the **bgp aggregate-timer** to 0 (zero), and the system will immediately check for aggregate routes and suppress specific routes.

Examples

The following example configures BGP route aggregation at 20-second intervals:

```
Router(config)# router bgp 50  
Router(config-router)# bgp aggregate-timer 20
```

The following example starts BGP route aggregation immediately:

```
Router(config)# router bgp 50  
Router(config-router)# aggregate-address 10.0.0.0 255.0.0.0 summary-only  
Router(config-router)# bgp aggregate-timer 0
```

Related Commands

Command	Description
aggregate-address	Creates an aggregate entry in a BGP database.

bgp always-compare-med

To enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems, use the **bgp always-compare-med** command in router configuration mode. To disallow the comparison, use the **no** form of this command.

bgp always-compare-med

no bgp always-compare-med

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco IOS software does not compare the MED for paths from neighbors in different autonomous systems if this command is not enabled or if the **no** form of this command is entered. The MED is compared only if the autonomous system path for the compared routes is identical.

Command Modes

Router configuration (config-router)

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 MED, as stated in RFC 1771, is an optional nontransitive attribute that is a four octet non-negative integer. The value of this attribute may be used by the BGP best path selection process to discriminate among multiple exit points to a neighboring autonomous system.

The MED is one of the parameters that is considered when selecting the best path among many alternative paths. The path with a lower MED is preferred over a path with a higher MED. During the best-path selection process, MED comparison is done only among paths from the same autonomous system. The **bgp always-compare-med** command is used to change this behavior by enforcing MED comparison between all paths, regardless of the autonomous system from which the paths are received.

The **bgp deterministic-med** command can be configured to enforce deterministic comparison of the MED value between all paths received from within the same autonomous system.

Examples

In the following example, the local BGP routing process is configured to compare the MED from alternative paths, regardless of the autonomous system from which the paths are received:

```
Router(config)# router bgp 500000  
Router(config-router)# bgp always-compare-med
```

Related Commands

Command	Description
bgp deterministic-med	Enforces deterministic comparison of the MED value between all paths received from within the same autonomous system

bgp asnotation dot

To change the default display and regular expression match format of Border Gateway Protocol (BGP) 4-byte autonomous system numbers from asplain (decimal values) to dot notation, use the **bgp asnotation dot** command in router configuration mode. To reset the default 4-byte autonomous system number display and regular expression match format to asplain, use the **no** form of this command.

bgp asnotation dot

no bgp asnotation dot

Syntax Description

This command has no arguments or keywords.

Command Default

BGP autonomous system numbers are displayed using asplain (decimal value) format in screen output, and the default format for matching 4-byte autonomous system numbers in regular expressions is asplain.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0(32)SY8	This command was introduced.
12.2(33)SX11	This command was integrated into Cisco IOS Release 12.2(33)SX11.
12.0(33)S3	This command was integrated into Cisco IOS Release 12.0(33)S3.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

Prior to January 2009, BGP autonomous system numbers that were allocated to companies were 2-octet numbers in the range from 1 to 65535 as described in RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*. Due to increased demand for autonomous system numbers, the Internet Assigned Number Authority (IANA) will start in January 2009 to allocate four-octet autonomous system numbers in the range from 65536 to 4294967295. RFC 5396, *Textual Representation of Autonomous System (AS) Numbers*, documents three methods of representing autonomous system numbers. Cisco has implemented the following two methods:

- Asplain--Decimal value notation where both 2-byte and 4-byte autonomous system numbers are represented by their decimal value. For example, 65526 is a 2-byte autonomous system number and 234567 is a 4-byte autonomous system number.
- Asdot--Autonomous system dot notation where 2-byte autonomous system numbers are represented by their decimal value and 4-byte autonomous system numbers are represented by a dot notation. For example, 65526 is a 2-byte autonomous system number and 1.169031 is a 4-byte autonomous system number (this is dot notation for the 234567 decimal number).

For details about the third method of representing autonomous system numbers, see RFC 5396.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain as the default display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain and asdot format. In addition, the default format for matching 4-byte autonomous system numbers in regular expressions is asplain, so you must ensure that any regular expressions to match 4-byte autonomous system numbers are written in the asplain format. If you want to change the default **show** command output to display 4-byte autonomous system numbers in the asdot format, use the **bgp asnotation dot** command under router configuration mode. When the asdot format is enabled as the default, any regular expressions to match 4-byte autonomous system numbers must be written using the asdot format, or the regular expression match will fail. The tables below show that although you can configure 4-byte autonomous system numbers in either asplain or asdot format, only one format is used to display **show** command output and control 4-byte autonomous system number matching for regular expressions, and the default is asplain format. To display 4-byte autonomous system numbers in **show** command output and to control matching for regular expressions in the asdot format, you must configure the **bgp asnotation dot** command. After enabling the **bgp asnotation dot** command, a hard reset must be initiated for all BGP sessions by entering the **clear ip bgp *** command.



Note

If you are upgrading to an image that supports 4-byte autonomous system numbers, you can still use 2-byte autonomous system numbers. The **show** command output and regular expression match are not changed and remain in asplain (decimal value) format for 2-byte autonomous system numbers regardless of the format configured for 4-byte autonomous system numbers.

Table 2: Default Asplain 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 65535 4-byte: 65536 to 4294967295	2-byte: 1 to 65535 4-byte: 65536 to 4294967295
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 65536 to 4294967295

Table 3: Asdot 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 65535 4-byte: 65536 to 4294967295	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535

Examples

The following output from the **show ip bgp summary** command shows the default asplain format of the 4-byte autonomous system numbers. Note the asplain format of the 4-byte autonomous system numbers, 65536 and 65550.

```
Router# show ip bgp summary
BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ  OutQ Up/Down  Statd
192.168.1.2      4    65536      7       7        1    0    0 00:03:04    0
192.168.3.2      4    65550      4       4        1    0    0 00:00:15    0
```

The following configuration is performed to change the default output format to the asdot notation format:

```
configure terminal
router bgp 65538
  bgp asnotation dot
end
clear ip bgp *
```

After the configuration is performed, the output is converted to asdot notation format as shown in the following output from the **show ip bgp summary** command. Note the asdot format of the 4-byte autonomous system numbers, 1.0 and 1.14 (these are the asdot conversions of the 65536 and 65550 autonomous system numbers).

```
Router# show ip bgp summary
BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ  OutQ Up/Down  Statd
192.168.1.2      4     1.0      9       9        1    0    0 00:04:13    0
192.168.3.2      4     1.14      6       6        1    0    0 00:01:24    0
```

After the **bgp asnotation dot** command is configured, the regular expression match format for 4-byte autonomous system paths is changed to asdot notation format. Although a 4-byte autonomous system number can be configured in a regular expression using either asplain format or asdot format, only 4-byte autonomous system numbers configured using the current default format are matched. In the first example, the **show ip bgp regexp** command is configured with a 4-byte autonomous system number in asplain format. The match fails because the default format is currently asdot format and there is no output. In the second example using asdot format, the match passes and the information about the 4-byte autonomous system path is shown using the asdot notation.



Note

The asdot notation uses a period, which is a special character in Cisco regular expressions. To remove the special meaning, use a backslash before the period.

```
Router# show ip bgp regexp ^65536$
Router# show ip bgp regexp ^1\.0$
```

```

BGP table version is 2, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
*> 10.1.1.0/24     192.168.1.2             0             0 1.0 i

```

Related Commands

Command	Description
router bgp	Configures the BGP routing process.
show ip bgp regexp	Displays routes matching the autonomous system path regular expression.
show ip bgp summary	Displays the status of all BGP connections.

bgp bestpath as-path ignore

To configure Border Gateway Protocol (BGP) to not consider the autonomous system (AS) path during best path route selection, use the **bgp bestpath as-path ignore** command in router configuration mode. To restore default behavior and configure BGP to consider the AS-path during route selection, use the **no** form of this command.

bgp bestpath as-path ignore

no bgp bestpath as-path ignore

Syntax Description

This command has no arguments or keywords.

Command Default

The AS-path is considered during BGP best path selection.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0	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.

Examples

In the following example, the BGP routing process is configured to not consider the AS-path during best path selection:

```
Router(config)# router bgp 40000
Router(config-router)# bgp bestpath as-path ignore
```

Related Commands

Command	Description
show ip bgp ipv4	Displays information about the TCP and BGP connections to neighbors.

bgp bestpath compare-routerid

To configure a Border Gateway Protocol (BGP) routing process to compare identical routes received from different external peers during the best path selection process and to select the route with the lowest router ID as the best path, use the **bgp bestpath compare-routerid** command in router configuration mode. To return the BGP routing process to the default operation, use the **no** form of this command.

bgp bestpath compare-routerid

no bgp bestpath compare-routerid

Syntax Description This command has no arguments or keywords.

Command Default The behavior of this command is disabled by default; BGP selects the route that was received first when two routes with identical attributes are received.

Command Modes Router configuration (config-router)

Command History	Release	Modification
	12.1(3)	This command was introduced.
	12.0(11)S	This command was integrated into Cisco IOS Release 12.0(11)S.
	12.1(3a)E	This command was integrated into Cisco IOS Release 12.1(3a)E.
	12.1(3)T	This command was integrated into Cisco IOS Release 12.1(3)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 The **bgp bestpath compare-routerid** command is used to configure a BGP routing process to use the router ID as the tie breaker for best path selection when two identical routes are received from two different peers (all the attributes are the same except for the router ID). When this command is enabled, the lowest router ID will be selected as the best path when all other attributes are equal.

Examples In the following example, the BGP routing process is configured to compare and use the router ID as a tie breaker for best path selection when identical paths are received from different peers:

```
Router(config)# router bgp 50000
```

```
Router(config-router)# bgp bestpath compare-routerid
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.

bgp bestpath cost-community ignore

To configure a router that is running the Border Gateway Protocol (BGP) to not evaluate the cost community attribute during the best path selection process, use the **bgp bestpath cost-community ignore** command in router configuration mode. To return the router to default operation, use the **no** form of this command.

bgp bestpath cost-community ignore

no bgp bestpath cost-community ignore

Syntax Description This command has no keywords or arguments.

Command Default The behavior of this command is enabled by default until the cost community attribute is manually configured.

Command Modes Address family configuration (config-router-af)
Router configuration (config-router)

Command History	Release	Modification
	12.0(24)S	This command was introduced.
	12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
	12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
	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.
	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 **bgp bestpath cost-community ignore** command is used to disable the evaluation of the cost community attribute to help isolate problems and troubleshoot issues that relate to BGP path selection. This command can also be used to delay the activation of cost community attribute evaluation so that cost community filtering can be deployed in a large network at the same time.

Examples The following example shows how to configure a router to not evaluate the cost community attribute during the best path selection process:

```
router bgp 50000
```

bgp bestpath cost-community ignore

```
address-family ipv4 unicast
bgp bestpath cost-community ignore
```

Related Commands

Command	Description
set extcommunity cost	Creates a set clause to apply the cost community attribute to routes that pass through a route map.
show ip bgp	Displays entries in the BGP routing table.

bgp bestpath igp-metric ignore

To specify that the system ignore the Interior Gateway Protocol (IGP) metric during Border Gateway Protocol (BGP) best path selection, use the **bgp bestpath igp-metric ignore** command in address family configuration mode. To remove the configuration to ignore the IGP metric, use the **no** form of this command.

bgp bestpath igp-metric ignore

no bgp bestpath igp-metric ignore

Syntax Description This command has no arguments or keywords.

Command Default This command is disabled by default.

Command Modes Address family configuration (config-router-af)

Command History	Release	Modification
	Cisco IOS XE Release 3.4S	This command was introduced.
	15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
	15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines The IGP metric is a configurable metric for EIGRP, IS-IS, or OSPF that is related to distance. The **bgp bestpath igp-metric ignore** command can be used independently or in conjunction with the BGP Diverse Path feature. This command does not enable the BGP Diverse Path feature.

Similarly, enabling the BGP Diverse Path feature does not necessarily require that the IGP metric be ignored. If you enable the BGP Diverse Path feature and the route reflector and its shadow route reflector are not colocated, this command must be configured on the route reflector, shadow route reflector, and provider edge (PE) routers.

This command is supported in the following address families:

- ipv4 unicast
- vpnv4 unicast
- ipv6 unicast
- vpnv6 unicast
- ipv4+label
- ipv6+label

**Note**

This command is not supported per virtual routing and forwarding (VRF); if you use it per VRF, it is at your own risk.

This command applies per VRF as follows (which is consistent with the BGP PIC/Best External feature):

- When configured under the VPNv4 or VPNv6 address-family, it applies to all VRFs, but it will be nvgened only under VPNv4/VPNv6 global.
- When configured under a particular VRF, it applies only to that VRF and will be nvgened only for that VRF.
- When configured under vpnv4 or vpnv6 global, this command can be disabled for a particular VRF by specifying the **no bgp bestpath igp-metric ignore** command. The **no** form will be nvgened under that VRF, while under VPNv4 or VPNv6 the **bgp bestpath igp-metric ignore** command is nvgened and the command applies to all other VRFs.

Examples

In the following example, the IGP metric is ignored during calculation of the BGP best path:

```
router bgp 1
 neighbor 10.1.1.1 remote-as 1
 address-family ipv4 unicast
 neighbor 10.1.1.1 activate
 maximum-paths ibgp 4
 bgp bestpath igp-metric ignore
 bgp additional-paths select backup
 bgp additional-paths install
 neighbor 10.1.1.1 advertise diverse-path backup
```

Related Commands

Command	Description
bgp additional-paths select	Specifies that the system calculate a second BGP best path.

bgp bestpath med confed

To configure a Border Gateway Protocol (BGP) routing process to compare the Multi Exit Discriminator (MED) between paths learned from confederation peers, use the **bgp bestpath med confed** command in router configuration mode. To disable MED comparison of paths received from confederation peers, use the **no** form of this command.

bgp bestpath med confed [**missing-as-worst**]

no bgp bestpath med confed [**missing-as-worst**]

Syntax Description

missing-as-worst	(Optional) Assigns the value of infinity to received routes that do not carry the MED attribute, making these routes the least desirable.

Command Default

Cisco IOS software does not consider the MED attribute when choosing among paths learned from confederation peers if this command is not enabled or if the **no** form of this command is entered.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.0	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 MED comparison between confederation peers occurs only if no external autonomous systems are in the path (an external autonomous system is an autonomous system that is not within the confederation). If an external autonomous system in the path, then the external MED is passed transparently through the confederation, and the comparison does not occur.

For example, assume that autonomous system 65000, 65001, 65002, and 65004 are part of the confederation; autonomous system 1 is not; and we are comparing route A with four paths. If the **bgp bestpath med confed** command is enabled, path 1 would be chosen. The fourth path has a lower MED, but it is not involved in the MED comparison because there is an external autonomous system in this path. The following list displays the MED for each autonomous system.

path = 65000 65004, med = 2

path = 65001 65004, med = 3

path = 65002 65004, med = 4

path = 65003 1, med = 1

Examples

In the following example, the BGP routing process is configured to compare MED values for paths learned from confederation peers:

```
Router(config)# router bgp 50000
```

```
Router(config-router)# bgp bestpath med confed
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.
show ip bgp ipv4	Displays information about the TCP and BGP connections to neighbors.

bgp bestpath med missing-as-worst

To configure a Border Gateway Protocol (BGP) routing process to assign a value of infinity to routes that are missing the Multi Exit Discriminator (MED) attribute (making the path without a MED value the least desirable path), use the **bgp bestpath med missing-as-worst** command in router configuration mode. To return the router to the default behavior (assign a value of 0 to the missing MED), use the **no** form of this command.

bgp bestpath med missing-as-worst

no bgp bestpath med missing-as-worst

Syntax Description This command has no arguments or keywords.

Command Default Cisco IOS software assigns a value of 0 to routes the are missing the MED attribute, causing the route with the missing MED attribute to be considered the best path.

Command Modes Router configuration (config-router)

Command History	Release	Modification
	12.0	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 BGP router process is configured to consider a route with a missing MED attribute as having a value of infinity (4294967294), making this path the least desirable path:

```
Router(config)# router bgp 50000
Router(config-router)# bgp bestpath med missing-as-worst
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.
show ip bgp ipv4	Displays information about the TCP and BGP connections to neighbors.

bgp bestpath prefix-validate

To disable the validation of Border Gateway Protocol (BGP) prefixes based on the autonomous system from which the prefix originates, or to allow invalid prefixes to be used as the bestpath even if valid prefixes are available, use the **bgp bestpath prefix-validate** command in router configuration mode or IPv4 or IPv6 address family configuration mode. To disable either behavior, use the **no** form of this command.

bgp bestpath prefix-validate {disable| allow-invalid}

no bgp bestpath prefix-validate {disable| allow-invalid}

Syntax Description

disable	Disables the checking of prefixes to see if they are valid and disables the storage of validation information.
allow-invalid	Allows invalid prefixes to be used as the bestpath, even if valid prefixes are available. You might want to allow invalid prefixes so that a route map can set the local preference, metric, or other property to allow the use of an invalid prefix only when no other path is available.

Command Default

Invalid prefixes are allowed to be used as the best path.

Command Modes

Router configuration (config-router)

IPv4 or IPv6 address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.
15.2(4)S	This command was implemented on the Cisco 7200 series routers.

Usage Guidelines

This command is useful for configuration testing and for use with a route map.

The default behavior, if neither the **bgp bestpath prefix-validate disable** nor the **bgp bestpath prefix-validate allow-invalid** command is configured, is to prefer prefixes in the following order:

- Those with a validation state of valid

- Those with a validation state of not found
- Those with a validation state of invalid (which will never be installed in the routing table)

These preferences override metric, local-preference, and other choices made during the bestpath computation. The standard bestpath decision tree applies only if the two paths are the same.

If both the **bgp bestpath prefix-validate disable** command and the **bgp bestpath prefix-validate allow-invalid** command are configured, the **disable** command will prevent a validation state from being assigned to prefixes, so the **allow-invalid** command will have no effect.

Examples

The following example disables the checking of prefixes to see if they are valid, and disables the storage of validation information:

```
router bgp 65000
 address-family ipv4 unicast
  bgp bestpath prefix-validate disable
```

Related Commands

Command	Description
bgp rpki server	Connects to an RPKI server and enables the validation of BGP prefixes based on the AS from which the prefix originates.
clear ip bgp rpki server	Closes the TCP connection to the specified RPKI server, purges SOVC records downloaded from that server, renegotiates the connection, and redownloads SOVC records.
show ip bgp rpki servers	Displays the current state of communication with RPKI servers.
show ip bgp rpki table	Displays the currently cached list of networks and associated AS numbers received from the RPKI server.

bgp client-to-client reflection

To enable route reflection from a BGP route reflector to clients, use the **bgp client-to-client reflection** command in router configuration mode. To disable client-to-client route reflection, use the **no** form of this command.

bgp client-to-client reflection [all]

no bgp client-to-client reflection [all]

Syntax Description

all	(Optional) This keyword does nothing in the positive or negative form of the command. It is just to remind the network administrator that the command enables [or disables] both intercluster and intracluster client-to-client reflection.

Command Default

Client-to-client route reflection is enabled by default; when a route reflector is configured, the route reflector reflects routes from a client to other clients.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
11.1	This command was introduced.
12.0(7)T	Address family configuration mode support 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 3.8S	This command was modified. The all keyword was added.

Usage Guidelines

This command affects route reflection of all routes, both intracluster and intercluster.

By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. However, if the clients are fully meshed, route reflection is not required. In this case, use the **no bgp client-to-client reflection** command to disable client-to-client reflection.

Note that the **bgp client-to-client reflection** command affects intracluster and intercluster client-to-client reflection, unlike the **bgp client-to-client reflection intra-cluster** command, which affects only intracluster (within a cluster) client-to-client route reflection.

There are three levels of configuration that can disable client-to-client reflection. The software performs them in the following order, from least specific to most specific:

- 1 Least specific: **no bgp client-to-client reflection [all]** Disables intracluster and intercluster client-to-client reflection.
- 2 More specific: **no bgp client-to-client reflection intra-cluster cluster-id any** Disables intracluster client-to-client reflection for any cluster-id.
- 3 Most specific: **no bgp client-to-client reflection intra-cluster cluster-id cluster-id1 cluster-id2 ...** Disables intracluster client-to-client reflection for the specified clusters.

When BGP is advertising updates, the software evaluates each level of configuration in order. Once any level of configuration disables client-to-client reflection, no further evaluation of more specific policies is necessary.

Note the results of the base (positive) and negative (**no**) forms of the three commands listed above:

- A negative configuration (that is, with the **no** keyword) overwrites any less specific configuration.
- A positive configuration (that is, without the **no** keyword) will lose out to (default to) what is configured in a less specific configuration.
- Configurations at any level appear in the configuration file only if they are negative.

Examples

In the following example, the local router is a route reflector, and the three neighbors are fully meshed. Because the neighbors are fully meshed, the network administrator disables both intracluster and intercluster client-to-client reflection by entering the **no** form of the command. The **no bgp client-to-client reflection** command affects all routes.

```
Device(config)# router bgp 50000
Device(config-router)# neighbor 10.24.95.22 route-reflector-client
Device(config-router)# neighbor 10.24.95.23 route-reflector-client
Device(config-router)# neighbor 10.24.95.24 route-reflector-client
Device(config-router)# no bgp client-to-client reflection
Device(config-router)# end
```

Related Commands

Command	Description
bgp client-to-client reflection intra-cluster	Enables or restores intracluster client-to-client route reflection to clients for the specified clusters.
bgp cluster-id	Sets the global cluster ID on a route reflector.
neighbor route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
show ip bgp cluster-ids	Displays cluster IDs, how many neighbors are in each cluster, and whether client-to-client route reflection has been disabled for each cluster.

bgp client-to-client reflection intra-cluster

To enable intracluster client-to-client route reflection to clients for the specified clusters, use the **bgp client-to-client reflection intra-cluster** command in router configuration mode. To disable intracluster client-to-client route reflection for the specified clusters, use the **no** form of this command.

bgp client-to-client reflection intra-cluster cluster-id {**any**| *cluster-id1* [*cluster-id2*] ...}

no bgp client-to-client reflection intra-cluster cluster-id {**any**| *cluster-id1* [*cluster-id2*] ...}

Syntax Description

cluster-id	Keyword that precedes the any keyword or the cluster IDs in the command.
any	Enables intracluster, client-to-client route reflection within any cluster configured on the route reflector.
<i>cluster-id1</i>	Cluster ID (specified by the neighbor cluster-id command) for which intracluster client-to-client route reflection is enabled. • At least one <i>cluster-id</i> is required, unless the any keyword is specified. • More than one <i>cluster-id</i> can be specified.

Command Default

Client-to-client route reflection is enabled by default; when a route reflector is configured, the route reflector reflects routes from a client to other clients.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

By default, the clients of a route reflector are not required to be fully meshed and the routes from a client are reflected to other clients. However, if the clients are fully meshed, route reflection is not required. In this case, use the **no bgp client-to-client reflection intra-cluster** command to disable client-to-client reflection; updates are not sent (reflected) because they are not necessary. Configure this command on a route reflector.

There are three levels of configuration that can disable client-to-client reflection. The software performs them in the following order, from least specific to most specific:

- 1 Least specific: **no bgp client-to-client reflection [all]** Disables intracluster and intercluster client-to-client reflection.
- 2 More specific: **no bgp client-to-client reflection intra-cluster cluster-id any** Disables intracluster client-to-client reflection for any cluster-id.
- 3 Most specific: **no bgp client-to-client reflection intra-cluster cluster-id *cluster-id1 cluster-id2* ...** Disables intracluster client-to-client reflection for the specified clusters.

When BGP is advertising updates, the software evaluates each level of configuration in order. Once any level of configuration disables client-to-client reflection, no further evaluation of more specific policies is necessary.

Note the results of the base (positive) and negative (**no**) forms of the three commands listed above:

- A negative configuration (that is, with the **no** keyword) overwrites any less specific configuration.
- A positive configuration (that is, without the **no** keyword) will lose out to (default to) what is configured in a less specific configuration.
- Configurations at any level appear in the configuration file only if they are negative.

All levels can be configured independently and all levels appear in the configuration file independently of the configuration of other levels.

Note that negative configuration makes any more specific configuration unnecessary (because even if the more specific configuration is positive, it is not processed after the negative configuration; if the more specific configuration is negative, it is functionally the same as the earlier negative configuration). The following examples illustrate this behavior.

Example 1

no bgp client-to-client reflection

no bgp client-to-client reflection intra-cluster cluster-id any

Intercluster and intracluster reflection are disabled (based on the first command). The second command disables intracluster reflection, but it is unnecessary because intracluster reflection is already disabled by the first command.

Example 2

no bgp client-to-client reflection intra-cluster cluster-id any

bgp client-to-client reflection intra-cluster cluster-id 1.1.1.1

Cluster ID 1.1.1.1 has intracluster route reflection disabled (even though the second command is positive), because the first command is used to evaluate the update. The first command was negative, and once any level of configuration disables client-to-client reflection, no further evaluation is performed.

Another way to look at this example is that the second command, because it is in a positive form, defaults to the behavior of the first command (which is less specific). Thus, the second command is unnecessary.

Note that the second command would not appear in a configuration file because it is not a negative command.

Examples

In the following example, intracluster client-to-client reflection is enabled within any cluster:

```
Device(config)# router bgp 50000
Device(config-router)# bgp client-to-client reflection intra-cluster cluster-id any
```

In the following example, intracluster client-to-client reflection is enabled within the cluster that has cluster ID 10.1.4.5:

```
Device(config)# router bgp 50000
Device(config-router)# bgp client-to-client reflection intra-cluster cluster-id 10.1.4.5
```

In the following example, intracluster client-to-client reflection is disabled for any cluster:

```
Device(config)# router bgp 50000
Device(config-router)# no bgp client-to-client reflection intra-cluster cluster-id any
```

In the following example, intracluster client-to-client reflection is disabled within the cluster that has cluster ID 10.1.4.5:

```
Device(config)# router bgp 50000
Device(config-router)# no bgp client-to-client reflection intra-cluster cluster-id 10.1.4.5
```

Related Commands

Command	Description
bgp client-to-client reflection	Enables or restores route reflection from a BGP route reflector to clients.
bgp cluster-id	Sets the cluster ID on a route reflector in a route reflector cluster.
neighbor cluster-id	Configures the cluster ID per neighbor.
neighbor route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
show ip bgp cluster-ids	Displays cluster IDs, how many neighbors are in each cluster, and whether client-to-client route reflection is disabled for each cluster.

bgp cluster-id

To set the cluster ID on a route reflector in a route reflector cluster, use the **bgp cluster-id** command in router configuration mode. To remove the cluster ID, use the **no** form of this command.

bgp cluster-id *cluster-id*

no bgp cluster-id *cluster-id*

Syntax Description

<i>cluster-id</i>	Cluster ID of this router acting as a route reflector; maximum of 4 bytes. The ID can be specified in dotted or decimal format.

Command Default

The local router ID of the route reflector is used as the cluster ID when no ID is specified or when the **no** form of this command is entered.

Command Modes

Router configuration (config-router)

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

Together, a route reflector and its clients form a *cluster*. When a single route reflector is deployed in a cluster, the cluster is identified by the router ID of the route reflector.

The **bgp cluster-id** command is used to assign a cluster ID to a route reflector when the cluster has one or more route reflectors. Multiple route reflectors are deployed in a cluster to increase redundancy and avoid a single point of failure. When multiple route reflectors are configured in a cluster, the same cluster ID is assigned to all route reflectors. This allows all route reflectors in the cluster to recognize updates from peers in the same cluster and reduces the number of updates that need to be stored in BGP routing tables.



Note

All route reflectors must maintain stable sessions between all peers in the cluster. If stable sessions cannot be maintained, then overlay route reflector clusters should be used instead (route reflectors with different cluster IDs).

Examples

In the following example, the local router is one of the route reflectors serving the cluster. It is configured with the cluster ID to identify the cluster.

```
Router(config)# router bgp 50000  
Router(config-router)# neighbor 192.168.70.24 route-reflector-client  
Router(config-router)# bgp cluster-id 10.0.1.2
```

Related Commands

Command	Description
bgp client-to-client reflection	Enables or restores route reflection from a BGP route reflector to clients.
neighbor route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
show ip bgp	Displays entries in the BGP routing table.

bgp confederation identifier

To specify a BGP confederation identifier, use the **bgp confederation identifier** command in router configuration mode. To remove the confederation identifier, use the **no** form of this command.

bgp confederation identifier *autonomous-system-number*

no bgp confederation identifier *autonomous-system-number*

Syntax Description

<i>autonomous-system-number</i>	Number of an autonomous system number used to configure a single autonomous system number to identify a group of smaller autonomous systems as a single confederation. Number in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the router bgp command.

Command Default

No BGP confederation identifier is identified.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.

Release	Modification
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(1)SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

The **bgp confederation identifier** command is used to configure a single autonomous system number to identify a group of smaller autonomous systems as a single confederation.

A confederation can be used to reduce the internal BGP (iBGP) mesh by dividing a large single autonomous system into multiple subautonomous systems and then grouping them into a single confederation. The subautonomous systems within the confederation exchange routing information like iBGP peers. External peers interact with the confederation as if it were a single autonomous system.

Each subautonomous system is fully meshed within itself and has a few connections to other autonomous systems within the confederation. Next hop, Multi Exit Discriminator (MED), and local preference information is preserved throughout the confederation, allowing you to retain a single Interior Gateway Protocol (IGP) for all the autonomous systems.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain--65538 for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot--1.2 for example--as the only configuration format, regular expression match, and output display, with no asplain support.

If one member of a BGP confederation is identified using a 4-byte autonomous system number, all other members of a BGP confederation must be upgraded to support 4-byte autonomous system numbers.

Examples

In the following example, the routing domain is divided into autonomous systems 50001, 50002, 50003, 50004, 50005, and 50006 and is identified by the confederation identifier 50007. Neighbor 10.2.3.4 is a peer inside of the routing domain confederation. Neighbor 10.4.5.6 is a peer outside of the routing domain confederation. To external peers and routing domains, the confederation appears as a single autonomous system with the number 50007.

```
router bgp 50000
  bgp confederation identifier 50007
  bgp confederation peers 50001 50002 50003 50004 50005 50006
  neighbor 10.2.3.4 remote-as 50001
  neighbor 10.4.5.6 remote-as 40000
end
```

In the following example, the routing domain is divided into autonomous systems using 4-byte autonomous system numbers 65538, 65536, and 65550 in asplain format and identified by the confederation identifier 65545. Neighbor 192.168.1.2 is a peer inside of the routing domain confederation. Neighbor 192.168.2.2 is a peer outside of the routing domain confederation. To external peers and routing domains, the confederation appears as a single autonomous system with the number 65545. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or a later release.

```
router bgp 65550
  bgp confederation identifier 65545
  bgp confederation peers 65538 65536 65550
  neighbor 192.168.1.2 remote-as 65536
  neighbor 192.168.2.2 remote-as 65547
end
```

In the following example, the routing domain is divided into autonomous systems using 4-byte autonomous system numbers 1.2 and 1.0 in asdot format and is identified by the confederation identifier 1.9. Neighbor 192.168.1.2 is a peer inside of the routing domain confederation. Neighbor 192.168.2.2 is a peer outside of the routing domain confederation. To external peers and routing domains, the confederation appears as a single autonomous system with the number 1.9. This example requires Cisco IOS Release 12.0(32)S12, 12.4(24)T, or Cisco IOS XE Release 2.3 where asdot notation is the only format for 4-byte autonomous system numbers. This configuration can also be performed using Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or later releases.

```
router bgp 1.14
  bgp confederation identifier 1.9
  bgp confederation peers 1.2 1.0
  neighbor 192.168.1.2 remote-as 1.0
  neighbor 192.168.2.2 remote-as 1.11
end
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
bgp confederation peers	Configures subautonomous systems to belong to a single confederation.
router bgp	Configures the BGP routing process.

bgp confederation peers

To configure subautonomous systems to belong to a single confederation, use the **bgp confederation peers** command in router configuration mode. To remove an autonomous system from the confederation, use the **no** form of this command.

bgp confederation peers *autonomous-system-number* [... *autonomous-system-number*]

no bgp confederation peers *autonomous-system-number* [... *autonomous-system-number*]

Syntax Description

<i>autonomous-system-number</i>	Autonomous system numbers for BGP peers that will belong to the confederation. Number in the range from 1 to 65535. The autonomous system number of the local router is not allowed to be specified in this command. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the router bgp command.

Command Default

No BGP peers are configured to be members of a BGP confederation.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.

Release	Modification
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS Release 15.1(1)SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

The **bgp confederation peers** command is used to configure multiple autonomous systems as a single confederation. The ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *autonomous-system-number* argument.

The autonomous system number of the router on which this command is being specified is not allowed in this command (not allowed as a confederation peer). If you specify the local router's autonomous system number in the **bgp confederation peers** command, the error message "Local member-AS not allowed in confed peer list" will appear.

The autonomous systems specified in this command are visible internally to the confederation. Each autonomous system is fully meshed within itself. Use the **bgp confederation identifier** command to specify the confederation to which the autonomous systems belong.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain--65538 for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot--1.2 for example--as the only configuration format, regular expression match, and output display, with no asplain support.

If one member of a BGP confederation is identified using a 4-byte autonomous system number, all other members of a BGP confederation must be upgraded to support 4-byte autonomous system numbers.

Examples

In the following example, autonomous systems 50001, 50002, 50003, 50004, and 50005 are configured to belong to a single confederation under the identifier 50000:

```
router bgp 50000
  bgp confederation identifier 50000
  bgp confederation peers 50001 50002 50003 50004 50005
```

In the following example, the routing domain is divided into autonomous systems using 4-byte autonomous system numbers 65538 and 65536, and is identified by the confederation identifier 65545. Neighbor 192.168.1.2 is a peer inside of the routing domain confederation. Neighbor 192.168.2.2 is a peer outside of the routing domain confederation. To external peers and routing domains, the confederation appears as a single autonomous system with the number 65545. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or a later release.

```
router bgp 65550
  bgp confederation identifier 65545
  bgp confederation peers 65538 65536
  neighbor 192.168.1.2 remote-as 65536
  neighbor 192.168.2.2 remote-as 65547
end
```

In the following example, the routing domain is divided into autonomous systems using 4-byte autonomous system numbers 1.2, 1.0, and 1.14 and is identified by the confederation identifier 1.9. Neighbor 192.168.1.2 is a peer inside of the routing domain confederation. Neighbor 192.168.2.2 is a peer outside of the routing domain confederation. To external peers and routing domains, the confederation appears as a single autonomous system with the number 1.9. This example requires Cisco IOS Release 12.0(32)S12, 12.4(24)T, or Cisco IOS XE Release 2.3 where asdot notation is the only format for 4-byte autonomous system numbers. This configuration can also be performed using Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or later releases.

```
router bgp 1.14
  bgp confederation identifier 1.9
  bgp confederation peers 1.2 1.0 1.14
  neighbor 192.168.1.2 remote-as 1.0
  neighbor 192.168.2.2 remote-as 1.11
end
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
bgp confederation identifier	Specifies a BGP confederation identifier.
router bgp	Configures the BGP routing process.

bgp consistency-checker

To enable the BGP Consistency Checker feature, use the **bgp consistency-checker** command in router configuration mode. To disable the BGP Consistency Checker feature, use the **no** form of this command.

bgp consistency-checker {**error-message**| **auto-repair**} [**interval** *minutes*]

no bgp consistency-checker

Syntax Description

error-message	Specifies that when an inconsistency is found, the system will only generate a syslog message.
auto-repair	Specifies that when an inconsistency is found, the system will generate a syslog message and take action based on the type of inconsistency found.
interval <i>minutes</i>	(Optional) Specifies the interval at which the BGP consistency checker process occurs. The range is 5 to 1440 minutes. The default is 1440 minutes (one day).

Command Default

No BGP consistency check is performed.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.1(2)S	This command was introduced.
Cisco IOS XE 3.3S	This command was integrated into Cisco IOS XE 3.3S.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

A BGP route inconsistency with a peer occurs when an update or a withdraw is not sent to a peer, and black-hole routing can result. The BGP consistency checker feature is a low-priority process created to address this issue. This feature performs nexthop-label, RIB-out, and aggregation consistency checks. When BGP consistency checker is enabled, it is performed for all address families. Once the process identifies such an inconsistency:

- If the **error-message** keyword is specified, the system will report the inconsistency with a syslog message, and will also perform forceful aggregation reevaluation in the case of an aggregation inconsistency.
- If the **auto-repair** keyword is specified, the system will report the inconsistency with a syslog message and also take appropriate action, such as a route refresh request or an aggregation reevaluation, depending on the type of inconsistency.

Examples

In the following example, BGP consistency checker is enabled. If a BGP route inconsistency is found, the system will send a syslog message and take appropriate action.

```
Router(config)# router bgp 65000  
Router(config-router)# bgp consistency-checker auto-repair
```

Related Commands

Command	Description
show ip bgp vpnv4 all inconsistency nexthop-label	Displays routes that have nexthop-label inconsistency found by BGP consistency checker.

bgp dampening

To enable BGP route dampening or change BGP route dampening parameters, use the **bgp dampening** command in address family or router configuration mode. To disable BGP dampening, use the **no** form of this command.

bgp dampening [*half-life reuse suppress max-suppress-time*] **route-map** *map-name*]

no bgp dampening [*half-life reuse suppress max-suppress-time*] **route-map** *map-name*]

Syntax Description

<i>half-life</i>	(Optional) Time (in minutes) after which a penalty is decreased. Once the route has been assigned a penalty, the penalty is decreased by half after the half-life period (which is 15 minutes by default). The process of reducing the penalty happens every 5 seconds. The range of the half-life period is 1 to 45 minutes. The default is 15 minutes.
<i>reuse</i>	(Optional) Reuse values based on accumulated penalties. If the penalty for a flapping route decreases enough to fall below this value, the route is unsuppressed. The process of unsuppressing routes occurs at 10-second increments. The range of the reuse value is from 1 to 20000; the default is 750.
<i>suppress</i>	(Optional) A route is suppressed when its penalty exceeds this limit. The range is from 1 to 20000; the default is 2000.
<i>max-suppress-time</i>	(Optional) Maximum time (in minutes) a route can be suppressed. The range is from 1 to 20000; the default is 4 times the <i>half-life</i> . If the <i>half-life</i> value is allowed to default, the maximum suppress time defaults to 60 minutes. When the <i>max-suppress-time</i> is configured, the maximum penalty will never be exceeded, regardless of the number of times that the prefix dampens. The maximum penalty is computed with the following formula: Maximum penalty = reuse-limit * 2 ^(maximum suppress time/half time)
route-map <i>map-name</i>	(Optional) Specified the name of the route map that controls where BGP route dampening is enabled.

Command Default

BGP dampening is disabled by default. The following values are used when this command is enabled without configuring any optional arguments:

half-life : 15 minutes *reuse*: 750 *suppress*: 2000 *max-suppress-time*: 4 times *half-life*

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	Address family configuration mode support 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.

Usage Guidelines

The **bgp dampening** command is used to enable BGP route dampening. This command can be entered without any arguments or keywords. The *half-life*, *reuse*, *suppress*, and *max-suppress-time* arguments are position-dependent; meaning that if any of these arguments are entered, then all optional arguments must be entered.

When BGP dampening is configured and a prefix is withdrawn, BGP considers the withdrawn prefix as a flap and increases the penalty by a 1000. If BGP receives an attribute change, BGP increases the penalty by 500. If then the prefix has been withdrawn, BGP keeps the prefix in the BGP table as a history entry. If the prefix has not been withdrawn by the neighbor and BGP is not using this prefix, the prefix is marked as dampened. Dampened prefixes are not used in the BGP decision process and not installed to the routing table.



Note

This command is not supported in the address family configuration mode in Cisco IOS Release 12.2SX and later releases.

Examples

In the following example, the BGP dampening values are set to 30 minutes for the half life, 1500 for the reuse value, 10000 for the suppress value, and 120 minutes for the maximum suppress time:

```
Router(config)# router bgp 5
Router(config-router)# address-family ipv4 unicast

Router(config-router-af)# bgp dampening 30 1500 10000 120
Router(config-router-af)# end
```

In the following example, BGP dampening is applied to prefixes filtered through the route-map named BLUE:

```
Router(config)# ip prefix-list RED permit 10.0.0.0/8
Router(config)# !
Router(config)# route-map BLUE

Router(config-route-map)# match ip address ip prefix-list RED
Router(config-route-map)# exit
```

```

Router(config)# router bgp 50000

Router(config-router)# address-family ipv4
Router(config-router-af)# bgp dampening route-map BLUE
Router(config-router-af)# end

```

Related Commands

Command	Description
clear bgp nsap flap-statistics	Clears BGP flap statistics.
clear ip bgp dampening	Clears BGP route dampening information and unsuppresses the suppressed routes.
set dampening	Applies BGP dampening to prefixes filtered through a route map.
show ip bgp dampened-paths	Displays BGP dampened routes.
show ip bgp flap-statistics	Displays BGP flap statistics.

bgp default ipv4-unicast

To set the IP version 4 (IPv4) unicast address family as default for BGP peering session establishment, use the **bgp default ipv4-unicast** command in router configuration mode. To disable default IPv4 unicast address family for peering session establishment, use the **no** form of this command.

bgp default ipv4-unicast

no bgp default ipv4-unicast

Syntax Description This command has no arguments or keywords.

Command Default IPv4 address family routing information is advertised by default for each BGP routing session configured with the **neighbor remote-as** command, unless you first configure the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

Command Modes Router configuration (config-router)

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 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
	15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines The **bgp default ipv4-unicast** command is used to enable the automatic exchange of IPv4 address family prefixes. The **neighbor activate** address family configuration command must be entered in each IPv4 address family session before prefix exchange will occur.

Examples In the following example, the automatic exchange of IP version 4 unicast address family routing information is disabled:

```
Device(config)# router bgp 50000
Device(config-router)# no bgp default ipv4-unicast
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a neighboring router.

bgp default local-preference

To change the default local preference value, use the **bgp default local-preference** command in router configuration mode. To return the local preference value to the default setting, use the **no** form of this command.

bgp default local-preference *number*

no bgp default local-preference *number*

Syntax Description

<i>number</i>	Local preference value from 0 to 4294967295.

Command Default

Cisco IOS software applies a local preference value of 100 if this command is not enabled or if the **no** form of this command is entered.

Command Modes

Router configuration (config-router)

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

The local preference attribute is a discretionary attribute that is used to apply the degree of preference to a route during the BGP best path selection process. This attribute is exchanged only between iBGP peers and is used to determine local policy. The route with the highest local preference is preferred.

Examples

In the following example, the local preference value is set to 200:

```
Router(config)# router bgp 50000
```

```
Router(config-router)# bgp default local-preference 200
```

Related Commands

Command	Description
set local-preference	Specifies a preference value for the autonomous system path.

bgp deterministic-med

To enforce the deterministic comparison of the Multi Exit Discriminator (MED) value between all paths received from within the same autonomous system, use the **bgp deterministic-med** command in router configuration mode. To disable the required MED comparison, use the **no** form of this command.

bgp deterministic-med

no bgp deterministic-med

Syntax Description This command has no arguments or keywords.

Command Default Cisco IOS software does not enforce the deterministic comparison of the MED variable between all paths received from the same autonomous system.

Command Modes Router configuration (config-router)

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.

Examples In the following example, BGP is configured to compare the MED during path selection for routes advertised by the same subautonomous system within a confederation:

```
Router(config)# router bgp 50000
Router(config-router)# bgp deterministic-med
```

The following example **show ip bgp** command output shows how route selection is affected by the configuration of the **bgp deterministic-med** command. The order in which routes are received affects how routes are selected for best path selection when the **bgp deterministic-med** command is not enabled. The following sample output from the **show ip bgp** command shows three paths that are received for the same prefix (10.100.0.0), and the **bgp deterministic-med** command is not enabled:

```
Router# show ip bgp 10.100.0.0

BGP routing table entry for 10.100.0.0/16, version 40
Paths: (3 available, best #3, advertised over IBGP, EBGP)
 109
   192.168.43.10 from 192.168.43.10 (192.168.43.1)
      Origin IGP, metric 0, localpref 100, valid, internal
 2051
   192.168.43.22 from 192.168.43.22 (192.168.43.2)
```

```

    Origin IGP, metric 20, localpref 100, valid, internal
2051
    192.168.43.3 from 192.168.43.3 (10.4.1.1)
    Origin IGP, metric 30, valid, external, best

```

If the **bgp deterministic-med** feature is not enabled on the router, the route selection can be affected by the order in which the routes are received. Consider the following scenario in which a router received three paths for the same prefix:

The **clear ip bgp *** command is entered to clear all routes in the local routing table.

```
Router# clear ip bgp *
```

The **show ip bgp** command is issued again after the routing table has been repopulated. Note that the order of the paths changed after clearing the BGP session. The results of the selection algorithm also changed because the order in which the paths were received was different for the second session.

```
Router# show ip bgp 10.100.0.0
```

```

BGP routing table entry for 10.100.0.0/16, version 2
Paths: (3 available, best #3, advertised over EBGp)
 109 192.168.43.10 from 192.168.43.10 (192.168.43.1)
    Origin IGP, metric 0, localpref 100, valid, internal
 2051
    192.168.43.3 from 192.168.43.3 (10.4.1.1)
    Origin IGP, metric 30, valid, external
 2051
    192.168.43.22 from 192.168.43.22 (192.168.43.2)
    Origin IGP, metric 20, localpref 100, valid, internal, best

```

If the **bgp deterministic-med** command is enabled, then the result of the selection algorithm will always be the same, regardless of the order in which the paths are received by the local router. The following output is always generated when the **bgp deterministic-med** command is entered on the local router in this scenario:

```
Router# show ip bgp 10.100.0.0
```

```

BGP routing table entry for 10.100.0.0/16, version 15
Paths: (3 available, best #1, advertised over EBGp)
 109
    192.168.43.10 from 192.168.43.10 (192.168.43.1)
    Origin IGP, metric 0, localpref 100, valid, internal, best 3
 192.168.43.22 from 192.168.43.22 (192.168.43.2)
    Origin IGP, metric 20, localpref 100, valid, internal 3
 192.168.43.3 from 192.168.43.3 (10.4.1.1)
    Origin IGP, metric 30, valid, external

```

Related Commands

Command	Description
bgp always-compare-med	Enables the comparison of the MED for paths from neighbors in different autonomous systems.
clear ip bgp	Resets a BGP connection or session.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

bgp dmzlink-bw

To configure BGP to distribute traffic proportionally over external links with unequal bandwidth when multipath load balancing is enabled, use the **bgp dmzlink-bw** command in address family configuration mode. To disable traffic distribution that is proportional to the link bandwidth, use the **no** form of this command.

bgp dmzlink-bw

no bgp dmzlink-bw

Syntax Description This command has no arguments or keywords.

Command Default BGP traffic is not distributed proportionally over external links with unequal bandwidth.

Command Modes Address family configuration (config-router-af)

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.
	12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
	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 **bgp dmzlink-bw** command is used to configure BGP to distribute traffic proportionally to the bandwidth of external links. This command is configured for multipath load balancing between directly connected external BGP (eBGP) neighbors. This command is used with BGP multipath features to configure load balancing over links with unequal bandwidth. The **neighbor dmzlink-bw** command must also be configured for each external link through which multipath load balancing is configured to advertise the link bandwidth as an extended community. The **neighbor send-community** command must be configured to exchange the link bandwidth extended community with internal BGP (iBGP) peers.

Examples The following example shows how to configure the **bgp dmzlink-bw** command to allow multipath load balancing to distribute link traffic proportionally to the bandwidth of each external link and to advertise the bandwidth of these links to iBGP peers as an extended community:

```
Router(config)# router bgp 45000
Router(config-router)# neighbor 10.10.10.1 remote-as 100
```

```

Router(config-router)# neighbor 10.10.10.1 update-source Loopback 0
Router(config-router)# neighbor 10.10.10.3 remote-as 100
Router(config-router)# neighbor 10.10.10.3 update-source Loopback 0
Router(config-router)# neighbor 172.16.1.1 remote-as 200
Router(config-router)# neighbor 172.16.1.1 ebgp-multihop 1
Router(config-router)# neighbor 172.16.2.2 remote-as 200
Router(config-router)# neighbor 172.16.2.2 ebgp-multihop 1
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp dmzlink-bw
Router(config-router-af)# neighbor 10.10.10.1 activate
Router(config-router-af)# neighbor 10.10.10.1 next-hop-self
Router(config-router-af)# neighbor 10.10.10.1 send-community both
Router(config-router-af)# neighbor 10.10.10.3 activate
Router(config-router-af)# neighbor 10.10.10.3 next-hop-self
Router(config-router-af)# neighbor 10.10.10.3 send-community both
Router(config-router-af)# neighbor 172.16.1.1 activate
Router(config-router-af)# neighbor 172.16.1.1 dmzlink-bw
Router(config-router-af)# neighbor 172.16.2.2 activate
Router(config-router-af)# neighbor 172.16.2.2 dmzlink-bw
Router(config-router-af)# maximum-paths ibgp 6
Router(config-router-af)# maximum-paths 6

```

Related Commands

Command	Description
neighbor dmzlink-bw	Configures BGP to advertise the bandwidth of links that are used to exit an autonomous system.
neighbor send-community	Specifies that a communities attribute should be sent to a BGP neighbor.

bgp enforce-first-as

To configure a router to deny an update received from an external BGP (eBGP) peer that does not list its autonomous system number at the beginning of the AS_PATH in the incoming update, use the **bgp enforce-first-as** command in router configuration mode. To disable this behavior, use the **no** form of this command.

bgp enforce-first-as

no bgp enforce-first-as

Syntax Description This command has no arguments or keywords.

Command Default The behavior of this command is enabled by default.

Command Modes Router configuration (config-router)

Command History	Release	Modification
	12.0(3)S	This command was introduced.
	12.0(26)S	The default behavior for this command was changed to enabled in Cisco IOS Release 12.0(26)S.
	12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
	12.3(2)	This command was integrated into Cisco IOS Release 12.3(2).
	12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
	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 **bgp enforce-first-as** command is used to deny incoming updates received from eBGP peers that do not list their autonomous system number as the first segment in the AS_PATH attribute. Enabling this command prevents a misconfigured or unauthorized peer from misdirecting traffic (spoofing the local router) by advertising a route as if it was sourced from another autonomous system.

Examples

In the following example, all incoming updates from eBGP peers are examined to ensure that the first autonomous system number in the AS_PATH is the local AS number of the transmitting peer. In the following example, updates from the 10.100.0.1 peer will be discarded if the first AS number is not 65001.

```
Router(config)# router bgp 50000

Router(config-router)# bgp enforce-first-as

Router(config-router)# address-family ipv4

Router(config-router-af)# neighbor 10.100.0.1 remote-as 65001
Router(config-router-af)# end
```

bgp enhanced-error

To restore the default behavior so that any malformed Update message is treat-as-withdraw, use the **bgp enhanced-error** command in router configuration mode. To disable the function, use the **no** form of this command.

bgp enhanced-error

no bgp enhanced-error

Syntax Description This command has no arguments or keywords.

Command Default The Enhanced Attribute Error Handling feature is enabled by default.

Command Modes Router configuration (config-router)

Command History	Release	Modification
	15.2(4)S	This command was introduced.
	Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS Release XE 3.7S.
	15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines This command controls the BGP Enhanced Attribute Error Handling feature, which is enabled by default. This feature avoids peer sessions flapping due to malformed Update messages. Such Update messages are treat-as-withdraw.

This feature causes BGP to format the MP_REACH attribute in front of other attributes in the Update message. That is necessary because if any of the attribute lengths are malformed, there is no way of reaching the MP_REACH attribute if it is put at the end, and therefore no way to withdraw the prefixes. If the feature is disabled, BGP will format the MP_REACH attribute at the end of the Update message.

Examples In the following example, Enhanced Attribute Error Handling is enabled (after it had been disabled):

```
router bgp 65000
  bgp enhanced-error
```

Related Commands	Command	Description
	show ip bgp neighbors	Displays the configured discard and treat-as-withdraw attribute values and counters of incoming Update messages containing those attributes.

 **bgp enhanced-error**

bgp fast-external-fallover

To configure a Border Gateway Protocol (BGP) routing process to immediately reset external BGP peering sessions if the link used to reach these peers goes down, use the **bgp fast-external-fallover** command in router configuration mode. To disable BGP fast external fallover, use the **no** form of this command.

bgp fast-external-fallover

no bgp fast-external-fallover

Syntax Description This command has no arguments or keywords.

Command Default BGP fast external fallover is enabled by default in Cisco IOS software.

Command Modes Router configuration (config-router)

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(7)T	Address family configuration mode support 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.

Usage Guidelines The **bgp fast-external-fallover** command is used to disable or enable fast external fallover for BGP peering sessions with directly connected external peers. The session is immediately reset if link goes down. Only directly connected peering sessions are supported.

If BGP fast external fallover is disabled, the BGP routing process will wait until the default hold timer expires (3 keepalives) to reset the peering session. BGP fast external fallover can also be configured on a per-interface basis using the **ip bgp fast-external-fallover** interface configuration command.

Examples In the following example, the BGP fast external fallover feature is disabled. If the link through which this session is carried flaps, the connection will not be reset.

```
Router(config)# router bgp 50000
```

```
Router(config-router)# no bgp fast-external-fallover
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
ip bgp fast-external-fallover	Configures per-interface BGP fast external fallover.

bgp graceful-restart

To enable the Border Gateway Protocol (BGP) graceful restart capability globally for all BGP neighbors, use the **bgp graceful-restart** command in address family or in router configuration mode. To disable the BGP graceful restart capability globally for all BGP neighbors, use the **no** form of this command.

bgp graceful-restart [**extended**] **restart-time** *seconds* [**stalepath-time** *seconds*] [**all**]

no bgp graceful-restart

Syntax Description

extended	(Optional) Enables BGP graceful restart extension.
restart-time <i>seconds</i>	(Optional) Sets the maximum time period that the local router will wait for a graceful-restart-capable neighbor to return to normal operation after a restart event occurs. The default value for this argument is 120 seconds. The configurable range of values is from 1 to 3600 seconds.
stalepath-time <i>seconds</i>	(Optional) Sets the maximum time period that the local router will hold stale paths for a restarting peer. All stale paths are deleted after this timer expires. The default value for this argument is 360 seconds. The configurable range of values is from 1 to 3600 seconds
all	(Optional) Enables BGP graceful restart capability for all address family modes.

Command Default

The following default values are used when this command is entered without any keywords or arguments:

restart-time : 120 seconds **stalepath-time**: 360 seconds



Note

Changing the restart and stalepath timer values is not required to enable the BGP graceful restart capability. The default values are optimal for most network deployments, and these values should be adjusted only by an experienced network operator.

Command Modes

Address-family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(28)SB	Support for this command was added 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	Support for IPv6 was added. The optional all keyword was added.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
12.2(33)XNE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)XNE .
Cisco IOS XE Release 3.11S	This command was modified. The extended keyword was added.

Usage Guidelines

The **bgp graceful-restart** command is used to enable or disable the graceful restart capability globally for all BGP neighbors in a BGP network. The graceful restart capability is negotiated between nonstop forwarding (NSF)-capable and NSF-aware peers in OPEN messages during session establishment. If the graceful restart capability is enabled after a BGP session has been established, the session will need to be restarted with a hard reset.

The graceful restart capability is supported by NSF-capable and NSF-aware routers. A router that is NSF-capable can perform a stateful switchover (SSO) operation (graceful restart) and can assist restarting peers by holding routing table information during the SSO operation. A router that is NSF-aware functions like a router that is NSF-capable but cannot perform an SSO operation.

The BGP graceful restart capability is enabled by default when a supporting version of Cisco IOS software is installed. The default timer values for this feature are optimal for most network deployments. We recommend that they are adjusted only by experienced network operators. When adjusting the timer values, the restart timer should not be set to a value greater than the hold time that is carried in the OPEN message. If consecutive restart operations occur, routes (from a restarting router) that were previously marked as stale will be deleted.

**Note**

Changing the restart and stalepath timer values is not required to enable the BGP graceful restart capability. The default values are optimal for most network deployments, and these values should be adjusted only by an experienced network operator.

Examples

In the following example, the BGP graceful restart capability is enabled:

```
Router# configure terminal
Router(config)# router bgp 65000
Router(config-router)# bgp graceful-restart
```

In the following example, the restart timer is set to 130 seconds:

```
Router# configure terminal
Router(config)# router bgp 65000
Router(config-router)# bgp graceful-restart restart-time 130
```

In the following example, the stalepath timer is set to 350 seconds:

```
Router# configure terminal
Router(config)# router bgp 65000
Router(config-router)# bgp graceful-restart stalepath-time 350
```

In the following example, the **extended** keyword is used:

```
Router# configure terminal
Router(config)# router bgp 65000
Router(config-router)# bgp graceful-restart extended
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

bgp graceful-shutdown all

To enable the Border Gateway Protocol (BGP) graceful shutdown capability globally for all BGP neighbors, including virtual routing and forwarding (VRF) neighbors, use the **bgp graceful-shutdown all** command in router configuration mode. To disable the BGP graceful shutdown capability, use the **no** form of this command.

bgp graceful-shutdown all {**neighbors** | **vrf**s} {*shutdown-time* {**community** {*community-number* | *formatted-community-value*} [**local-preference** [*local-pref-value*]] | **local-preference** *local-pref-value* [**community** [*community-number* | *formatted-community-value*]]} | **activate**}

no bgp graceful-shutdown all {**neighbors** | **vrf**s} {*shutdown-time* {**community** {*community-number* | *formatted-community-value*} [**local-preference** [*local-pref-value*]] | **local-preference** *local-pref-value* [**community** [*community-number* | *formatted-community-value*]]} | **activate**}

Syntax Description

neighbors	Enables graceful shutdown of all BGP neighbors.
vrf s	Enables graceful shutdown of BGP sessions associated only with VRF neighbors.
<i>shutdown-time</i>	Sets the shutdown time for all BGP neighbors or only for VRF neighbors. The shutdown time ranges from 30 to 65535 seconds.
community	Sets community for all BGP graceful shutdown routes.
<i>community-number</i>	Sets the community value for BGP graceful shutdown routes. This value ranges from 1 to 4294967295.
<i>formatted-community-value</i>	Sets the community value for BGP graceful shutdown routes in the aa:nn format.
local-preference	Sets local preference for all BGP graceful shutdown routes.
<i>local-pref-value</i>	Sets local preference value for all BGP graceful shutdown routes. This value ranges from 1 to 4294967295.
activate	Enables activation of graceful shutdown of all BGP neighbors or only VRF neighbors.

Command Default

The BGP graceful-shutdown feature is disabled by default.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

Using the BGP GSHUT enhancement feature, you can gracefully shutdown either all (including VRF) neighbors or only the VRF neighbors that are already configured across all BGP sessions. To enable the BGP GSHUT enhancement feature on the device, you must configure either the **community** keyword or the **local-preference** keyword in the **bgp graceful-shutdown all** command. Use the **activate** keyword to activate graceful shutdown either across all neighbors or only across all VRF neighbors, across all BGP sessions.

Examples

The following example shows how to enable and activate the BGP GSHUT enhancement feature across all neighbors:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bgp graceful-shutdown all neighbors 180 local-preference 20 community 10
Device(config-router)# bgp graceful-shutdown all neighbors activate
Device(config-router)# end
```

**Note**

In this example, the neighbors will gracefully shutdown within the specified duration of 180 seconds.

Following is sample output from the **show ip bgp** command, which displays the graceful shutdown time for each neighbor:

**Note**

In this example, there are two IPv4 neighbors configured with IP address 10.2.2.2 and 172.16.2.1 and one VRF neighbor, tagged v1, is configured with IP address 192.168.1.1.

```
Device# show ip bgp neighbors 10.2.2.2 | include shutdown

Graceful Shutdown Timer running, schedule to reset the peer in 00:02:47 seconds
Graceful Shutdown Localpref set to 20
Graceful Shutdown Community set to 10
```

```
Device# show ip bgp neighbors 172.16.2.1 | include shutdown

Graceful Shutdown Timer running, schedule to reset the peer in 00:02:38 seconds
Graceful Shutdown Localpref set to 20
Graceful Shutdown Community set to 10
```

```
Device# show ip bgp vpnv4 vrf v1 neighbors 192.168.1.1 | include shutdown

Graceful Shutdown Timer running, schedule to reset the peer in 00:01:45 seconds
Graceful Shutdown Localpref set to 20
Graceful Shutdown Community set to 10
```

Following is sample output from the **show running-config** command, which displays information associated with the BGP session in router configuration mode:

```
Device# show running-config | session router bgp
```

bgp graceful-shutdown all

```

router bgp 65000
bgp log-neighbor-changes
bgp graceful-shutdown all neighbors 180 local-preference 20 community 10
network 10.1.1.0 mask 255.255.255.0
neighbor 10.2.2.2 remote-as 40
neighbor 10.2.2.2 shutdown
neighbor 172.16.2.1 remote-as 10
neighbor 172.16.2.1 shutdown
!
address-family vpnv4
neighbor 172.16.2.1 activate
neighbor 172.16.2.1 send-community both
exit-address-family
!
address-family ipv4 vrf v1
neighbor 192.168.1.1 remote-as 30
neighbor 192.168.1.1 shutdown
neighbor 192.168.1.1 activate
neighbor 192.168.1.1 send-community both
exit-address-family

```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.
show running-config	Displays running configuration on a device.

bgp inject-map

To configure conditional route injection to inject more specific routes into a Border Gateway Protocol (BGP) routing table, use the **bgp inject-map** command in address family or router configuration mode. To disable a conditional route injection configuration, use the **no** form of this command.

bgp inject-map *inject-map* **exist-map** *exist-map* [**copy-attributes**]

no bgp inject-map *inject-map* **exist-map** *exist-map*

Syntax Description

<i>inject-map</i>	Name of the route map that specifies the prefixes to inject into the local BGP routing table.
exist-map <i>exist-map</i>	Specifies the name of the route map containing the prefixes that the BGP speaker will track.
copy-attributes	(Optional) Configures the injected route to inherit attributes of the aggregate route.

Command Default

No specific routes are injected into a BGP routing table.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.

Usage Guidelines

The **bgp inject-map** command is used to configure conditional route injection. Conditional route injection allows you to originate a more specific prefix into a BGP routing table without a corresponding match. Two route maps (*exist-map* and *inject-map*) are configured in global configuration mode and then specified with the **bgp inject-map** command in address family or router configuration mode.

The *exist-map* argument specifies a route map that defines the prefix that the BGP speaker will track. This route map must contain a **match ip address prefix-list** command statement to specify the aggregate prefix and a **match ip route-source prefix-list** command statement to specify the route source.

The *inject-map* argument defines the prefixes that will be created and installed into the routing table. Injected prefixes are installed in the local BGP RIB. A valid parent route must exist; Only prefixes that are equal to or more specific than the aggregate route (existing prefix) can be injected.

The optional **copy-attributes** keyword is used to optionally configure the injected prefix to inherit the same attributes as the aggregate route. If this keyword is not entered, the injected prefix will use the default attributes for locally originated routes.

Examples

In the following example, conditional route injection is configured. Injected prefixes will inherit the attributes of the aggregate (parent) route.

```
Router(config)# ip prefix-list ROUTE permit 10.1.1.0/24
Router(config)# ip prefix-list ROUTE_SOURCE permit 10.2.1.1/32
Router(config)# ip prefix-list ORIGINATED_ROUTES permit 10.1.1.0/25
Router(config)# ip prefix-list ORIGINATED_ROUTES permit 10.1.1.128/25
Router(config)# route-map LEARNED_PATH permit 10
Router(config-route-map)# match ip address prefix-list ROUTE
Router(config-route-map)# match ip route-source prefix-list ROUTE_SOURCE
Router(config-route-map)# exit
Router(config)# route-map ORIGINATE permit 10
Router(config-route-map)# set ip address prefix-list ORIGINATED_ROUTES
Router(config-route-map)# set community 14616:555 additive
Router(config-route-map)# exit
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp inject-map ORIGINATE exist-map LEARNED_PATH copy-attributes
Router(config-router-af)# end
```

Related Commands

Command	Description
ip prefix-list	Creates an entry in a prefix list.
match ip address	Distributes any routes that have a destination network number address permitted by a standard or extended access list, or performs policy routing on packets.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
set ip address prefix-list	Sets a route to criteria specified in the source prefix list.
set community	Sets the BGP communities attribute.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp injected-paths	Displays injected routes or prefixes in the BGP routing table.

Command	Description
show ip prefix-list	Displays information about a prefix list or prefix list entries.

bgp listen

To associate a subnet range with a Border Gateway Protocol (BGP) peer group and activate the BGP dynamic neighbors feature, use the **bgp listen** command in router configuration mode. To disable the BGP dynamic neighbors feature, use the **no** form of this command.

bgp listen[*limit max-number* | **range** *network/length* **peer-group** *peer-group-name*]

bgp listen[*limit* | **range** *network/length* **peer-group** *peer-group-name*]

Syntax Description

limit	(Optional) Sets a maximum limit number of BGP dynamic subnet range neighbors.
<i>max-number</i>	(Optional) Number from 1 to 5000. Default is 100.
range	(Optional) Specifies a subnet range that is to be associated with a specified peer group.
<i>network / length</i>	(Optional) The IP prefix representing a subnet, and the length of the subnet mask in bits. The <i>network</i> argument can be any valid IP prefix. The <i>length</i> argument can be a number from 0 to 32.
peer-group	(Optional) Specifies a BGP peer group that is to be associated with the specified subnet range.
<i>peer-group-name</i>	(Optional) Name of a BGP peer group. This peer group is referred to as a listen range group.

Command Default

No subnets are associated with a BGP listen range group, and the BGP dynamic neighbor feature is not activated.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
15.1(2)T	This command was integrated into Cisco IOS Release 15.1(2)T.
15.0(1)S	This command was integrated into Release 15.0(1)S.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS Release 3.1S.

Release	Modification
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use the **limit** keyword and *max-number* argument to define the global maximum number of BGP dynamic neighbors that can be created.

BGP dynamic neighbors are configured using a range of IP addresses and BGP peer groups. Each range can be configured as a subnet IP address. After a subnet range is configured for a BGP peer group, and a TCP session is initiated for an IP address in the subnet range, a new BGP neighbor is dynamically created as a member of that group. The new BGP neighbor will inherit any configuration for the peer group. Only IPv4 peering is supported. The output for three **show** commands has been updated to display information about dynamic neighbors. The commands are **show ip bgp neighbors**, **show ip bgp peer-group**, and the **show ip bgp summary** command.

Examples

The following example configures a subnet range of 192.168.0.0/16 and associates this listen range with a BGP peer group. Note that the listen range peer group that is configured for the BGP dynamic neighbor feature can be activated in the IPv4 address family using the **neighbor activate** command. After the initial configuration on Router 1, when Router 2 starts a BGP router session and adds Router 1 to its BGP neighbor table, a TCP session is initiated and Router 1 creates a new BGP neighbor dynamically because the IP address of the new neighbor is within the listen range subnet.

Examples

```
enable
configure terminal
router bgp 45000
  bgp log-neighbor-changes
  neighbor group192 peer-group
  bgp listen range 192.168.0.0/16 peer-group group192
  neighbor group192 ebgp-multihop 255
  neighbor group192 remote-as 40000 alternate-as 50000
  address-family ipv4 unicast
  neighbor group192 activate
end
```

Examples

```
enable
configure terminal
router bgp 50000
  neighbor 192.168.3.1 remote-as 45000
exit
```

If the **show ip bgp summary** command is now entered on Router 1, the output shows the dynamically created BGP neighbor, 192.168.3.2.

```
Router1# show ip bgp summary
BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1
Neighbor        V    AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
*192.168.3.2    4  50000      2        2        0    0    0 00:00:37      0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(100 max), Subnet ranges: 1
BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

Related Commands

Command	Description
neighbor peer-group	Creates a BGP peer group.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
router bgp	Configures the BGP routing process.
show ip bgp summary	Displays the status of all BGP connections.

bgp log-neighbor-changes

To enable logging of BGP neighbor resets, use the **bgp log-neighbor-changes** command in router configuration mode. To disable the logging of changes in BGP neighbor adjacencies, use the **no** form of this command.

bgp log-neighbor-changes

no bgp log-neighbor-changes

Syntax Description This command has no arguments or keywords.

Command Default Logging of BGP neighbor resets is not enabled.

Command Modes Router configuration (config-router)

Command History	Release	Modification
	11.1CC	This command was introduced.
	12.0	This command was integrated into Cisco IOS release 12.0.
	12.0(7)T	Address family configuration mode support was added.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SRB	Support for IPv6 was added.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
	12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
	Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
	15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines The **bgp log-neighbor-changes** command enables logging of BGP neighbor status changes (up or down) and resets for troubleshooting network connectivity problems and measuring network stability. Unexpected neighbor resets might indicate high error rates or high packet loss in the network and should be investigated.

Using the **bgp log-neighbor-changes** command to enable status change message logging does not cause a substantial performance impact, unlike, for example, enabling per BGP update debugging. If the UNIX syslog facility is enabled, messages are sent to the UNIX host running the syslog daemon so that the messages can be stored and archived. If the UNIX syslog facility is not enabled, the status change messages are retained in

the internal buffer of the router, and are not stored to disk. You can set the size of this buffer, which is dependent upon the available RAM, using the **logging buffered** command.

The neighbor status change messages are not tracked if the **bgp log-neighbor-changes** command is not enabled, except for the reset reason, which is always available as output of the **show ip bgp neighbors** and **show bgp ipv6 neighbors** commands.

The **eigrp log-neighbor-changes** command enables logging of Enhanced Interior Gateway Routing Protocol (EIGRP) neighbor adjacencies, but messages for BGP neighbors are logged only if they are specifically enabled with the **bgp log-neighbor-changes** command.

Use the **show logging** command to display the log for the BGP neighbor changes.

Examples

The following example logs neighbor changes for BGP in router configuration mode:

```
Device(config)# bgp router 40000
Device(config-router)# bgp log-neighbor-changes
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
eigrp log-neighbor-changes	Enables the logging of neighbor adjacency changes to monitor the stability of the routing system and to help detect problems.
logging buffered	Logs messages to an internal buffer.
show ip bgp ipv4	Displays information about the TCP and BGP connections to neighbors.
show ip bgp neighbors	Displays information about BGP neighbors.
show logging	Displays the state of logging (syslog).

bgp maxas-limit

To configure Border Gateway Protocol (BGP) to discard routes that have a number of autonomous system numbers in AS-path that exceed the specified value, use the **bgp maxas-limit** command in router configuration mode. To return the router to default operation, use the **no** form of this command.

bgp maxas-limit *number*

no bgp maxas-limit

Syntax Description

<i>number</i>	Maximum number of autonomous system numbers in the AS-path attribute of the BGP Update message, ranging from 1 to 254. In addition to setting the limit on the number of autonomous system numbers within the AS-path segment, the command limits the number of AS-path segments to ten. The behavior to allow ten AS-path segments is built into the bgp maxas-limit command. Note In some earlier Cisco IOS software releases, values up to 2000 can be configured. Cisco does not recommend that a value higher than 254 be configured. These releases also have no limit on the number of autonomous system segments in the AS-path attribute.

Command Default

No routes are discarded.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2	This command was introduced.
12.0(17)S	This command was integrated into Cisco IOS Release 12.0(17)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

The **bgp maxas-limit** command is used to limit the number of autonomous system numbers in the AS-path attribute that are permitted in inbound routes. If a route is received with an AS-path segment that exceeds the configured limit, the BGP routing process will discard the route.

Examples

This example sets a maximum number of autonomous systems numbers in the AS-path attribute to 30:

```
Router(config)# router bgp 40000  
Router(config-router-af)# bgp maxas-limit 30
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection or session.

bgp mpls-local-label

To enable Border Gateway Protocol (BGP) local label allocation for unadvertised /32 prefixes, use the **bgp mpls-local-label** command in address family configuration mode. To disable BGP local label allocation for unadvertised /32 prefixes, use the **no** form of this command.

bgp mpls-local-label

no bgp mpls-local-label

Syntax Description	This command has no arguments or keywords.

Command Default	BGP local label allocation for unadvertised /32 prefixes is not enabled.

Command Modes	Address-family configuration (config-router-af)

Command History	Release	Modification
	15.2(4)S	This command was introduced.

Usage Guidelines

The **bgp mpls-local-label** command enables BGP local label allocation for unadvertised /32 prefixes. The local label allocation is done at the time of bestpath calculation for the route. The allocation is done for /32 prefixes learned from BGP peers with which the label capability was negotiated at the time of session establishment. Subsequently, if that prefix is chosen during update generation and for transmission to a certain update-group member, a new label will not be allocated for that route. The route will be advertised with the label allocated during bestpath computation in accordance with the peer's policies.

Turning on and off this command (toggling) will cause all existing sessions configured under IPv4 Address Family Identifiers (AFIs) to be flapped and all routes will be relearned for local label allocation during bestpath computation. A warning message also will be displayed to notify you that additional labels are required for /32 prefixes.



Note	The bgp mpls-local-label command is supported only on the Cisco 7600 series router.

Examples

```
Device(config)# router bgp 100
Device(config-router)# address-family ipv4
Device(config-router-af)# bgp mpls-local-label
```

Related Commands

Command	Description
address-family ipv4	Enters address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv4 address prefixes.
router bgp	Configures the BGP routing process.

bgp nexthop

To configure Border Gateway Protocol (BGP) next-hop address tracking, use the **bgp nexthop** command in address family or router configuration mode. To disable BGP next-hop address tracking, use the **no** form of this command.

bgp nexthop {**trigger** {**delay** *seconds*| **enable**}| **route-map** *map-name*}

no bgp nexthop {**trigger** {**delay**| **enable**}| **route-map** *map-name*}

Syntax Description

trigger	Specifies the use of BGP next-hop address tracking. Use this keyword with the delay keyword to change the next-hop tracking delay. Use this keyword with the enable keyword to enable next-hop address tracking.
delay	Changes the delay interval between checks on updated next-hop routes installed in the routing table.
seconds	Number of seconds specified for the delay. Range is from 0 to 100. Default is 5.
enable	Enables BGP next-hop address tracking.
route-map	Specifies the use of a route map that is applied to the route in the routing table that is assigned as the next-hop route for BGP prefixes.
<i>map-name</i>	Name of a route map.

Command Default

BGP next-hop address tracking is enabled by default for IPv4 and VPNv4 address families. It is also enabled by default for the VPNv6 address family as of Cisco IOS Release 12.2(33)SB6.

Command Modes

Address family configuration (config-router-af) Router configuration (config-router)

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.0(31)S	The default delay interval was changed from 1 to 5 seconds.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.

Release	Modification
12.4(4)T	The route-map keyword and <i>map-name</i> argument were added to support the BGP Selective Address Tracking feature.
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.
12.2(33)SRB	The route-map keyword and <i>map-name</i> argument were added to support the BGP Selective Address Tracking 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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SB6	This command was modified. Next-hop address tracking is enabled by default for VPNv6 prefixes.
15.0(1)SY	This command was modified. Support for the route-map keyword and <i>map-name</i> argument was disabled in Cisco IOS Release 15.0(1)SY.

Usage Guidelines

BGP next-hop address tracking is event driven. BGP prefixes are automatically tracked as peering sessions are established. Next-hop changes are rapidly reported to BGP as they are updated in the routing information base (RIB). This optimization improves overall BGP convergence by reducing the response time to next-hop changes for routes installed in the RIB. When a best-path calculation is run in between BGP scanner cycles, only the changes are processed and tracked.



Note

BGP next-hop address tracking improves BGP response time significantly. However, unstable Interior Gateway Protocol (IGP) peers can introduce instability to BGP. We recommend that you aggressively dampen unstable IGP peering sessions to mitigate the possible impact to BGP.



Note

BGP next-hop address tracking is not supported under the IPv6 address family.

Use the **trigger** keyword with the **delay** keyword and *seconds* argument to change the delay interval between routing table walks for BGP next-hop address tracking. You can increase the performance of BGP next-hop address tracking by tuning the delay interval between full routing table walks to match the tuning parameters for the IGP. The default delay interval is 5 seconds, which is an optimal value for a fast-tuned IGP. In the case of an IGP that converges more slowly, you can change the delay interval to 20 seconds or more, depending on the IGP convergence time.

Use the **trigger** keyword with the **enable** keyword to enable BGP next-hop address tracking. BGP next-hop address tracking is enabled by default.

Use the **route-map** keyword and *map-name* argument to allow a route map to be used. The route map is used during the BGP best-path calculation and is applied to the route in the routing table that covers the Next_Hop attribute for BGP prefixes. If the next-hop route fails the route-map evaluation, the next-hop route is marked as unreachable. This command is per address family, so different route maps can be applied for next-hop routes in different address families.

**Note**

The **route-map** keyword and *map-name* argument are not supported in Cisco IOS Release 15.0(1)SY.

**Note**

Only the **match ip address** and **match source-protocol** commands are supported in the route map. No **set** commands or other **match** commands are supported.

Examples

The following example shows how to change the delay interval between routing table walks for BGP next-hop address tracking to occur every 20 seconds under an IPv4 address family session:

```
router bgp 50000
 address-family ipv4 unicast
  bgp nexthop trigger delay 20
end
```

The following example shows how to disable next-hop address tracking for the IPv4 address family:

```
router bgp 50000
 address-family ipv4 unicast
  no bgp nexthop trigger enable
end
```

The following example shows how to configure a route map that permits a route to be considered as a next-hop route only if the address mask length is more than 25. This configuration will avoid any prefix aggregates being considered as a next-hop route.

```
router bgp 45000
 address-family ipv4 unicast
  bgp nexthop route-map CHECK-NEXTHOP
 exit-address-family
 exit
ip prefix-list FILTER25 seq 5 permit 0.0.0.0/0 ge 25
route-map CHECK-NEXTHOP permit 10
 match ip address prefix-list FILTER25
end
```

Related Commands

Command	Description
match ip address	Matches IP addresses defined by a prefix list.
match source-protocol	Matches the route type based on the source protocol.

bgp nexthop trigger delay

The **trigger** and **delay** keywords for the **bgp nexthop** command are no longer documented as a separate command.

The information for using the **trigger** and **delay** keywords for the **bgp nexthop** command has been incorporated into the **bgp nexthop** command documentation. See the **bgp nexthop** command documentation for more information.

bgp nexthop trigger enable

The **trigger** and **enable** keywords for the **bgp nexthop** command are no longer documented as a separate command.

The information for using the **trigger** and **enable** keywords for the **bgp nexthop** command has been incorporated into the **bgp nexthop** command documentation. See the **bgp nexthop** command documentation for more information.

bgp nopeerup-delay

To configure the time duration that Border Gateway Protocol (BGP) waits for the first peer to come up before populating the routing information base (RIB), use the **bgp nopeerup-delay** command in router configuration mode. To remove the configured values, use the **no** form of this command.

bgp nopeerup-delay {cold-boot| nsf-switchover| post-boot| user-initiated} *seconds*

no bgp nopeerup-delay {cold-boot| nsf-switchover| post-boot| user-initiated} *seconds*

Syntax Description

cold-boot	Specifies the delay time for the first peer to come up after a cold boot.
nsf-switchover	Specifies the delay time for the first peer to come up post Non-Stop Forwarding (NSF) switchover.
post-boot	Specifies the delay time for the first peer to come up once the system is booted and all peers go down.
user-initiated	Specifies the delay time for the first peer to come up after a manual clear of BGP peers by the administrative user.
<i>seconds</i>	Delay in seconds. Valid values are from 1 to 3600.

Command Default

Delay time is not configured.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

In a Virtual Switching System (VSS), Open Shortest Path First (OSPF) NSF Engineering Task Force (IETF) operations and BGP are configured and peers are propagated through OSPF. In such a VSS, the OSPF restart interval should be shorter than the time BGP waits for the first peer to come up before populating the RIB; otherwise traffic will be dropped. To make the OSPF restart interval shorter than the time BGP waits for the first peer to come up, use the **nsf ietf restart-interval** command. To change the time duration that BGP waits for the first peer to come up, and make it longer than the OSPF restart interval, use the **bgp nopeerup-delay** command.

Examples

The following example shows how to configure the delay time to 234 seconds for the first peer to come up after NSF switchover.

```
Router(config)# router bgp 100  
Router(config-router)# bgp nopeerup-delay nsf-switchover 234
```

Related Commands

Command	Description
clear ip bgp peer-group	Resets the BGP connections using hard or soft reconfiguration for all the members of a BGP peer group.
nsf ietf restart-interval	Enables IETF NSF operations on a router that is running OSPF.
router bgp	Configures the BGP routing process.

bgp recursion host

To enable the recursive-via-host flag for IP Version 4 (IPv4), VPN Version 4 (VPNv4), virtual routing and forwarding (VRF) address families, and IPv6 address families, use the **bgp recursion host** command in address family configuration or router configuration mode. To disable the recursive-via-host flag, use the **no** form of this command.

bgp recursion host

no bgp recursion host

Syntax Description

This command has no arguments or keywords.

Command Default

For an internal Border Gateway Protocol (iBGP) IPv4 address family, irrespective of whether Prefix Independent Convergence (PIC) is enabled, the recursive-via-host flag in Cisco Express Forwarding is not set.

For the VPNv4 and IPv4 VRF address families, the recursive-via-host flag is set and the **bgp recursion host** command is automatically restored when PIC is enabled under the following conditions:

- The **bgp additional-paths install** command is enabled.
- The **bgp advertise-best-external** command is enabled.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.3S	Support for IPv6 address family configuration mode was added.
15.1(2)S	Support for IPv6 address family configuration mode was added.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

The **bgp recursion host** command is used to help Cisco Express Forwarding during traffic blackholing when a node failure occurs.

For link protection, BGP automatically restricts the recursion for the next hop resolution of connected routes. These routes are provided by the route reflector, which receives the prefix from another provider edge (PE) router that needs the customer edge (CE) router to be protected.

For node protection, BGP automatically restricts the recursion for the next hop resolution of host routes. These routes are provided by the route reflector, which receives the prefix from the host PE router. If a PE router or Autonomous System Boundary Router (ASBR) fails, for the **bgp recursion host** command to work, the PE routers must satisfy the following options:

- The host prefix must be used on the PE loopback interfaces.
- The next-hop-self must be configured on iBGP sessions.
- The **recursive via host prefix** command must be configured.

To enable Cisco Express Forwarding to use strict recursion rules for an IPv4 address family, you must configure the **bgp recursion host** command that enables the recursive-via-host flag when PIC is enabled.

The recursive-via-connected flag is set for directly connected peers only. For example, if the **bgp additional-paths install** command is configured in IPv4 and IPv4 VRF address family configuration modes, the running configuration shows the following details:

```
address-family ipv4
bgp additional-paths-install
no bgp recursion host
!
address-family ipv4 vrf red
bgp additional-paths-install
bgp recursion host
```

In the case of an external Border Gateway Protocol (eBGP) directly connected peers route exchange, the recursion is disabled for the connected routes. The recursive-via-connected flag is automatically set in the RIB and Cisco Express Forwarding for the routes from the eBGP single-hop peers.

For all the VPNs, irrespective of whether PIC is enabled, when the **bgp recursion host** command is configured in VPNv4 and IPv4 address family configuration modes, the normal recursion rules are disabled and only recursion via host-specific routes is allowed for primary, backup, and multipaths under those address families. To enable the normal recursion rules, configure the **no bgp recursion host** command in VPNv4 and IPv4 address family configuration modes.

Examples

The following example shows the configuration of the **bgp advertise-best-external** and **bgp recursion host** commands:

```
Router> enable
Router# configure terminal
Router(config)# router ospf 10
Router(config-router)# log-adjacency-changes
Router(config-router)# redistribute connected subnets
Router(config-router)# network 192.168.0.0 0.0.255.255 area 0
Router(config-router)# router bgp 64500
Router(config-router)# no synchronization
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 10.5.5.5 remote-as 64500
Router(config-router)# neighbor 10.5.5.5 update-source Loopback0
Router(config-router)# neighbor 10.6.6.6 remote-as 64500
```

```

Router(config-router)# neighbor 10.6.6.6 update-source Loopback0
Router(config-router)# no auto-summary
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 10.5.5.5 activate
Router(config-router-af)# neighbor 10.5.5.5 send-community extended
Router(config-router-af)# neighbor 10.6.6.6 activate
Router(config-router-af)# neighbor 10.6.6.6 send-community extended
Router(config-router-af)# exit-address-family
Router(config-router)# address-family ipv4 vrf test1
Router(config-router-af)# no synchronization
Router(config-router-af)# bgp advertise-best-external
Router(config-router-af)# bgp recursion host
Router(config-router-af)# neighbor 192.168.9.2 remote-as 64511
Router(config-router-af)# neighbor 192.168.9.2 fall-over bfd
Router(config-router-af)# neighbor 192.168.9.2 activate
Router(config-router-af)# neighbor 192.168.9.2 as-override
Router(config-router-af)# neighbor 192.168.9.2 route-map LOCAL_PREF in
Router(config-router-af)# exit-address-family

```

The following example shows the configuration of the **bgp additional-paths install** and **bgp recursion host** commands:

```

Router> enable
Router# configure terminal
Router(config)# router ospf 10
Router(config-router)# log-adjacency-changes
Router(config-router)# redistribute connected subnets
Router(config-router)# network 192.168.0.0 0.0.255.255 area 0
Router(config-router)# router bgp 64500
Router(config-router)# no synchronization
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 10.5.5.5 remote-as 64500
Router(config-router)# neighbor 10.5.5.5 update-source Loopback0
Router(config-router)# neighbor 10.6.6.6 remote-as 64500
Router(config-router)# neighbor 10.6.6.6 update-source Loopback0
Router(config-router)# no auto-summary
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 10.5.5.5 activate
Router(config-router-af)# neighbor 10.5.5.5 send-community extended
Router(config-router-af)# neighbor 10.6.6.6 activate
Router(config-router-af)# neighbor 10.6.6.6 send-community extended
Router(config-router-af)# exit-address-family
Router(config-router)# address-family ipv4 vrf test1
Router(config-router-af)# no synchronization
Router(config-router-af)# bgp additional-paths install
Router(config-router-af)# bgp recursion host
Router(config-router-af)# neighbor 192.168.9.2 remote-as 64511
Router(config-router-af)# neighbor 192.168.9.2 fall-over bfd
Router(config-router-af)# neighbor 192.168.9.2 activate
Router(config-router-af)# neighbor 192.168.9.2 as-override
Router(config-router-af)# neighbor 192.168.9.2 route-map LOCAL_PREF in
Router(config-router-af)# exit-address-family

```

The following example shows the best external routes and the BGP recursion flags enabled:

```

Router# show ip bgp vpnv4 vrf test1 192.168.13.1

BGP routing table entry for 400:1:192.168.13.0/24, version 4
Paths: (2 available, best #2, table test1)
  Advertise-best-external
    Advertised to update-groups:
      1
  64511, imported path from 300:1:192.168.13.0/24
    10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 50, valid, internal, backup/repair
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.7.7.7, Cluster list: 10.5.5.5 , recursive-via-host
      mpls labels in/out 25/17
  64511
    10.8.8.8 from 10.8.8.8 (192.168.13.1)

```

```
Origin IGP, metric 0, localpref 100, valid, external, best
Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1 , recursive-via-connected
mpls labels in/out 25/nolabel
```

The following example shows the additional paths and the BGP recursion flags enabled:

```
Router# show ip bgp vpnv4 vrf test1 192.168.13.1

BGP routing table entry for 400:1:192.168.13.0/24, version 25
Paths: (2 available, best #2, table test1)
  Additional-path
  Advertised to update-groups:
    1
  64511, imported path from 300:1:192.168.13.0/24
    10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 50, valid, internal, backup/repair
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.7.7.7, Cluster list: 10.5.5.5 , recursive-via-host
      mpls labels in/out 25/17
  64511
    10.8.8.8 from 10.8.8.8 (192.168.13.1)
      Origin IGP, metric 0, localpref 100, valid, external, best
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1 , recursive-via-connected
      mpls labels in/out 25/nolabel
```

The table below describes the significant fields shown in the display.

Table 4: show ip bgp vpnv4 vrf network-address Field Descriptions

Field	Description
BGP routing table entry for ... version	Internal version number of the table. This number is incremented whenever the table changes.
Paths	Number of autonomous system paths to the specified network. If multiple paths exist, one of the multipaths is designated the best path.
Advertised to update-groups	IP address of the BGP peers to which the specified route is advertised.
10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)	Indicates the next hop address and the address of the gateway that sent the update.
Origin	Indicates the origin of the entry. It can be one of the following values: - IGP--Entry originated from Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. - incomplete--Entry originated from other than an IGP or Exterior Gateway Protocol (EGP) and was advertised with the redistribute router configuration command. - EGP--Entry originated from an EGP.
metric	The value of the interautonomous system metric.

Field	Description
localpref	Local preference value as set with the set local-preference route-map configuration command. The default value is 50.
valid	Indicates that the route is usable and has a valid set of attributes.
internal/external	The field is <i>internal</i> if the path is learned via iBGP. The field is <i>external</i> if the path is learned via eBGP.
best	If multiple paths exist, one of the multipaths is designated the best path and this path is advertised to neighbors.
Extended Community	Route Target value associated with the specified route.
Originator	The router ID of the router from which the route originated when route reflector is used.
Cluster list	The router ID of all the route reflectors that the specified route has passed through.

Related Commands

Command	Description
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
bgp advertise-best-external	Enables BGP to use an external route as the backup path after a link or node failure.
bgp additional-paths install	Enables BGP to use an additional path as the backup path.

bgp redistribute-internal

To configure iBGP redistribution into an interior gateway protocol (IGP), such as IS-IS or OSPF, use the **bgp redistribute-internal** command in address family or router configuration mode. To stop iBGP redistribution into IGPs, use the **no** form of this command.

bgp redistribute-internal

no bgp redistribute-internal

Syntax Description This command has no arguments or keywords.

Command Default In releases prior to Cisco IOS Release 15.1(2)S, 15.2(1)T, and Cisco IOS XE 3.3S, in the IPv4 VRF and IPv6 VRF address families, IBGP routes are not redistributed into IGPs.

Beginning with Cisco IOS Release 15.1(2)S, 15.2(1)T, and Cisco IOS XE 3.3S, in the IPv4 VRF and IPv6 VRF address families, IBGP routes are redistributed into IGPs.

For all other address families, IBGP routes are not redistributed into IGPs.

Command Modes Address family configuration (config-router-af)
Router configuration (config-router)

Command History	Release	Modification
	12.1	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.
	15.1(2)S	This command was modified. In the IPv4 VRF and IPv6 VRF address families, bgp redistribute-internal is the default.
	15.2(1)T	This command was modified. In the IPv4 VRF and IPv6 VRF address families, bgp redistribute-internal is the default.
	Cisco IOS XE Release 3.3S	This command was modified. In the IPv4 VRF and IPv6 VRF address families, bgp redistribute-internal is the default.

Usage Guidelines The **bgp redistribute-internal** command is used to configure iBGP redistribution into an IGP. The **clear ip bgp** command must be entered to reset BGP connections after this command is configured.

When redistributing BGP into any IGP, be sure to use IP prefix-list and route-map statements to limit the number of prefixes that are redistributed.



Caution

Caution should be exercised when redistributing iBGP into an IGP. Use IP prefix-list and route-map statements to limit the number of prefixes that are redistributed. Redistributing an unfiltered BGP routing table into an IGP can have a detrimental effect on normal IGP network operation.

Examples

In the following example, BGP to OSPF route redistribution is enabled:

```
Router(config)# router ospf 300
Router(config-router)# redistribute bgp 200
Router(config-router)# exit

Router(config)# router bgp 200
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp redistribute-internal
Router(config-router-af)# end
Router# clear ip bgp
*
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection or session.

bgp refresh max-eor-time

To cause the router to generate a Route-Refresh End-of-RIB (EOR) message if it was not able to generate one due to route flapping, use the **bgp refresh max-eor-time** command in router configuration mode. To disable the timer, use the **no** form of this command.

bgp refresh max-eor-time *seconds*

no bgp refresh max-eor-time

Syntax Description

<i>seconds</i>	Number of seconds after which, if the router was unable to generate a Route-Refresh EOR message due to route flapping, the router generates a Route-Refresh EOR message. - Valid values are from 600 to 3600, or 0. - The default is 0, meaning the command is disabled.

Command Default

0 seconds

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

The BGP Enhanced Route Refresh feature is enabled by default. The **bgp refresh max-eor-time** command is not needed under normal circumstances. You might configure the **bgp refresh max-eor-time** command in the event of continuous route flapping, when the router is unable to generate a Route-Refresh EOR message, in which case a Route-Refresh EOR is generated after the timer expires.

Examples

In the following example, if no Route-Refresh EOR message is received after 800 seconds, stale routes will be removed from the BGP table. If no Route-Refresh EOR message is generated after 800 seconds, one is generated.

```
router bgp 65000
  bgp refresh stalepath-time 800
  bgp refresh max-eor-time 800
```

Related Commands

Command	Description
bgp refresh stalepath-time	Causes the router to remove stale routes from the BGP table even if the router does not receive a Route-Refresh EOR message.

bgp refresh stalepath-time

To cause the router to remove stale routes from the BGP table even if the router does not receive a Route-Refresh EOR message, use the **bgp refresh stalepath-time** command in router configuration mode. To disable the timer, use the **no** form of this command.

bgp refresh stalepath-time *seconds*

no bgp refresh stalepath-time

Syntax Description

<i>seconds</i>	Number of seconds the router waits to receive a Route-Refresh End-of-RIB (EOR) message, and then removes the stale paths from BGP table if the router hasn't received an EOR message. • Valid values are 600 to 3600, or 0. • The default is 0, meaning the command is disabled.

Command Default

0 seconds

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

The BGP Enhanced Route Refresh feature is enabled by default. The **bgp refresh stalepath-time** command is not needed under normal circumstances. You might configure the **bgp refresh stalepath-time** command in the event of continuous route flapping, when the router does not receive a Route-Refresh EOR after an Adj-RIB-Out, in which case the router removes the stale routes from the BGP table after the timer expires. The stale path timer is started when the router receives a Route-Refresh SOR.

Examples

In the following example, if no Route-Refresh EOR message is received after 800 seconds, stale routes will be removed from the BGP table. If no Route-Refresh EOR message is generated after 800 seconds, one is generated.

```
router bgp 65000
```

bgp refresh stalepath-time

```
bgp refresh stalepath-time 800
bgp refresh max-eor-time 800
```

Related Commands

Command	Description
bgp refresh max-eor-time	Causes the router to generate a Route-Refresh EOR message if it was not able to generate one due to route churn.

bgp regexp deterministic

To configure system to use the regular expression engine that internally uses the DFA-based algorithm, use the **bgp regexp deterministic** command in router configuration mode. To configure Cisco IOS software to use the regular expression engine that internally uses the NFA-based algorithm, use the **no** form of this command.

bgp regexp deterministic

no bgp regexp deterministic

Syntax Description This command has no arguments or keywords.

Command Default The regular expression engine that internally uses the DFA-based algorithm is enabled.

Command Modes Router configuration (config-router)

Command History	Release	Modification
	12.0(26)S	This command was introduced.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
	12.2(22)S	This command was integrated into Cisco IOS Release 12.2(22)S.
	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 and 12.2(33)XNE	This command was modified. The default changed from the regular expression engine that internally uses the Nondeterministic Finite Automaton-based (NFA-based) algorithm to the regular expression engine that internally uses the Deterministic Finite Automaton-based (DFA-based) algorithm.

Usage Guidelines This command controls a choice between the use of two different algorithms to evaluate regular expressions.

- The regular expression engine that internally uses the NFA-based algorithm uses a recursive algorithm. This engine is effective, but uses more system resources as the complexity of regular expressions increases. The recursive algorithm works well for simple regular expressions, but is less efficient when processing very complex regular expressions because of the backtracking that is required to process partial matches. In some cases, CPU watchdog timeouts and stack overflow traces have occurred because of the length of time that this engine requires to process very complex regular expressions.

- The regular expression engine that internally uses the DFA-based algorithm is the default engine used. This engine employs an improved algorithm that eliminates excessive backtracking and greatly improves performance when processing complex regular expressions. When this engine is enabled, complex regular expressions are evaluated more quickly, and CPU watchdog timeouts and stack overflow traces will not occur. However, this engine takes longer to process simple regular expressions than the regular expression engine that internally uses the NFA-based algorithm.

Recommendations

- We recommend that you use the regular expression engine that internally uses the DFA-based algorithm if you need to evaluate complex regular expressions or if you have observed problems related to evaluating regular expressions. This engine is enabled by default or re-enabled by entering the **bgp regexp deterministic** command under a Border Gateway Protocol (BGP) routing process.
- We recommend that you use the regular expression engine that internally uses the NFA-based algorithm if you use only simple regular expressions. This engine can be enabled by entering the **no bgp regexp deterministic** command.



Note

Only the negative version of the command (**no bgp regexp deterministic**) will appear in a configuration file (nvgened), if configured.

Examples

The following example shows how to configure the software to use the regular expression engine that internally uses the DFA-based algorithm, which is also the default behavior:

```
Router(config)# router bgp 50000
Router(config-router)# bgp regexp deterministic
```

The following examples shows how to configure the software to use the regular expression engine that internally uses the NFA-based algorithm:

```
Router(config)# router bgp 50000
Router(config-router)# no bgp regexp deterministic
```

Related Commands

Command	Description
router bgp	Configures the BGP routing process.
show ip bgp regexp	Displays routes matching the autonomous system path regular expression.

bgp route-map priority

To configure the route map priority for a local Border Gateway Protocol (BGP) routing process, use the **bgp route-map priority** command in address family configuration mode. To remove the route map priority for a local BGP routing process, use the **no** form of this command.

bgp route-map priority

no bgp route-map priority

Command Default Route map priority is not configured for a local BGP process.

Command Modes Address family configuration (config-router-af)

Command History	Release	Modification
	12.2(33)SRE	This command was introduced.

Usage Guidelines The **bgp route-map priority** command is used to configure the route map priority for the local Border Gateway Protocol (BGP) routing process. The specified route map will take priority over the bgp next-hop unchanged and bgp next-hop unchanged allpaths settings.

Examples The following example shows how to configure the local router with route map priority:

```
router bgp 50000
address-family ipv4 unicast vrf inside
  bgp route-map priority
```

Related Commands	Command	Description
	set ip next-hop self	Configures local routes with next hop of self (for BGP only).

bgp router-id

To configure a fixed router ID for the local Border Gateway Protocol (BGP) routing process, use the **bgp router-id** command in router or address family configuration mode. To remove the fixed router ID from the running configuration file and restore the default router ID selection, use the **no** form of this command.

Router Configuration

bgp router-id {*ip-address*| **vrf auto-assign**}

no bgp router-id [**vrf auto-assign**]

Address Family Configuration

bgp router-id {*ip-address*| **auto-assign**}

no bgp router-id

Syntax Description

<i>ip-address</i>	Router identifier in the form of an IP address.
vrf	Configures a router identifier for a Virtual Routing and Forwarding (VRF) instance.
auto-assign	Automatically assigns a router identifier for each VRF.

Command Default

The following behavior determines local router ID selection when this command is not enabled:

- If a loopback interface is configured, the router ID is set to the IP address of the loopback interface. If multiple loopback interfaces are configured, the router ID is set to the IP address of the loopback interface with the highest IP address.
- If no loopback interface is configured, the router ID is set to the highest IP address on a physical interface.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	The vrf and auto-assign keywords were added, and this command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command, including the vrf and auto-assign keywords, was integrated into Cisco IOS Release 12.2(31)SB2.

Release	Modification
12.2(33)SXH	This command, including the vrf and auto-assign keywords, was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	The vrf and auto-assign keywords were added.

Usage Guidelines

The **bgp router-id** command is used to configure a fixed router ID for the local BGP routing process. The router ID is entered in IP address format. Any valid IP address can be used, even an address that is not locally configured on the router. If you use an IP address from a local interface, we recommend that you use the address of a loopback interface rather than the address of a physical interface. (A loopback interface is more effective than a fixed interface as an identifier because there is no physical link to go down.) Peering sessions are automatically reset when the router ID is changed.

In Cisco IOS Release 12.2(33)SRA, 12.2(31)SB2, 12.2(33)SXH, 12.4(20)T, and later releases, the Per-VRF Assignment of BGP Router ID feature introduced VRF-to-VRF peering in BGP on the same router. BGP is designed to refuse a session with itself because of the router ID check. The per-VRF assignment feature allows a separate router ID per VRF. The router ID can be manually configured for each VRF or automatically assigned either for each VRF or globally under address family configuration mode.

Examples

The following example shows how to configure the local router with a fixed BGP router ID of 192.168.254.254:

```
router bgp 50000
  bgp router-id 192.168.254.254
```

The following example shows how to configure a BGP router ID for the VRF named VRF1. This configuration is done under address family IPv4 VRF configuration mode.

```
router bgp 45000
  address-family ipv4 vrf VRF1
    bgp router-id 10.1.1.99
```

The following example shows how to configure an automatically assigned VRF BGP router ID for all VRFs. This configuration is done under BGP router configuration mode.

```
router bgp 45000
  bgp router-id vrf auto-assign
```

The following example shows how to configure an automatically assigned VRF BGP router ID for a single VRF. This configuration is done under address family IPv4 VRF configuration mode.

```
router bgp 45000
  address-family ipv4 vrf VRF2
    bgp router-id auto-assign
```

Related Commands

Command	Description
show ip bgp	Displays entries in the BGP routing table.
show ip bgp vpnv4	Displays VPNv4 address information from the BGP routing table.

bgp rpki server

To connect to a Resource Public Key Infrastructure (RPKI) server and enable the validation of Border Gateway Protocol (BGP) prefixes based on the autonomous system (AS) from which the prefix originates, use the **bgp rpki server** command in router configuration mode. To stop the connection to the RPKI server and stop the validation of BGP prefixes based on the origin AS, use the **no** form of this command.

bgp rpki server tcp {*ipv4-address* | *ipv6-address*} **port** *port-number* **refresh** *seconds*

no bgp rpki server tcp {*ipv4-address* | *ipv6-address*} **port** *port-number* **refresh** *seconds*

Syntax Description

tcp	Specifies the protocol used by the router to communicate with the RPKI server.
<i>ipv4-address</i>	IPv4 address of the RPKI server.
<i>ipv6-address</i>	IPv6 address of the RPKI server.
port <i>port-number</i>	Specifies the 16-bit port number of the RPKI server, in the range from 1 to 65535.
refresh <i>seconds</i>	Specifies the refresh interval (in seconds) at which the system will download SOVC records from the RPKI server. The range is from 1 to 65535.

Command Default

The router is not connected to an RPKI server.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
XE 3.5S	This command was introduced.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.
15.2(4)S	This command was implemented on the Cisco 7200 series routers.

Usage Guidelines

Use this command to enable the BGP—Origin AS Validation feature. A separate, external RPKI server must be configured, and its address and port number known. The actual authentication of public key certificates is done on the RPKI server.

If more than one RPKI server is configured, the router will connect to all configured servers and download prefix information from all of them.

After configuration or upon bootup, the router will open a TCP connection to the RPKI server at the specified address and port number. If the connection attempt fails, the router will retry the connection once per minute.

Examples

The following example configures BGP to connect to the RPKI server at 192.168.1.1 and download a list of prefixes and permitted origin AS numbers. Once every 600 seconds the router will query the server to obtain any new prefixes that the server might send.

```
Router(config)# router bgp 65000
Router(config-router)# bgp rpki server tcp 192.168.1.1 port 1033 refresh 600
```

Related Commands

Command	Description
bgp bestpath prefix-validate	Determines whether invalid prefixed are allowed to be used as the best path, even if valid prefixes are available, or disables the checking of prefixes.
clear ip bgp rpki server	Purges SOVC records downloaded from the specified server, and optionally closes the TCP connection to the indicated cache server.
debug ip bgp event rpki	Provides details about RPKI events.
neighbor announce rpki state	Sends and receives the RPKI state and prefix/AS pairs to and from an IBGP neighbor.
show ip bgp ipv4	Displays entries in the BGP IPv4 routing table.
show ip bgp ipv6 unicast	Displays entries in the BGP IPv6 unicast routing table.
show ip bgp rpki servers	Displays the current state of communication with the RPKI servers.
show ip bgp rpki table	Displays the current cached list of prefix/AS pairs.
show ip bgp summary	Displays information about how many prefix/AS pairs are in each RPKI state.

bgp rr-group

To create a route-reflector group and enable automatic inbound filtering for VPN version 4 (VPNv4) updates based on the allowed route target (RT) extended communities, use the **bgp rr-group** command in address family configuration mode. To disable a route-reflector group, use the **no** form of this command.

bgp rr-group *extcom-list-number*

no bgp rr-group *extcom-list-number*

Syntax Description

<i>extcom-list-number</i>	Extended community-list that defines the route targets that will be permitted by the route-reflector group. The range of t numbers that can be entered is from 1 to 500. Only one extended community-list is specified for each route-reflector group.

Command Default

No default behavior or values

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
12.1	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(22)S	The maximum number of extended community-lists that can supported by a route-reflector group was changed from 199 to 500 in Cisco IOS Release 12.0(22)S.
12.2(15)T	The maximum number of extended community-lists that can supported by a route-reflector group was changed from 199 to 500 in Cisco IOS Release 12.2(15)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

The **bgp rr-group** command is used to partition large VPNv4 Border Gateway Protocol (BGP) networks into smaller route-reflector groups. Each route-reflector group permits only routes from route targets defined in

an extended community list. Only one extended community list can be configured for each route-reflector group.

Examples

In the following example, a route-reflector group is created. The route target is associated with the VRF and then defined in an extended community list. This route reflector will accept routes from only route target 50000:1024.

```
Router(config)# ip vrf RED
Router(config-vrf)# rd 50000:10000
Router(config-vrf)# route-target both 50000:10000
Router(config-vrf)# route-target export 50000:1024
Router(config-vrf)# exit
Router(config)# ip extcommunity-list 1 permit rt 50000:1024
Router(config)# router bgp 50000
Router(config-router)# address family vpnv4

Router(config-router-af)# bgp rr-group 1
Router(config-router-af)# neighbor 192.168.0.1 activate

Router(config-router-af)# neighbor 192.168.0.1 route-reflector-client
Router(config-router-af)# neighbor 192.168.0.1 send-community extended
Router(config-router-af)# end
```

Related Commands

Command	Description
ip extcommunity-list	Creates an extended community access list.

bgp scan-time

To configure scanning intervals of Border Gateway Protocol (BGP) routers for next hop validation or to decrease import processing time of Virtual Private Network version 4 (VPNv4) routing information, use the **bgp scan-time** command in address family or router configuration mode. To return the scanning interval of a router to its default scanning interval of 60 seconds, use the **no** form of this command.

bgp scan-time [**import**] *scanner-interval*

no bgp scan-time [**import**] *scanner-interval*

Syntax Description

import	(Optional) Configures import processing of VPNv4 unicast routing information from BGP routers into routing tables.
<i>scanner-interval</i>	The scanning interval in seconds of BGP routing information. Valid values are from 5 to 60. The default is 60.

Command Default

The default scanning interval is 60 seconds.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

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.
15.0(1)M	This command was modified. The import keyword was removed. It is not available in Cisco IOS Release 15.0(1)M and later Cisco IOS Release 15.0M releases.
12.2(33)SRE	This command was modified. The import keyword was removed. It is not available in Cisco IOS Release 12.2(33)SRE and later Cisco IOS Release 12.2SR releases.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Release	Modification
15.1(2)T	This command was modified. The minimum scan time was increased from 5 seconds to 15 seconds.
15.0(1)S	This command was modified. The minimum scan time was increased from 5 seconds to 15 seconds.
Cisco IOS XE 3.1S	This command was modified. The minimum scan time was increased from 5 seconds to 15 seconds.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
Cisco IOS XE 3.4.1S	This command was modified. The minimum scan time was decreased from 15 seconds to 5 seconds. The command can be configured even if NHT is enabled.
15.1(3)S1	This command was modified. The minimum scan time was decreased from 15 seconds to 5 seconds. The command can be configured even if NHT is enabled.

Usage Guidelines

Entering the **no** form of this command does not disable scanning, but removes it from the output of the **show running-config** command.

The **import** keyword is supported in address family VPNv4 unicast mode only.

The BGP Event Based VPN Import feature introduced a modification to the existing BGP path import process using new commands and the **import** keyword was removed from the **bgp scan-time** command in Cisco IOS Release 15.0(1)M, 12.2(33)SRE, and later releases.

While **bgp nexthop** address tracking (NHT) is enabled for an address family, the **bgp scan-time** command will not be accepted in that address family and will remain at the default value of 60 seconds. NHT must be disabled before the **bgp scan-time** command will be accepted in either router mode or address family mode. However, for Cisco IOS Release 15.1(3)S1 and Cisco IOS XE Release 3.4.1S, the **bgp scan-time** command can be configured even if NHT is enabled.

Examples

In the following router configuration example, the scanning interval for next hop validation of IPv4 unicast routes for BGP routing tables is set to 20 seconds:

```
router bgp 100
 no synchronization
 bgp scan-time 20
```

In the following address family configuration example, the scanning interval for next hop validation of address family VPNv4 unicast routes for BGP routing tables is set to 45 seconds:

```
router bgp 150
 address-family vpnv4 unicast
  bgp scan-time 45
```

In the following address family configuration example, the scanning interval for importing address family VPNv4 routes into IP routing tables is set to 30 seconds:

```
router bgp 150
 address-family vpnv4 unicast
  bgp scan-time import 30
```

Related Commands

Command	Description
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
bgp nexthop	Configures BGP next-hop address tracking.

bgp slow-peer detection

To specify a threshold time that dynamically determines a slow peer, use the **bgp slow-peer detection** command in address-family configuration mode. To restore the default value, use the **no** form of this command.

bgp slow-peer detection [*threshold seconds*]

no bgp slow-peer detection

Syntax Description

<i>seconds</i>	(Optional) Threshold time in seconds that the timestamp of the oldest message in a peers queue can be lagging behind the current time before the peer is determined to be a slow peer. The range is from 120 to 3600; the default is 300.

Command Default

300 seconds

Command Modes

Address-family configuration (config-router-af)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines

Update messages are timestamped when they are formatted. The timestamp of the oldest update message in a peers queue is compared to the current time to determine if the peer is lagging more than the configured number of seconds. When a peer is dynamically detected to be a slow peer, the system will send a syslog message. The peer will be marked as recovered and another syslog message will be generated only after the peer's update group converges.



Note

If you want detection for only some peers, use the **neighbor slow-peer detection** command. The **neighbor slow-peer detection** command overrides the **bgp slow-peer detection** command. If the **neighbor slow-peer detection** command is unconfigured or if **no neighbor slow-peer detection** is configured, the system will inherit the global, address-family level configuration.

**Note**

The **slow-peer detection** command performs the same function as the **bgp slow-peer detection** command, except through a peer policy template.

Examples

The following example specifies that if the timestamp on a peer's update message is more than 360 seconds before the current time, the peer that sent the update message is marked as a slow peer.

```
Router(config-router-af) # bgp slow-peer detection threshold 360
```

Related Commands

Command	Description
bgp slow-peer split-update-group dynamic	Moves a dynamically detected slow peer to a slow update group.
clear ip bgp slow	Moves dynamically configured slow peers back to their original update groups.

bgp slow-peer split-update-group dynamic

To move a dynamically detected slow peer to a slow update group, use the **bgp slow-peer split-update-group dynamic** command in address-family configuration mode. To cancel this method of moving dynamically detected slow peers to a slow update group, use the **no** form of this command.

bgp slow-peer split-update-group dynamic [permanent]

no bgp slow-peer split-update-group dynamic

Syntax Description

permanent	(Optional) Specifies that after the slow peer becomes a regular peer (converges), it is not moved back to its original update group automatically. After resolving the root cause of the slow peer, (network congestion, and so forth), the network administrator can use one of the clear commands to move the peer to its original update group.

Command Default

No dynamically detected slow peer is moved to a slow peer update group.

Command Modes

Address-family configuration (config-router-af)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines

When a peer is dynamically detected to be a slow peer (based on the threshold of the **bgp slow-peer detection** command), the slow peer is moved to a slow update group. If a *static* slow peer update group exists, (based on the **neighbor slow-peer split-update-group static** command, the dynamic slow peer is moved to the static slow peer update group; otherwise, a new slow peer update group is created and the peer is moved to that group. Furthermore:

- If the **permanent** keyword is configured, the peer is not automatically moved to its original update group. This is the recommended option. You can the **clear ip bgp slow** command to move the peer back to its original update group.
- If the **permanent** keyword is not configured, the slow peer will be moved back to its regular original update group after it becomes a regular peer (converges).

**Note**

The **neighbor slow-peer split-update-group dynamic** command performs the same function as the **bgp slow-peer split-update-group dynamic** command (at the address-family level), except that the **neighbor slow-peer split-update-group dynamic** command overrides the address-family level command. When the **neighbor slow-peer split-update-group dynamic** command is unconfigured, the system will function according to the address-family level configuration. The **slow-peer split-update-group dynamic** command performs the same function through a peer policy template.

If **bgp slow-peer split-update-group dynamic** is configured, but no slow peer detection is configured, the detection will be done at the default threshold of 300 seconds.

Examples

In the following example, the timestamp of the oldest message in a peers queue is compared to the current time to determine if the peer is lagging more than 360 seconds. If it is lagging, the peer is marked as a slow peer and is put in the slow peer update group. Because the **permanent** keyword is not configured, the slow peer will be moved back to its regular original update group after it becomes a regular peer (converges).

```
Router(config-router-af) # bgp slow-peer detection threshold 360
Router(config-router-af) # bgp slow-peer split-update-group dynamic
```

Related Commands

Command	Description
bgp slow-peer detection	Specifies a threshold time that dynamically determines a slow peer.
clear ip bgp slow	Moves dynamically configured slow peers back to their original update groups.

bgp soft-reconfig-backup

To configure a Border Gateway Protocol (BGP) speaker to perform inbound soft reconfiguration for peers that do not support the route refresh capability, use the **bgp soft-reconfig-backup** command in address-family or router configuration mode. To disable this function, use the **no** form of this command.

bgp soft-reconfig-backup

no bgp soft-reconfig-backup

Syntax Description This command has no arguments or keywords.

Command Default Inbound soft reconfiguration for peers that do not support the route refresh capability is not performed.

Command Modes Address-family configuration (config-router-af)
Router configuration (config-router)

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

Usage Guidelines The **bgp soft-reconfig-backup** command is used to configure BGP to perform inbound soft reconfiguration for peers that do not support the route refresh capability. The configuration of this command allows you to configure BGP to store updates (soft reconfiguration) only as necessary. Peers that support the route refresh capability are unaffected by the configuration of this command.

Use the **show ip bgp neighbors** command to determine if a peer supports the route refresh capability. If supported, the following will be displayed in the output:

```
Route refresh: advertised and received(new)
```

Use the **show ip bgp** command to determine if the BGP speaker is storing inbound updates for peer that does not support the route refresh capability. If updates are stored, the following will be displayed in the output:

```
(received-only)
```

Examples The following example, starting in Global configuration mode, configures the router perform inbound soft reconfiguration only if the peer does not support the route refresh capability:

```
Router(config)# router bgp 50000
Router(config-router)# bgp soft-reconfig-backup

Router(config-router)# neighbor 10.1.1.1 remote-as 40000

Router(config-router)# neighbor 192.168.1.1 remote-as 60000
```

Related Commands

Command	Description
show ip bgp	Displays entries in the Border Gateway Protocol (BGP) routing table.
show ip bgp neighbors	Displays information about the TCP and Border Gateway Protocol (BGP) connections to neighbors.

bgp sso route-refresh-enable

To enable BGP to send route-refresh requests to nonstop routing (NSR) peers in the event of an RP failover, use the **bgp sso route-refresh-enable** command in router configuration mode. To disable the sending of route-refresh requests to NSR peers in the event of an RP failover, use the **no** form of this command.

bgp sso route-refresh-enable

no bgp sso route-refresh-enable

Syntax Description This command has no arguments or keywords.

Command Default Route-refresh requests are not sent to NSR peers in the event of a failover.

Command Modes Router configuration (config-router)

Command History	Release	Modification
	15.2(2)S	This command was introduced.
	Cisco IOS XE Release 3.6S	This command was integrated into Cisco IOS XE Release 3.6S.

Usage Guidelines By default, if an Active RP fails, the new Active RP does not send route-refresh requests to NSR peers because it creates unnecessary churn during switchover from the Standby RP to the Active RP. Use the **bgp sso route-refresh-enable** command only if, for some reason, you want the new Active RP to send route-refresh requests to NSR peers upon failover.

Examples The following example shows how to configure BGP to send route-refresh requests to NSR peers in the event of a failover:

```
Router(config-router)# bgp sso route-refresh-enable
```

Related Commands	Command	Description
	show ip bgp vpnv4 all neighbor	Displays information about BGP peers.
	show ip bgp vpnv4 all sso summary	Displays the number of BGP peers that support BGP NSR with stateful switchover.

bgp suppress-inactive

To suppress the advertisement of routes that are not installed in the routing information base (RIB), use the **bgp suppress-inactive** command in address family or router configuration mode.

bgp suppress-inactive

no bgp suppress inactive

Syntax Description This command has no arguments or keywords.

Command Default No routes are suppressed.

Command Modes Address family configuration (config-router-af)
Router configuration (config-router)

Command History	Release	Modification
	12.2(11)T	This command was introduced.
	12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
	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.
	15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
	15.1S	This command was modified. Support for IPv6 and VRFv6 address families was added.

Usage Guidelines The **bgp suppress-inactive** command is used to prevent routes that are not installed in the RIB (inactive routes) from being advertised to peers. If this feature is not enabled or if the **no** form of this command is used, Border Gateway Protocol (BGP) will advertise inactive routes.

**Note**

BGP marks routes that are not installed into the RIB with a RIB-failure flag. This flag will also appear in the output of the **show ip bgp** command; for example, Rib-Failure (17). This flag does not indicate an error or problem with the route or the RIB, and the route may still be advertised depending on the configuration of this command. Enter the **show ip bgp rib-failure** command to see more information about the inactive route.

Examples

In the following example, the BGP routing process is configured for IPv4 address family to not advertise routes that are not installed in the RIB:

```
Router(config)# router bgp 500000
Router(config-router)# address-family ipv4
Router(config-router)# bgp suppress-inactive
```

In the following example, the BGP routing process is configured for IPv6 address family to not advertise routes that are not installed in the RIB:

```
Router(config)# router bgp 500000
Router(config-router)# address-family ipv6
Router(config-router)# bgp suppress-inactive
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection using BGP soft reconfiguration.
show ip bgp rib-failure	Display BGP routes were not installed in the RIB.

bgp transport

To enable TCP transport session parameters globally for all Border Gateway Protocol (BGP) sessions, use the **bgp transport** command in router configuration mode. To disable TCP transport session parameters globally for all BGP sessions, use the **no** form of this command.

bgp transport path-mtu-discovery

no bgp transport path-mtu-discovery

Syntax Description

path-mtu-discovery	Enables transport path maximum transmission unit (MTU) discovery.

Command Default

TCP path MTU discovery is enabled by default for all BGP sessions.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(33)SRA	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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command is enabled by default because it is used to allow BGP sessions to take advantage of larger MTU links, which can be very important for internal BGP (iBGP) sessions. Use the **show ip bgp neighbors** command to ensure that TCP path MTU discovery is enabled.

Examples

The following example shows how to disable TCP path MTU discovery for all BGP sessions:

```
router bgp 45000
 no bgp transport path-mtu-discovery
```

The following example shows how to enable TCP path MTU discovery for all BGP sessions:

```
router bgp 45000
 bgp transport path-mtu-discovery
```

Related Commands

Command	Description
neighbor transport	Enables transport session parameters for a BGP neighbor session.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.

bgp update-delay

To set the maximum initial delay period before a Border Gateway Protocol (BGP)-speaking networking device sends its first updates, use the **bgp update-delay** command in router configuration mode. To remove the **bgp update-delay** command from the configuration file and restore the initial delay to its default value, use the **no** form of this command.

bgp update-delay *seconds*

no bgp update-delay

Syntax Description

<i>seconds</i>	The maximum delay, in seconds, before a BGP-speaking networking device sends its updates. The range is from 0 to 3600. The default is 120 seconds.

Command Default

If this command is not configured, the default initial delay value is 120 seconds.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2	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

When BGP is started, it waits a specified period of time for its neighbors to be established themselves and to begin sending their initial updates. Once that period is complete, or when the time expires, the best path is calculated for each route, and the software starts sending advertisements out to its peers. This behavior improves convergence time because, if the software were to start sending advertisements out immediately, it would have to send extra advertisements if it later received a better path for the prefix from another peer.

The **bgp update-delay** command is used to tune the maximum time the software will wait after the first neighbor is established until it starts calculating best paths and sending out advertisements. This command can be used when configuring the **bgp graceful-restart** command as part of the Nonstop Forwarding (NSF) capability.

Examples

The following example sets the maximum initial delay to 240 seconds:

```
router bgp 65000
  bgp update-delay 240
```

Related Commands

Command	Description
bgp graceful-restart	Enables the BGP graceful restart capability.

bgp update-group split as-override

To keep peers that are configured with **neighbor as-override** in separate, single-member update groups, use the **bgp update-group split as-override** command in address-family configuration mode. To restore the peers back to the original state of uniting with other peers under the same VRF configured with the same policies, use the **no** form of this command.

bgp update-group split as-override

no bgp update-group split as-override

Syntax Description

This command has no arguments or keywords.

Command Default

BGP update groups are not split based on a policy of AS-override.

Command Modes

Address-family configuration mode (config-router-af)

Command History

Release	Modification
12.2(33)SRD4	This command was introduced.
15.1(4)S	Support for VPNv6 and VPNv4 multicast address family configuration modes were added.

Usage Guidelines

When the **neighbor as-override** command is specified to configure that a PE router overrides the autonomous system number (ASN) of a site with the ASN of a provider, it is standard practice to also configure Site of Origin (SoO). SoO prevents the route originated by a CE towards a PE from being sent back to the same CE by the PE.

An alternative to the SoO feature is using the **bgp update-group split as-override** command. The **bgp update-group split as-override** command causes the peers configured with the **neighbor as-override** command under the same IPv4 VRF, which were previously under one update group, to be removed (split) from that update group and each placed in their own update group (each becoming the only member in an update group).

This command is supported in the following address families:

- VPNv4 unicast
- VPNv4 multicast
- VPNv6 unicast
- VPNv6 multicast
- MVPNv4
- MVPNv6

**Note**

The **bgp update-group split as-override** command cancels the resource optimization during update generation that was achieved by having the peers under the same VRF with common outbound policies belong to the same update group.

Examples

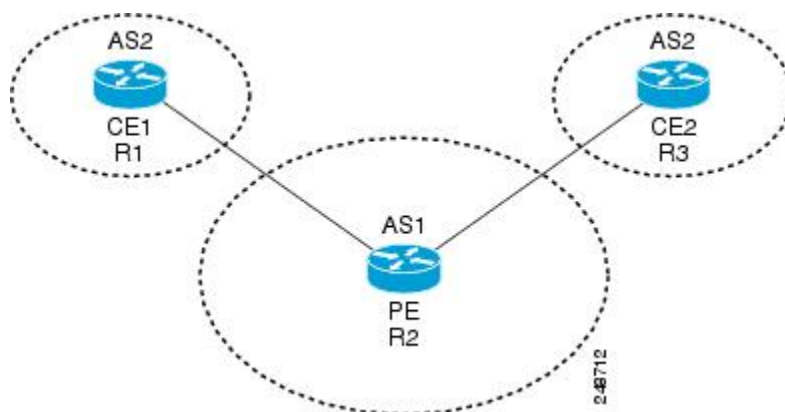
In the following example, the **neighbor as-override** command is configured on a PE for neighbors CE1 and CE2. When CE1 advertises a route to the PE, this command replaces the peer AS number (2) in the AS path with its own AS number (1) before advertising the route to its peers, in this case, CE2. Enabling the AS override feature allows routes originating from an AS to be accepted by another router (CE2) residing in the same AS. Without AS override enabled, CE2 would refuse the route advertisement once the AS path shows that the route originated from its own AS (2). This behavior occurs by default to prevent route loops. The **neighbor as-override** command overrides this default behavior.

If these PE peers, CE1 and CE2, under the **address-family ipv4 vrf name** command have the **neighbor as-override** configured on the PE, by default they are placed in the same update group. This causes the source router, CE1, to receive back its own prefix, since it's part of an update group [with CE1 and CE2] to which the prefix is advertised. This situation might result in route loops if not properly configured or if **neighbor as-override** is not accompanied by a feature such as SoO.

An alternative to SoO is to use the **bgp update-group split as-override** command. This command configured under **address-family vpnv4**, causes peers with **neighbor as-override** configured under **address-family ipv4 vrf name** to be put in separate update groups. As a result of this update-group segregation, the prefixes sent out by a router, say CE1, do not get returned to itself by the PE.

The **bgp update-group split as-override** command, although configured under address family VPNv4, splits only the peers configured under address family IPv4 VRF B and no peers configured under any other address family. The figure below illustrates the PE in AS1 and the two CEs in AS2.

Figure 5: Example of bgp update-group split as-override Scenario



The configuration for the PE (Router 2) follows:

```

Router2(config)# router bgp 1
Router2(config-router)# address-family ipv4 vrf B
Router2(config-router-af)# neighbor 192.168.11.2 as-override
Router2(config-router-af)# neighbor 192.168.14.3 as-override
Router2(config-router-af)# exit
Router2(config-router)# address-family vpnv4
  
```

```
Router2(config-router-af)# bgp update-group split as-override  
Router2(config-router-af)# exit-address-family
```

Related Commands

Command	Description
neighbor as-override	Configures a provider edge (PE) router to override the autonomous system number (ASN) of a site with the ASN of a provider.
neighbor soo	Sets the site-of-origin (SoO) value for a BGP neighbor or peer group.

bgp upgrade-cli

To upgrade a Network Layer Reachability Information (NLRI) formatted router configuration file to the address-family identifier (AFI) format and set the router command-line interface (CLI) to use only AFI commands, use the **bgp upgrade-cli** command in router configuration mode.

bgp upgrade-cli

Syntax Description This command has no keywords or arguments.

Command Default NLRI commands are not upgraded to the AFI format.

Command Modes Router configuration (config-router)

Command History	Release	Modification
	12.0(14)ST	This command was introduced.
	12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)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 The **bgp upgrade-cli** command is used to upgrade a router that is running in the NLRI formatted CLI to the AFI CLI format. The upgrade is automatic and does not require any further configuration by the network operator, and no configuration information is lost but you cannot return to the NLRI configuration because a **no** form does not exist for this command. Several NLRI-based commands do not exist under the AFI format but have equivalent commands under the AFI format. See the table below for NLRI to AFI command mapping.

Table 5: Mapping NLRI Commands with Address Family Commands

NLRI Commands	Address Family Command
distance mbgp	distance bgp
match nlri	address-family ipv4

NLRI Commands	Address Family Command
set nlri	address-family ipv4
show ip mbgp	show ip bgp ipv4 multicast
show ip mbgp summary	show ip bgp ipv4 multicast summary

Examples

In the following example, the existing NLRI router configuration file is converted to the AFI format and the router is configured to use only AFI format commands:

```
Router(config)#  
router bgp 5  
Router(config-router)#  
bgp upgrade-cli
```

bgp-policy

To enable Border Gateway Protocol (BGP) policy accounting or policy propagation on an interface, use the **bgp-policy** command in interface configuration mode. To disable BGP policy accounting or policy propagation, use the **no** form of this command.

bgp-policy {**accounting** [{**input**|**output**} [**source**]]|**destination** {**ip-prec-map**|**ip-qos-map**}|**source** {**ip-prec-map**|**ip-qos-map**}}

no bgp-policy {**accounting** [**input**|**output**]|**destination** {**ip-prec-map**|**ip-qos-map**}|**source** {**ip-prec-map**|**ip-qos-map**}}

Syntax Description

accounting	Enables accounting policy on the basis of community lists, autonomous system numbers, or autonomous system paths.
input	(Optional) Enables accounting policy on the basis of traffic that is traveling through an input interface.
output	(Optional) Enables accounting policy on the basis of traffic that is traveling through an output interface.
source	Enables accounting policy on the basis of the source address. This keyword is optional when used with the accounting keyword.
destination	Enables accounting policy on the basis of the destination address.
ip-prec-map	(Optional) Enables quality of service (QoS) policy on the basis of the IP precedence.
ip-qos-map	(Optional) Enables packet classification on the basis of the specified QoS group.

Command Default

BGP policy accounting and policy propagation are not enabled on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1CC	This command was introduced.

Release	Modification
12.0(9)S	This command was integrated into Cisco IOS Release 12.0(9)S and the accounting keyword was added.
12.0(17)ST	This command was integrated into Cisco IOS Release 12.0(17)ST.
12.0(22)S	The input , output , and source keywords were added for the Cisco 7200 series and Cisco 7500 series platforms.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(4)T	The input , output , and source keywords were integrated into Cisco IOS Release 12.3(4)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

For BGP policy propagation to function, you must enable BGP and either Cisco Express Forwarding (CEF) or distributed CEF (dCEF).

To specify the QoS policy based on the IP precedence or a QoS group, the proper route-map configuration must be in place (for example, the **set ip precedence** or **set qos-group** route-map configuration command). To display QoS policy information for the interface, use the **show ip interface** command.



Note

If you specify both the source and destination addresses when configuring policy propagation based on an access control list (ACL), the software looks up the source address in the routing table and classifies the packet based on the source address first; then the software looks up the destination address in the routing table and reclassifies the packet based on the destination address.

To specify the accounting policy, the proper route-map configuration must be in place matching specific BGP attributes using the **set traffic-index** command. In BGP router configuration mode, use the **table-map** command to modify the accounting buckets when the IP routing table is updated with routes learned from BGP. To display accounting policy information, use the **show cef interface policy-statistics**, **show ip bgp**, and **show ip cef detail EXEC** commands.

Examples

In the following example, the BGP policy propagation feature is enabled on an interface based on the source address and the IP precedence setting:

```
Router(config)# interface ethernet 4/0/0
Router(config-if)# bgp-policy source ip-prec-map
Router(config-if)# end
```

In the following example, the BGP policy accounting feature is configured using a source address on input traffic being enabled on GE-WAN interface 9/1. The policy is classified by autonomous system paths.

```
Router(config)# router bgp 50000

Router(config-router)# no synchronization
Router(config-router)# table-map buckets

Router(config-router)# exit
Router(config)# ip as-path access-list 1 permit _10_

Router(config)# ip as-path access-list 2 permit _11_

Router(config)# route-map buckets permit 10
Router(config-route-map)# match as-path 1
Router(config-route-map)# set traffic-index 1

Router(config-route-map)# exit

Router(config)# route-map buckets permit 20
Router(config-route-map)# match as-path 2

Router(config-route-map)# set traffic-index 2

Router(config-route-map)# exit

Router(config)# route-map buckets permit 80
Router(config-route-map)# set traffic-index 7
Router(config-route-map)# exit
Router(config)# interface GE-WAN9/1

Router(config-int)# ip address 10.0.2.2 255.255.255.0

Router(config-int)# bgp-policy accounting input source

Router(config-int)# no negotiation auto

Router(config-int)# end
```

Related Commands

Command	Description
set ip precedence	Sets the precedence values in the IP header.
set qos-group	Sets a QoS group ID to classify packets.
set traffic-index	Defines where to output packets that pass a match clause of a route map for BGP policy accounting.
show cef interface policy-statistics	Displays detailed CEF policy statistical information for all interfaces.
show ip bgp	Displays entries in the BGP routing table.
show ip cef	Displays entries in the FIB or FIB summary information.
show ip interface	Displays the usability status of interfaces.

Command	Description
table-map	Classifies routes according to a route map.

To configure BGP monitoring protocol (BMP) parameters for BGP neighbors and to enter the BMP server configuration mode to configure BMP servers, use the **bmp** command in router configuration mode. To disable configuration of the BMP neighbors and servers, use the **no** form of the command.

bmp {**buffer-size** *buffer-bytes* | **initial-refresh** {**delay** *refresh-delay* | **skip**} | **server** *server-number-n*}

no bmp {**buffer-size** *buffer-bytes* | **initial-refresh** {**delay** *refresh-delay* | **skip**} | **server** *server-number-n*}

Syntax Description

buffer-size <i>buffer-bytes</i>	Sets the BMP buffer size, in MB, for input-output (I/O) operations in a BGP neighbor. The value that you can set for the <i>buffer-bytes</i> argument ranges from 1 to 2048 MB.
initial-refresh	Configures the initial refresh options to handle refresh requests sent by BMP servers to BGP BMP neighbors.
delay <i>refresh-delay</i>	Sets the delay, in seconds, before initial refresh request is sent by a BMP server to a BGP BMP neighbor. The delay that you can set ranges from 1 to 3600 seconds.
skip	Configures BMP to skip any refresh requests sent by a BMP server to a BGP BMP neighbor.
server <i>server-number-n</i>	Configures BMP monitoring on a specific BGP BMP server. The value of <i>n</i> ranges from 1 to 4. You can randomly specify any server number to activate BMP monitoring on it. The server keyword also enables BMP server configuration mode.

Command Default

BMP configuration for BGP neighbors is disabled by default.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

While the **neighbor bmp-activate** command activates BMP for BGP neighbors, the **bmp** command configures parameters to establish connection between BGP BMP neighbors and BMP server. Besides configuring

parameters such as maximum buffer size, request refresh delay, and request skip; the **bmp server** command enables BMP server configuration mode, which is a sub-mode of router configuration. In BMP server configuration mode, you can configure the following parameters for a specific BMP server:

- Connection of BGP BMP neighbors to BMP servers.
- IP address of BMP servers.
- Description of the BMP servers.
- Failure retry delay in sending BMP server updates.
- Flapping delay in sending BMP server updates.
- Initial delay in sending BMP server updates.
- Setting IP Differentiated Services Code Point (DSCP) values for BMP servers.
- Statistics reporting period for BMP servers.
- Interface source of routing updates.
- Exit from BMP server configuration mode.

Examples

The following example shows how to configure initial refresh delay of 30 seconds for BGP neighbors on which BMP is activated using the **neighbor bmp-activate** command:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp initial-refresh delay 30
Device(config-router)# end
```

The following is sample output from the **show ip bgp bmp neighbors** command, which displays the refresh value of 30 seconds configured for the BGP BMP neighbors:

```
Device# show ip bgp bmp server neighbors

Number of BMP neighbors configured: 10
BMP Refresh not in progress, refresh not scheduled
Initial Refresh Delay configured, refresh value 30s
BMP buffer size configured, buffer size 2048 MB, buffer size bytes used 0 MB
```

Neighbor	PriQ	MsgQ	CfgSvr#	ActSvr#	RM Sent
30.1.1.1	0	0	1 2	1 2	16
2001:DB8::2001	0	0	1 2	1 2	15
40.1.1.1	0	0	1 2	1 2	26
2001:DB8::2002	0	0	1 2	1 2	15
50.1.1.1	0	0	1 2	1 2	16
60.1.1.1	0	0	1 2	1 2	26
2001:DB8::2002	0	0	1	1	9
70.1.1.1	0	0	2	2	12
Neighbor	PriQ	MsgQ	CfgSvr#	ActSvr#	RM Sent
80.1.1.1	0	0	1	1	10
2001:DB8::2002	0	0	1 2	1 2	16

Related Commands

Command	Description
neighbor bmp-activate	Activates BMP monitoring for BGP neighbors.

Command	Description
show ip bgp bmp	Displays information about BMP servers and neighbors.

 bmp



BGP Commands: C through I

- [clear bgp l2vpn evpn, page 180](#)
- [clear bgp nsap, page 183](#)
- [clear bgp nsap dampening, page 185](#)
- [clear bgp nsap external, page 187](#)
- [clear bgp nsap flap-statistics, page 188](#)
- [clear bgp nsap peer-group, page 190](#)
- [clear ip bgp, page 191](#)
- [clear ip bgp dampening, page 196](#)
- [clear ip bgp external, page 198](#)
- [clear ip bgp flap-statistics, page 201](#)
- [clear ip bgp in prefix-filter, page 204](#)
- [clear ip bgp ipv4, page 205](#)
- [clear ip bgp ipv6, page 210](#)
- [clear ip bgp l2vpn, page 214](#)
- [clear ip bgp mvpn, page 217](#)
- [clear ip bgp peer-group, page 219](#)
- [clear ip bgp rpki server, page 223](#)
- [clear ip bgp table-map, page 225](#)
- [clear ip bgp update-group, page 228](#)
- [clear ip bgp vpnv4, page 231](#)
- [clear ip bgp vpnv4 unicast dampening, page 235](#)
- [clear ip bgp vpnv6, page 237](#)
- [clear ip bgp vpnv6 unicast dampening, page 241](#)
- [clear ip prefix-list, page 243](#)

- [continue](#), page 245
- [debug ip bgp event rpki](#), page 251
- [debug ip bgp igp-metric ignore](#), page 253
- [debug ip bgp import](#), page 254
- [debug ip bgp route-server](#), page 257
- [default \(bmp\)](#), page 259
- [default-information originate \(BGP\)](#), page 262
- [default-metric \(BGP\)](#), page 264
- [description \(bmp\)](#), page 267
- [description \(route server context\)](#), page 269
- [distance bgp](#), page 271
- [distribute-list in \(BGP\)](#), page 273
- [distribute-list out \(BGP\)](#), page 276
- [exit-bmp-server-mode \(bmp\)](#), page 279
- [exit-peer-policy](#), page 281
- [exit-peer-session](#), page 282
- [exit-route-server-context](#), page 283
- [export map \(VRF table to global table\)](#), page 284
- [failure-retry-delay \(bmp\)](#), page 287
- [flapping-delay \(bmp\)](#), page 289
- [ha-mode graceful-restart](#), page 291
- [import ipv4](#), page 293
- [import map](#), page 296
- [import path limit](#), page 299
- [import path selection](#), page 301
- [import-map](#), page 304
- [inherit peer-policy](#), page 306
- [inherit peer-session](#), page 308
- [initial-delay \(bmp\)](#), page 310
- [ip as-path access-list](#), page 312
- [ip bgp fast-external-fallover](#), page 316
- [ip bgp-community new-format](#), page 318
- [ip community-list](#), page 320

- [ip extcommunity-list, page 326](#)
- [ip policy-list, page 333](#)
- [ip prefix-list, page 335](#)
- [ip prefix-list description, page 339](#)
- [ip prefix-list sequence-number, page 341](#)
- [ip verify unicast vrf, page 343](#)

clear bgp l2vpn evpn

To reset Border Gateway Protocol (BGP) neighbor session information for Layer 2 Virtual Private Network (L2VPN) address family Ethernet VPN, use the **clear bgp l2vpn evpn** command in privileged EXEC mode.

clear bgp l2vpn evpn {***| *as-number*| *ip-address* [*cease*| **flap-statistics**]| **external**| **internal**| **peer-group** *peer-group-name*| **update-group** [*number*| *ipv4-address*| *ipv6-address*]} [**in** [*prefix-filter*]| **out**| **slow**| **soft** [*in* [*prefix-filter*]| **out**| **slow**]]

Syntax Description

<i>*</i>	Specifies that all current BGP sessions will be reset.
<i>as-number</i>	Autonomous system number for which to clear and then reset BGP sessions for BGP neighbors. The range is from 1 to 4294967295.
<i>ip-address</i>	IP address of the BGP neighbor for which to clear the TCP connection and remove all routes learned from the connection from the BGP table.
cease	(Optional) Sends cease notification to the BGP neighbor.
flap-statistics	(Optional) Clears flap statistics for the BGP neighbor.
external	Clears all external BGP (eBGP) peers.
internal	Clears all BGP internal statistics counters.
peer-group <i>peer-group-name</i>	Clears the identified BGP peer group.
update-group	Clears the identified BGP update group.
<i>number</i>	(Optional) Update group number for which to clear update group session information.
<i>ipv4-address</i>	(Optional) IPv4 address for which to clear update group session information for the BGP peer.
<i>ipv6-address</i>	(Optional) IPv6 address for which to clear update group session information for the BGP peer.
in	(Optional) Initiates inbound reconfiguration. If neither the in keyword nor out keyword is specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.

out	(Optional) Initiates inbound or outbound reconfiguration. If neither the in keyword nor out keyword is specified, both inbound and outbound sessions are reset.
slow	(Optional) Clears slow peer status forcefully and moves it to original update group.
soft	(Optional) Initiates a soft reset. Does not tear down the session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

The **clear bgp l2vpn evpn** command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

Generating Updates from Stored Information

To generate new inbound updates from stored update information (rather than dynamically) without resetting the BGP session, you must preconfigure the local BGP router using the **neighbor soft-reconfiguration inbound** command. This preconfiguration causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy. Storing updates is memory intensive and should be avoided if possible.

Outbound BGP soft configuration has no memory overhead and does not require any preconfiguration. You can trigger an outbound reconfiguration on the other side of the BGP session to make the new inbound policy take effect.

Use this command whenever any of the following changes occur:

- Additions or changes to the BGP-related access lists
- Changes to BGP-related weights
- Changes to BGP-related distribution lists
- Changes to BGP-related route maps

Dynamic Inbound Soft Reset

The route refresh capability, as defined in RFC 2918, allows the local router to reset inbound routing tables dynamically by exchanging route refresh requests to supporting peers. The route refresh capability does not store update information locally for non-disruptive policy changes. It instead relies on dynamic exchange with supporting peers. Route refresh is advertised through BGP capability negotiation. All BGP routers must support the route refresh capability.

To determine if a BGP router supports this capability, use the **show ip bgp neighbors** command. The following message is displayed in the output when the router supports the route refresh capability:

```
Received route refresh capability from peer.
```

If all BGP routers support the route refresh capability, use the **clear ip bgp** command with the **in** keyword. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.



Note

After configuring a soft reset (inbound or outbound), it is normal for the BGP routing process to hold memory. The amount of memory that is held depends on the size of routing tables and the percentage of the memory chunks that are utilized. Partially used memory chunks will be used or released before more memory is allocated from the global router pool.

Examples

The following example configures soft reconfiguration for the inbound session with BGP L2VPN peers in the 45000 autonomous system. The outbound session is unaffected:

```
Router# clear bgp l2vpn evpn 45000 soft in
```

Related Commands

Command	Description
address-family l2vpn	Enters address family configuration mode to configure a routing session using L2VPN endpoint provisioning information.
clear ip bgp l2vpn	Resets BGP neighbor session information for L2VPN address family.
neighborsoft-reconfiguration	Configures the Cisco IOS software to start storing updates.

clear bgp nsap

To clear and then reset Connectionless Network Service (CLNS) network service access point (NSAP) Border Gateway Protocol (BGP) sessions, use the **clear bgp nsap** command in privileged EXEC mode.

clear bgp nsap [*| *as-number*| *ip-address*] [**soft**] [**in**| **out**]

Syntax Description

*	Clears and then resets all current BGP sessions.
<i>as-number</i>	Clears and then resets BGP sessions for BGP neighbors within the specified autonomous system.
<i>ip-address</i>	Clears the TCP connection to the specified BGP neighbor and removes all routes learned from the connection from the BGP table. The TCP connections are then reset.
soft	(Optional) Soft reset. Allows routing tables to be reconfigured and activated without clearing the BGP session.
in out	(Optional) Triggers inbound or outbound soft reconfiguration. If the in or out option is not specified, both inbound and outbound soft reset are triggered.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **clear bgp nsap** command is similar to the **clear ip bgp** command, except that it is NSAP address family-specific.

Use of the **clear bgp nsap** command allows a reset of the neighbor sessions with varying degrees of severity, depending on the specified keywords and arguments.

Use the *****keyword to reset all neighbor sessions. The software will clear and then reset the neighbor connections. Use this form of the command in the following situations:

- BGP timer specification change
- BGP administrative distance changes

Use the **soft out**keywords to clear and reset only the outbound neighbor connections. Inbound neighbor sessions will not be reset. Use this form of the command in the following situations:

- Additions or changes are made to the BGP-related access lists
- BGP-related weights change
- BGP-related distribution lists change
- BGP-related route maps change

Use the **in**keyword to clear only the inbound neighbor connections. Outbound neighbor sessions will not be reset. Use this form of the command in the following situations:

- BGP-related access lists change or get additions
- BGP-related weights change
- BGP-related distribution lists change
- BGP-related route maps change

Examples

In the following example, the inbound session with the neighbor 172.20.16.6 is cleared without the outbound session being reset:

```
Router# clear bgp nsap 172.20.16.6 in
```

In the following example, a soft clear is applied to outbound sessions with the neighbors in autonomous system 65000 without the inbound session being reset:

```
Router# clear bgp nsap 65000 soft out
```

Related Commands

Command	Description
show bgp nsap	Displays entries in the BGP routing table for the NSAP address family.

clear bgp nsap dampening

To clear Border Gateway Protocol (BGP) route dampening information for the network service access point (NSAP) address family and unsuppress the suppressed routes, use the **clear bgp nsap dampening** command in privileged EXEC mode.

clear bgp nsap dampening [*nsap-prefix*]

Syntax Description

<i>nsap-prefix</i>	(Optional) NSAP prefix about which to clear dampening information. This argument can be up to 20 octets long.

Command Default

When the *nsap-prefix* argument is not specified, the **clear bgp nsap dampening** command clears route dampening information for the entire BGP routing table for the NSAP address family.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **clear bgp nsap dampening** command is similar to the **clear ip bgp dampening** command, except that it is specific to the NSAP address family.

Examples

In the following example, route dampening information is cleared for the route to NSAP prefix 49.6001 and locally suppressed routes are unsuppressed:

```
Router# clear bgp nsap dampening 49.6001
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.

 **clear bgp nsap dampening**

Command	Description
show bgp nsap dampened-paths	Displays BGP dampened routes for the NSAP address family.

clear bgp nsap external

To clear all external BGP (eBGP) peers for the network service access point (NSAP) address family, use the **clear bgp nsap external** command in privileged EXEC mode.

clear bgp nsap external [**soft**] [**in**| **out**]

Syntax Description

soft	(Optional) Soft reset. Does not reset the session.
in out	(Optional) Triggers inbound or outbound soft reconfiguration. If the in or out option is not specified, both inbound and outbound soft reset are triggered.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **clear bgp nsap external** command is similar to the **clear ip bgp external** command, except that it is specific to the NSAP address family.

Examples

In the following example, the inbound sessions with external BGP peers are cleared without the outbound sessions being reset:

```
Router# clear bgp nsap external soft in
```

Related Commands

Command	Description
clear bgp nsap	Resets an NSAP BGP connection by dropping all neighbor sessions.

clear bgp nsap flap-statistics

To clear Border Gateway Protocol (BGP) flap statistics for the network service access point (NSAP) address family, use the **clear bgp nsap flap-statistics** command in privileged EXEC mode.

clear bgp nsap flap-statistics [*nsap-prefix*] [**regex** *regex*] **filter-list** *access-list-number*

Syntax Description

<i>nsap-prefix</i>	(Optional) NSAP prefix about which to clear dampening information. This argument can be up to 20 octets long.
regex <i>regex</i>	(Optional) Clears flap statistics for all the paths that match the regular expression.
filter-list <i>access-list-number</i>	(Optional) Clears flap statistics for all the paths that pass the access list. The acceptable access list number range is from 1 to 199.

Command Default

No statistics are cleared.

If no arguments or keywords are specified, the software clears flap statistics for all routes.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **clear bgp nsap flap-statistics** command is similar to the **clear ip bgp flap-statistics** command, except that it is specific to the NSAP address family.

The flap statistics for a route are also cleared when an NSAP BGP peer is reset. Although the reset withdraws the route, no penalty is applied in this instance even though route flap dampening is enabled.

Examples

In the following example, all of the flap statistics for paths that pass access list 3 are cleared:

```
Router# clear bgp nsap flap-statistics filter-list 3
```


Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
show bgp nsap flap-statistics	Displays BGP flap statistics for the NSAP address family.

clear bgp nsap peer-group

To clear the Border Gateway Protocol (BGP) TCP connections to all members of a BGP peer group for the network service access point (NSAP) address family, use the **clear bgp nsap peer-group** command in privileged EXEC mode.

clear bgp nsap peer-group *peer-group-name*

Syntax Description

<i>peer-group-name</i>	Name of the NSAP BGP peer group.

Command Default

No BGP TCP connections are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **clear bgp nsap peer-group** command is similar to the **clear ip bgp peer-group** command, except that it is specific to the NSAP address family.

Examples

In the following example, the BGP TCP connections are cleared for all members of the NSAP BGP peer group named internal:

```
Router# clear bgp nsap peer-group internal
```

Related Commands

Command	Description
neighbor peer-group (assigning members)	Configures a BGP neighbor to be a member of a peer group.

clear ip bgp

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration, use the **clear ip bgp** command in privileged EXEC mode.

clear ip bgp {***| **all**| *autonomous-system-number*| *neighbor-address*| **peer-group** *group-name*} [**in** [*prefix-filter*]| **out**| **slow**| **soft** [**in** [*prefix-filter*]| **out**| **slow**]]

Syntax Description

<i>*</i>	Specifies that all current BGP sessions will be reset.
all	(Optional) Specifies the reset of all address family sessions.
<i>autonomous-system-number</i>	Number of the autonomous system in which all BGP peer sessions will be reset. Number in the range from 1 to 65535. - In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. - In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the router bgp command.
<i>neighbor-address</i>	Specifies that only the identified BGP neighbor will be reset. The value for this argument can be an IPv4 or IPv6 address.
peer-group <i>group-name</i>	Specifies that only the identified BGP peer group will be reset.
in	(Optional) Initiates inbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.

out	(Optional) Initiates inbound or outbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.
slow	(Optional) Clears slow-peer status forcefully and moves it to original update group.
soft	(Optional) Initiates a soft reset. Does not tear down the session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(2)S	This command was integrated into Cisco IOS Release 12.0(2)S, and dynamic inbound soft reset capability was added.
12.0(7)T	The dynamic inbound soft reset capability was integrated into Cisco IOS Release 12.0(7)T.
12.0(22)S	The vpnv4 and ipv4 keywords were added.
12.0(29)S	The mdt keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.

Release	Modification
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)S	This command was modified. The slow keyword was added.
Cisco IOS XE 3.1S	This command was modified. The slow keyword was added.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

The **clear ip bgp** command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.



Note

Due to the complexity of some of the keywords available for the **clear ip bgp** command, some of the keywords are documented as separate commands. All of the complex keywords that are documented separately start with **clear ip bgp**. For example, for information on resetting BGP connections using hard or soft reconfiguration for all BGP neighbors in IPv4 address family sessions, refer to the **clear ip bgp ipv4** command.

Generating Updates from Stored Information

To generate new inbound updates from stored update information (rather than dynamically) without resetting the BGP session, you must preconfigure the local BGP router using the **neighbor soft-reconfiguration inbound** command. This preconfiguration causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy. Storing updates is memory intensive and should be avoided if possible.

Outbound BGP soft configuration has no memory overhead and does not require any preconfiguration. You can trigger an outbound reconfiguration on the other side of the BGP session to make the new inbound policy take effect.

Use this command whenever any of the following changes occur:

- Additions or changes to the BGP-related access lists
- Changes to BGP-related weights
- Changes to BGP-related distribution lists
- Changes to BGP-related route maps

Dynamic Inbound Soft Reset

The route refresh capability, as defined in RFC 2918, allows the local router to reset inbound routing tables dynamically by exchanging route refresh requests to supporting peers. The route refresh capability does not store update information locally for non-disruptive policy changes. It instead relies on dynamic exchange with supporting peers. Route refresh is advertised through BGP capability negotiation. All BGP routers must support the route refresh capability.

To determine if a BGP router supports this capability, use the **show ip bgp neighbors** command. The following message is displayed in the output when the router supports the route refresh capability:

```
Received route refresh capability from peer.
```

If all BGP routers support the route refresh capability, use the **clear ip bgp** command with the **in** keyword. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.



Note

After configuring a soft reset (inbound or outbound), it is normal for the BGP routing process to hold memory. The amount of memory that is held depends on the size of routing tables and the percentage of the memory chunks that are utilized. Partially used memory chunks will be used or released before more memory is allocated from the global router pool.

Examples

In the following example, a soft reconfiguration is initiated for the inbound session with the neighbor 10.100.0.1, and the outbound session is unaffected:

```
Router#
  clear ip bgp 10.100.0.1 soft in
```

In the following example, the route refresh capability is enabled on the BGP neighbor routers and a soft reconfiguration is initiated for the inbound session with the neighbor 172.16.10.2, and the outbound session is unaffected:

```
Router#
  clear ip bgp 172.16.10.2 in
```

In the following example, a hard reset is initiated for sessions with all routers in the autonomous system numbered 35700:

```
Router#
  clear ip bgp 35700
```

In the following example, a hard reset is initiated for sessions with all routers in the 4-byte autonomous system numbered 65538 in asplain notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or a later release.

```
Router#
  clear ip bgp 65538
```

In the following example, a hard reset is initiated for sessions with all routers in the 4-byte autonomous system numbered 1.2 in asdot notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, 12.4(24)T, and Cisco IOS XE Release 2.3, or a later release.

```
Router#
  clear ip bgp 1.2
```

Related Commands

Command	Description
bgp slow-peer split-update-group dynamic permanent	Moves a dynamically detected slow peer to a slow update group.
clear ip bgp ipv4	Resets BGP connections using hard or soft reconfiguration for IPv4 address family sessions.
clear ip bgp ipv6	Resets BGP connections using hard or soft reconfiguration for IPv6 address family sessions.
clear ip bgp vpnv4	Resets BGP connections using hard or soft reconfiguration for VPNv4 address family sessions.
clear ip bgp vpnv6	Resets BGP connections using hard or soft reconfiguration for VPNv6 address family sessions.
neighbor slow-peer split-update-group dynamic permanent	Moves a dynamically detected slow peer to a slow update group.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
router bgp	Configures the BGP routing process.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.
slow-peer split-update-group dynamic permanent	Moves a dynamically detected slow peer to a slow update group.

clear ip bgp dampening

To clear BGP route dampening information and to unsuppress suppressed routes, use the **clear ip bgp dampening** command in privileged EXEC mode.

Syntax Without Address Family Syntax

clear ip bgp [*vrf vrf-name*] **dampening** [*network-address*] [*ipv4-mask*]

Syntax With Address Family Syntax

clear ip bgp [*ipv4 {multicast| unicast}*] **dampening** [*network-address*] [*ipv4-mask*]

clear ip bgp [*vrf vrf-name*] [*vpn4 unicast*] **dampening** [*rd route-distinguisher*] [*network-address*] [*ipv4-mask*]

Syntax Description

vrf	(Optional) Specifies an instance of a routing table.
<i>vrf-name</i>	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
<i>network-address</i>	(Optional) IPv4 address of the network or neighbor to clear dampening information. If no address family keyword is specified when entering the <i>neighbor-address</i> argument, you will be prompted for an IPv4 address.
<i>ipv4-mask</i>	(Optional) IPv4 network mask.
ipv4	(Optional) Specifies the reset of IPv4 address family sessions.
multicast	(Optional) Specifies multicast address family sessions.
unicast	(Optional) Specifies unicast address family sessions.
vpn4	(Optional) Specifies the reset of Virtual Private Network Version 4 (VPNv4) address family sessions.
rd <i>route-distinguisher</i>	(Optional) Specifies the VPN route distinguisher.

Command Modes

Privileged EXEC (#)

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.
15.1(2)T	This command was modified. The vrf keyword and <i>vrf-name</i> argument were added.

Usage Guidelines

The **clear ip bgp dampening** is used to clear stored route dampening information. If no keywords or arguments are entered, route dampening information for the entire routing table is cleared.

Examples

The following example clears route dampening information for VPNv4 address family prefixes from network 192.168.10.0/24 and unsuppress suppressed routes.

```
Router#
clear ip bgp vpnv4 unicast dampening 192.168.10.0 255.255.255.0
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or configures BGP route dampening parameters.
clear ip bgp flap-statistics	Resets BGP route dampening flap-statistics.
set dampening	Sets set BGP route dampening parameters in a route map.
show ip bgp dampened-paths	Displays BGP dampened routes.

clear ip bgp external

To reset external Border Gateway Protocol (eBGP) peering sessions using hard or soft reconfiguration, use the **clear ip bgp external** command in privileged EXEC mode.

Syntax Without Address Family Syntax

```
clear ip bgp external [in [prefix-filter]] [out] [soft [in [prefix-filter]] out]]
```

Syntax With Address Family Syntax

```
clear ip bgp external [all | ipv4 {multicast | mdt | unicast} | ipv6 {multicast | unicast} | vpn4 unicast | vpn6 unicast] [in [prefix-filter]] [out] [soft [in [prefix-filter]] out]]
```

Syntax Description

in	(Optional) Initiates inbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.
out	(Optional) Initiates inbound or outbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.
soft	(Optional) Initiates a soft reset. Does not tear down the session.
all	(Optional) Specifies the reset of eBGP peering sessions for all address families.
ipv4	(Optional) Specifies the reset of eBGP peering sessions for IPv4 address family sessions.
multicast	(Optional) Specifies multicast address family sessions.
mdt	(Optional) Specifies multicast distribution tree (MDT) address family sessions.
unicast	(Optional) Specifies unicast address family sessions.
ipv6	(Optional) Specifies the reset of eBGP peering sessions for IPv6 address family sessions.
vpn4	(Optional) Specifies the reset of eBGP peering sessions for Virtual Private Network Version 4 (VPNv4) address family sessions.

vpnv6	(Optional) Specifies the reset of eBGP peering sessions for Virtual Private Network Version 6 (VPNv6) address family sessions.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(2)S	This command was introduced.
	12.0(22)S	The vpnv4 and ipv4 keywords were added.
	12.0(29)S	The mdt keyword 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.

Usage Guidelines

The **clear ip bgp external** command can be used to initiate a hard reset or soft reconfiguration of eBGP neighbor sessions. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

Generating Updates from Stored Information

To generate new inbound updates from stored update information (rather than dynamically) without resetting the BGP session, you must preconfigure the local BGP router using the **neighbor soft-reconfiguration inbound** command. This preconfiguration causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy. Storing updates is memory intensive and should be avoided if possible.

Outbound BGP soft configuration has no memory overhead and does not require any preconfiguration. You can trigger an outbound reconfiguration on the other side of the BGP session to make the new inbound policy take effect.

Use this command whenever any of the following changes occur:

- Additions or changes to the BGP-related access lists
- Changes to BGP-related weights
- Changes to BGP-related distribution lists
- Changes to BGP-related route maps

Dynamic Inbound Soft Reset

The route refresh capability, as defined in RFC 2918, allows the local router to reset inbound routing tables dynamically by exchanging route refresh requests to supporting peers. The route refresh capability does not store update information locally for non-disruptive policy changes. It instead relies on dynamic exchange with supporting peers. Route refresh is advertised through BGP capability negotiation. All BGP routers must support the route refresh capability.

To determine if a BGP router supports this capability, use the **show ip bgp neighbors** command. The following message is displayed in the output when the router supports the route refresh capability:

```
Received route refresh capability from peer.
```

If all BGP routers support the route refresh capability, use the **clear ip bgp** command with the **in** keyword. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.



Note

After configuring a soft reset (inbound or outbound), it is normal for the BGP routing process to hold memory. The amount of memory that is held depends on the size of routing tables and the percentage of the memory chunks that are utilized. Partially used memory chunks will be used or released before more memory is allocated from the global router pool.

Examples

In the following example, a soft reconfiguration is configured for all inbound eBGP peering sessions:

```
Router# clear ip bgp external soft in
```

In the following example, all outbound address family IPv4 multicast eBGP peering sessions are cleared:

```
Router# clear ip bgp external ipv4 multicast out
```

Related Commands

Command	Description
clear ip bgp	Resets BGP connections using hard or soft reconfiguration.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.

clear ip bgp flap-statistics

To clear BGP route dampening flap statistics, use the **clear ip bgp flap-statistics** command in privileged EXEC mode.

Syntax Without Address Family Syntax

clear ip bgp [*vrf vrf-name*] **flap-statistics** [*neighbor-address* [*ipv4-mask*]] **regex** *regex* | **filter-list** *extcom-number*

Syntax With Address Family Syntax

clear ip bgp [*neighbor-address*] [*vrf vrf-name*] [**all** | **ipv4** {**multicast** | **mdt** | **unicast**} | **ipv6** {**multicast** | **unicast**} | **vpn** {**vpn4 unicast** | **vpn6 unicast**}] **flap-statistics**

Syntax Description

<i>neighbor-address</i>	(Optional) Clears flap statistics for the specified IP address. If this argument is placed before flap-statistics keyword, the router clears flap statistics for all paths from the specified neighbor or network. The value for this argument can be an IPv4 or IPv6 address.
vrf	(Optional) Specifies an instance of a routing table.
<i>vrf-name</i>	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
<i>ipv4-mask</i>	(Optional) IPv4 network mask.
regex	(Optional) Clears flap statistics for all the paths that match the regular expression.
<i>regex</i>	(Optional) Regular expression.
filter-list	(Optional) Clears flap statistics for all the paths that pass the access list. The access list is specified using an extended community list number.
<i>extcom-number</i>	(Optional) Extended community list number.
all	(Optional) Clears flap statistics for all address family sessions.
ipv4	(Optional) Clears flap statistics for IPv4 address family sessions.
multicast	(Optional) Clears flap statistics for multicast address family sessions.

mdt	(Optional) Clears flap statistics for multicast distribution tree (MDT) address family sessions.
unicast	(Optional) Clears flap statistics for unicast address family sessions.
ipv6	(Optional) Clears flap statistics for IPv6 address family sessions.
vpn4	(Optional) Clears flap statistics for Virtual Private Network Version 4 (VPNv4) address family sessions.
vpn6	(Optional) Clears flap statistics for Virtual Private Network Version 6 (VPNv6) address family sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.0(22)S	The vpn4 and ipv4 keywords were added.
12.0(29)S	The mdt keyword 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.
15.1(2)T	This command was modified. The vrf keyword and <i>vrf-name</i> argument were added.

Usage Guidelines

The **clear ip bgp flap-statistics** command is used to clear the accumulated penalty for routes that are received on a router that has BGP dampening enabled. If no arguments or keywords are specified, flap statistics are cleared for all routes. Flap statistics are also cleared when the peer is stable for the half-life time period.

Examples

In the following example, all of the flap statistics are cleared for paths that pass filter list 3:

```
Router#
clear ip bgp flap-statistics filter-list 3
```

In the following example, all of the flap statistics are cleared for the paths to the BGP neighbor at 10.2.1.3:

```
Router#  
clear ip bgp 10.2.1.3 flap-statistics
```

In the following example, all of the flap statistics are cleared for the paths to the BGP neighbor at 10.2.1.3 under IPv4 multicast address family:

```
Router#  
clear ip bgp 10.2.1.3 ipv4 multicast flap-statistics
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear ip bgp dampening	Clears BGP route dampening information and to unsuppress suppressed routes.
set dampening	Sets set BGP route dampening parameters in a route map.
show ip bgp dampened-paths	Displays BGP dampened routes.

clear ip bgp in prefix-filter

The **in** and **prefix-filter** keywords for the **clear ip bgp** command are no longer documented as a separate command.

The information for using the **in** and **prefix-filter** keywords with the **clear ip bgp** command has been incorporated into all the appropriate **clear ip bgp** command documentation. Due to the complexity of some of the keywords available for the **clear ip bgp** command, some of the keywords are documented as separate commands. All of the complex keywords that are documented separately start with **clear ip bgp**. For example, for information on resetting BGP connections using hard or soft reconfiguration for all BGP neighbors in IPv4 address family sessions, refer to the **clear ip bgp ipv4** command.

clear ip bgp ipv4

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration for IPv4 address family sessions, use the **clear ip bgp ipv4** command in privileged EXEC mode.

```
clear ip bgp [vrf vrf-name] ipv4 {multicast| mdt| unicast} autonomous-system-number [in [prefix-filter]]
out| slow| soft [in [prefix-filter]] out| slow]]
```

Syntax Description

vrf	(Optional) Specifies an instance of a routing table.
vrf-name	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
multicast	Resets multicast address family sessions.
mdt	Resets multicast distribution tree (MDT) address family sessions.
unicast	Resets unicast address family sessions.
<i>autonomous-system-number</i>	Resets BGP peers with the specified autonomous system number. Number in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the router bgp command.
in	(Optional) Initiates inbound reconfiguration. If neither the in keyword nor the out keyword is specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.

out	(Optional) Initiates outbound reconfiguration. If neither the in keyword nor the out keyword is specified, both inbound and outbound sessions are reset.
slow	(Optional) Clears slow-peer status forcefully and moves it to original update group.
soft	(Optional) Initiates a soft reset. Does not tear down the session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(29)S	The mdt keyword was added.
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(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.4(20)T	This command was modified. The mdt keyword was added.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.

Release	Modification
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(2)T	This command was modified. The vrf keyword and <i>vrf-name</i> argument were added.

Usage Guidelines

The **clear ip bgp ipv4** command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

Generating Updates from Stored Information

To generate new inbound updates from stored update information (rather than dynamically generating inbound updates) without resetting the BGP session, you must preconfigure the local BGP router using the **neighbor soft-reconfiguration inbound** command. This preconfiguration causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy. Storing updates is memory intensive and should be avoided if possible.

Outbound BGP soft configuration has no memory overhead and does not require any preconfiguration. You can trigger an outbound reconfiguration on the other side of the BGP session to make the new inbound policy take effect.

Use this command whenever any of the following changes occur:

- Additions or changes to the BGP-related access lists
- Changes to BGP-related weights
- Changes to BGP-related distribution lists
- Changes to BGP-related route maps

Dynamic Inbound Soft Reset

The route refresh capability, as defined in RFC 2918, allows the local router to reset inbound routing tables dynamically by exchanging route refresh requests to supporting peers. The route refresh capability does not store update information locally for nondisruptive policy changes. It instead relies on dynamic exchange with supporting peers. Route refresh is advertised through BGP capability negotiation. All BGP routers must support the route refresh capability.

To determine if a BGP router supports this capability, use the **show ip bgp neighbors** command. The following message is displayed in the output when the router supports the route refresh capability:

```
Received route refresh capability from peer.
```

If all BGP routers support the route refresh capability, use the **clear ip bgp ipv4** command with the **in** keyword. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.

**Note**

After configuring a soft reset (inbound or outbound), it is normal for the BGP routing process to hold memory. The amount of memory that is held depends on the size of the routing tables and the percentage of the memory chunks that are utilized. Partially used memory chunks will be used or released before more memory is allocated from the global router pool.

Examples

In the following example, a soft reconfiguration is initiated for the inbound sessions for BGP neighbors in IPv4 unicast address family sessions in autonomous system 65400, and the outbound session is unaffected:

```
Router#
clear ip bgp ipv4 unicast 65400 soft in
```

In the following example, the route refresh capability is enabled on the IPv4 multicast address family BGP neighbors in autonomous system 65000, a soft reconfiguration is initiated for all inbound sessions with the IPv4 multicast address family neighbors, and the outbound session is unaffected:

```
Router#
clear ip bgp ipv4 multicast 65000 in
```

In the following example, a hard reset is initiated for all BGP neighbor in IPv4 MDT address family sessions in the autonomous system numbered 65400:

```
Router#
clear ip bgp ipv4 mdt 65400
```

In the following example, a hard reset is initiated for BGP neighbors in IPv4 unicast address family sessions in the 4-byte autonomous system numbered 65538 in asplain notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or a later release.

```
Router#
clear ip bgp ipv4 unicast 65538
```

In the following example, a hard reset is initiated for BGP neighbors in IPv4 unicast address family sessions in the 4-byte autonomous system numbered 1.2 in asdot notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, 12.4(24)T, and Cisco IOS XE Release 2.3, or a later release.

```
Router#
clear ip bgp ipv4 unicast 1.2
```

Related Commands

Command	Description
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
router bgp	Configures the BGP routing process.
show ip bgp ipv4	Displays entries in the IPv4 BGP routing table.

Command	Description
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.

clear ip bgp ipv6

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration for IPv6 address family sessions, use the **clear ip bgp ipv6** command in privileged EXEC mode.

clear ip bgp [*vrf vrf-name*] **ipv6** {**multicast**|**unicast**} *autonomous-system-number* [**in** [**prefix-filter**]] **out** **slow**| **soft** [**in** [**prefix-filter**]] **out** **slow**]]

Syntax Description

vrf	(Optional) Specifies an instance of a routing table.
<i>vrf-name</i>	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
multicast	(Optional) Specifies the reset of multicast address family sessions.
unicast	(Optional) Specifies the reset of unicast address family sessions.
<i>autonomous-system-number</i>	Specifies that sessions with BGP peers in the specified autonomous system will be reset. Number in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the router bgp command.
in	(Optional) Initiates inbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.

out	(Optional) Initiates inbound or outbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.
slow	(Optional) Clears slow-peer status forcefully and moves it to original update group.
soft	(Optional) Initiates a soft reset. Does not tear down the session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
15.1(2)T	This command was modified. The vrf keyword and <i>vrf-name</i> argument were added.

Usage Guidelines

The **clear ip bgp ipv6** command can be used to initiate a hard reset or soft reconfiguration of IPv6 address family sessions. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

Generating Updates from Stored Information

To generate new inbound updates from stored update information (rather than dynamically) without resetting the BGP session, you must preconfigure the local BGP router using the **neighbor soft-reconfiguration inbound** command. This preconfiguration causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy. Storing updates is memory intensive and should be avoided if possible.

Outbound BGP soft configuration has no memory overhead and does not require any preconfiguration. You can trigger an outbound reconfiguration on the other side of the BGP session to make the new inbound policy take effect.

Use this command whenever any of the following changes occur:

- Additions or changes to the BGP-related access lists
- Changes to BGP-related weights
- Changes to BGP-related distribution lists
- Changes to BGP-related route maps

Dynamic Inbound Soft Reset

The route refresh capability, as defined in RFC 2918, allows the local router to reset inbound routing tables dynamically by exchanging route refresh requests to supporting peers. The route refresh capability does not store update information locally for non-disruptive policy changes. It instead relies on dynamic exchange with supporting peers. Route refresh is advertised through BGP capability negotiation. All BGP routers must support the route refresh capability.

To determine if a BGP router supports this capability, use the **show ip bgp neighbors** command. The following message is displayed in the output when the router supports the route refresh capability:

```
Received route refresh capability from peer.
```

If all BGP routers support the route refresh capability, use the **clear ip bgp ipv6** command with the **in** keyword. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.

**Note**

After configuring a soft reset (inbound or outbound), it is normal for the BGP routing process to hold memory. The amount of memory that is held depends on the size of routing tables and the percentage of the memory chunks that are utilized. Partially used memory chunks will be used or released before more memory is allocated from the global router pool.

Examples

In the following example, a soft reconfiguration is initiated for the inbound sessions for BGP neighbors in IPv6 unicast address family sessions, and the outbound session is unaffected:

```
Router#
clear ip bgp ipv6 unicast soft in
```

In the following example, the route refresh capability is enabled on the IPv6 multicast address family BGP neighbors and a soft reconfiguration is initiated for all inbound session with the IPv6 multicast address family neighbors, and the outbound session is unaffected:

```
Router#
clear ip bgp ipv6 multicast in
```

In the following example, a hard reset is initiated for neighbor sessions with all IPv6 unicast address family routers in the autonomous system numbered 35400:

```
Router#
clear ip bgp ipv6 unicast 35400
```

In the following example, a hard reset is initiated for BGP neighbors in IPv6 unicast address family sessions in the 4-byte autonomous system numbered 65538 in asplain notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or a later release.

```
Router#
clear ip bgp ipv6 unicast 65538
```

In the following example, a hard reset is initiated for BGP neighbors in IPv6 unicast address family sessions in the 4-byte autonomous system numbered 1.2 in asdot notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, 12.4(24)T, and Cisco IOS XE Release 2.3, or a later release.

```
Router#
clear ip bgp ipv6 unicast 1.2
```

Related Commands

Command	Description
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
router bgp	Configures the BGP routing process.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.

clear ip bgp l2vpn

To reset Border Gateway Protocol (BGP) neighbor session information for Layer 2 Virtual Private Network (L2VPN) address family, use the **clear ip bgp l2vpn** command in privileged EXEC mode.

```
clear ip bgp [vrf vrf-name] l2vpn vpls {autonomous-system-number| peer-group peer-group-name|  
update-group [number| ip-address]} [in [prefix-filter]| out| slow| soft [in [prefix-filter]| out| slow]]
```

Syntax Description

vrf	(Optional) Specifies an instance of a routing table.
<i>vrf-name</i>	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
vpls	Specifies that Virtual Private LAN Service (VPLS) subsequent address family identifier (SAFI) information will be cleared.
<i>autonomous-system-number</i>	Autonomous system number in which peers are reset.
peer-group <i>peer-group-name</i>	Clears peer group information for the peer group specified with the <i>peer-group-name</i> argument.
update-group	Clears update group session information.
<i>number</i>	(Optional) Clears update-group session information for the specified update group number.
<i>ip-address</i>	(Optional) Clears update-group session information for the peer specified with the <i>ip-address</i> argument.
in	(Optional) Initiates inbound reconfiguration. If neither the in keyword nor out keyword is specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the inbound prefix filter.
out	(Optional) Initiates outbound reconfiguration. If neither the in keyword nor out keyword is specified, both inbound and outbound sessions are reset.
slow	(Optional) Clears slow-peer status forcefully and moves it to original update group.
soft	(Optional) Initiates a soft reset. Does not tear down the session.

Command Default If no arguments or keywords are specified, all BGP L2VPN VPLS neighbor session information is cleared.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2(33)SRB	This command was introduced.
	Cisco IOS XE Release 2.4	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
	12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
	12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
	15.1(2)T	This command was modified. The vrf keyword and <i>vrf-name</i> argument were added.

Usage Guidelines The **clear ip bgp l2vpn** command clears BGP session information for the L2VPN address family and VPLS SAFI. This command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

Generating Updates from Stored Information

To generate new inbound updates from stored update information (rather than dynamically) without resetting the BGP session, you must preconfigure the local BGP router using the **neighbor soft-reconfiguration inbound** command. This preconfiguration causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy. Storing updates is memory intensive and should be avoided if possible.

Outbound BGP soft configuration has no memory overhead and does not require any preconfiguration. You can trigger an outbound reconfiguration on the other side of the BGP session to make the new inbound policy take effect.

Use the **clear ip bgp l2vpn** command whenever any of the following changes occur:

- Additions or changes to the BGP-related access lists
- Changes to BGP-related weights
- Changes to BGP-related distribution lists
- Changes to BGP-related route maps

Dynamic Inbound Soft Reset

The route refresh capability, as defined in RFC 2918, allows the local router to reset inbound routing tables dynamically by exchanging route refresh requests to supporting peers. The route refresh capability does not store update information locally for non-disruptive policy changes. It instead relies on dynamic exchange with supporting peers. Route refresh is advertised through BGP capability negotiation. All BGP routers must support the route refresh capability.

To determine if a BGP router supports this capability, use the **show ip bgp neighbors** command. The following message is displayed in the output when the router supports the route refresh capability:

Received route refresh capability from peer.

If all BGP routers support the route refresh capability, use the **clear ip bgp l2vpn**

vpls {*autonomous-system-number* | **peer-group** *peer-group-name* | **update-group** [*number* | *ip-address*]} in command. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.



Note

After a soft reset (inbound or outbound) is configured, it is normal for the BGP routing process to hold memory. The amount of memory that is held depends on the size of the routing tables and the percentage of memory chunks that are utilized. Partially used memory chunks will be used or released before more memory is allocated from the global router memory pool.

Examples

The following example configures soft reconfiguration for the inbound session with BGP L2VPN peers in the 45000 autonomous system. The outbound session is unaffected:

```
Router#
clear ip bgp l2vpn vpls 45000 soft in
```

Related Commands

Command	Description
address-family l2vpn	Enters address family configuration mode to configure a routing session using L2VPN endpoint provisioning information.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

clear ip bgp mvpn

To clear Border Gateway Protocol (BGP) route dampening information with multicast VPN (MVPN) address family sessions and to unsuppress suppressed routes, use the **clear ip bgp mvpn** command in privileged EXEC mode.

clear ip bgp {**ipv4** | **ipv6**} **mvpn vrf** *vrf-name* {**dampening** | **flap-statistics**}

Syntax Description

ipv4	Specifies the reset of IPv4 address family sessions.
ipv6	Specifies the reset of IPv6 address family sessions.
vrf <i>vrf-name</i>	Specifies the name of the VPN routing and forwarding (VRF) instance.
dampening	Clears multicast VPN BGP dampening information.
flap-statistics	Clears multicast VPN BGP dampening flap statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

The **clear ip bgp mvpn** command is used to clear stored route dampening information for multicast VPN BGP dampening. You must specify a VRF instance using the **vrf** *vrf-name* keyword and argument prior to clearing either the dampening information (using the **dampening** keyword) or the flap statistics (using the **flap-statistics** keyword).

Examples

The following example clears route dampening information for IPv4 MVPN address family prefixes (VRF named blue) and unsuppresses suppressed routes.

```
Device# clear ip bgp ipv4 mvpn vrf blue dampening
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or configures BGP route dampening parameters.

 clear ip bgp mvpn

Command	Description
show bgp mvpn	Resets BGP route dampening flap statistics.

clear ip bgp peer-group

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration for all the members of a BGP peer group, use the **clear ip bgp peer-group** command in privileged EXEC mode.

Syntax Without Address Family Syntax

```
clear ip bgp [vrf vrf-name] peer-group peer-group-name [in [prefix-filter]] [out] [soft [in [prefix-filter]] out]]
```

Syntax With Address Family Syntax

```
clear ip bgp [vrf vrf-name] [all|ipv4 {multicast|mdt|unicast}|ipv6 {multicast|unicast}|vpnv4 unicast|vpn6 unicast] peer-group peer-group-name [in [prefix-filter]] [out] [soft [in [prefix-filter]] out]]
```

Syntax Description

vrf	(Optional) Specifies an instance of a routing table.
<i>vrf-name</i>	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
<i>peer-group-name</i>	Peer group name.
in	(Optional) Initiates inbound reconfiguration. If neither the in keyword nor the out keyword is specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.
out	(Optional) Initiates outbound reconfiguration. If neither the in keyword nor the out keyword is specified, both inbound and outbound sessions are reset.
soft	(Optional) Initiates a soft reset. Does not tear down the session.
all	(Optional) Specifies the reset of peer group members in all address families.
ipv4	(Optional) Specifies the reset of peer group members in IPv4 address family sessions.
multicast	(Optional) Specifies the reset of peer group members in multicast address family sessions.

mdt	(Optional) Specifies the reset of peer group members in multicast distribution tree (MDT) address family sessions.
unicast	(Optional) Specifies the reset of peer group members in unicast address family sessions.
ipv6	(Optional) Specifies the reset of peer group members in IPv6 address family sessions.
vpn4	(Optional) Specifies the reset of peer group members in Virtual Private Network Version 4 (VPNv4) address family sessions.
vpn6	(Optional) Specifies the reset of peer group members in Virtual Private Network Version 6 (VPNv6) address family sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.0(2)S	This command was integrated into Cisco IOS Release 12.0(2)S, and dynamic inbound soft reset capability was added.
12.0(7)T	The dynamic inbound soft reset capability was integrated into Cisco IOS Release 12.0(7)T.
12.0(22)S	The vpn4 and ipv4 keywords were added.
12.0(29)S	The mdt keyword was added.
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.
15.1(2)T	This command was modified. The vrf keyword and <i>vrf-name</i> argument were added.

Usage Guidelines

The **clear ip bgp peer-group** command is used to initiate a hard reset or soft reconfiguration for neighbor sessions for BGP peer groups. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

Generating Updates from Stored Information

To generate new inbound updates from stored update information (rather than dynamically generating inbound updates) without resetting the BGP session, you must preconfigure the local BGP router using the **neighbor soft-reconfiguration inbound** command. This preconfiguration causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy. Storing updates is memory intensive and should be avoided if possible.

Outbound BGP soft configuration has no memory overhead and does not require any preconfiguration. You can trigger an outbound reconfiguration on the other side of the BGP session to make the new inbound policy take effect.

Use this command whenever any of the following changes occur:

- Additions or changes to the BGP-related access lists
- Changes to BGP-related weights
- Changes to BGP-related distribution lists
- Changes to BGP-related route maps

Dynamic Inbound Soft Reset

The route refresh capability, as defined in RFC 2918, allows the local router to reset inbound routing tables dynamically by exchanging route refresh requests to supporting peers. The route refresh capability does not store update information locally for nondisruptive policy changes. It instead relies on dynamic exchange with supporting peers. Route refresh is advertised through BGP capability negotiation. All BGP routers must support the route refresh capability.

To determine if a BGP router supports this capability, use the **show ip bgp neighbors** command. The following message is displayed in the output when the router supports the route refresh capability:

```
Received route refresh capability from peer.
```

If all BGP routers support the route refresh capability, use the **clear ip bgp peer-group** command with the **in** keyword. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.



Note

After configuring a soft reset (inbound or outbound), it is normal for the BGP routing process to hold memory. The amount of memory that is held depends on the size of the routing tables and the percentage of the memory chunks that are utilized. Partially used memory chunks will be used or released before more memory is allocated from the global router pool.

Examples

In the following example, all members of the BGP peer group named INTERNAL are reset:

```
Router#
clear ip bgp peer-group INTERNAL
```

In the following example, members of the peer group named EXTERNAL in IPv4 multicast address family sessions are reset:

```
Router#
clear ip bgp ipv4 multicast peer-group EXTERNAL
```

In the following example, a soft reconfiguration is initiated for the inbound session with members of the peer group INTERNAL, and the outbound session is unaffected:

```
Router#
clear ip bgp peer-group INTERNAL soft in
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection or session.
neighbor peer-group (assigning members)	Configures a BGP neighbor to be a member of a peer group.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.

clear ip bgp rpki server

To close the TCP connection to the specified Resource Public Key Infrastructure (RPKI) server, purge SOVC records downloaded from that server, renegotiate the TCP connection, and redownload SOVC records, use the **clear ip bgp rpki server** command in privileged EXEC mode.

clear ip bgp rpki server {*ipv4-address* | *ipv6-address*} **port** *port-number* [**reset-only**]

Syntax Description

<i>ipv4-address</i>	IPv4 address of the RPKI server.
<i>ipv6-address</i>	IPv6 address of the RPKI server.
port <i>port-number</i>	Specifies the port number of the RPKI server.
reset-only	(Optional) Purges all downloaded SOVC records from the specified server, sends a Reset Query PDU to the server, and redownloads all SOVC records, but does not close the TCP connection.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
XE 3.5S	This command was introduced.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.
15.2(4)S	This command was implemented on the Cisco 7200 series routers.

Usage Guidelines

Use this command without the **reset-only** keyword to close the TCP connection to the indicated cache server, purge all SOVC records downloaded from that server, and then renegotiate the TCP connection(s) and redownload all SOVC records. If there is no TCP connection, the router will ignore the 60-second reconnect timer and try to connect right away.

Use this command with the **reset-only** keyword to purge all downloaded SOVC records from that server, send a Reset Query PDU to the server, and redownload all SOVC records from the server.

If more than one server is at the same address, but at different ports, the router will clear only for the RPKI server at the specified address and port.

The command causes the immediate emptying of the RPKI table for SOVC records obtained from the indicated server. The command does not trigger an immediate update of the routing table. The routing table will instead be updated upon receipt of an EOD PDU from a server, or the expiration of the stale path timer for a server,

or the removal of a server's configuration. Note that the server that sends the EOD, or whose stale path timer expires or is deconfigured, need not be the same server for which the **clear** command was issued.

Examples

The following example closes the TCP connection to the RPKI server at the specified address and port, purges all SOVC records downloaded from that server, renegotiates the TCP connection, and redownloads all SOVC records:

```
Router# clear ip bgp rpki server 192.168.14.2 port 1030
```

Related Commands

Command	Description
bgp rpki server	Connects to an RPKI server and enables the validation of BGP prefixes based on the AS from which the prefix originates.

clear ip bgp table-map

To reload information in the Border Gateway Protocol (BGP) routing table after a change in a table map or the route map referenced by a table map, use the **clear ip bgp table-map** command in privileged EXEC mode.

Syntax Without Address Family Syntax

clear ip bgp [*vrf vrf-name*] **table-map**

Syntax With Address Family Syntax

clear ip bgp [*ipv4|ipv6|vpnv4|vpnv6 {unicast|multicast}*] *vrf vrf-name* **table-map**

Syntax Description

vrf	(Optional) Specifies a virtual routing and forwarding instance.
<i>vrf-name</i>	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
ipv4	(Optional) Reloads information for IPv4 address family sessions.
ipv6	(Optional) Reloads information for IPv6 address family sessions.
vpnv4	(Optional) Reloads information for IPv4 VPN address family sessions.
vpnv6	(Optional) Reloads information for IPv6 VPN address family sessions.
unicast	(Optional) Reloads information for unicast address family sessions.
multicast	(Optional) Reloads information for multicast address family sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.0(21)S	This command was integrated into Cisco IOS Release 12.0(21)S.

Release	Modification
12.0(22)S	The vpn4 and ipv4 keywords were added.
12.1(13)E	This command was integrated into Cisco IOS Release 12.1(13)E.
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.
12.2SX	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(2)T	This command was modified. The vrf keyword and <i>vrf-name</i> argument were added.

Usage Guidelines

The **clear ip bgp table-map** command is used to clear or reload BGP routing tables. This command should be issued after a table map or the route map that it references is configured or changed, so that the change takes effect.

This command can be used to clear traffic-index information configured with the BGP Policy Accounting feature.

Examples

In the following example, a table map is configured and a traffic index is set. The new policy is applied after the **clear ip bgp table-map** command is entered.

```
Router(config)# route-map SET_BUCKET permit 10
Router(config-route-map)# match community 1
Router(config-route-map)# set traffic-index 2
Router(config-route-map)# exit
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4
Router(config-router-af)# table-map SET_BUCKET
Router(config-router-af)# end
Router# clear ip bgp table-map
```

The following example reloads the BGP routing table for IPv4 unicast peering sessions:

```
Router# clear ip bgp ipv4 unicast table-map
```

Related Commands

Command	Description
bgp-policy	Enables BGP policy accounting or policy propagation on an interface.

Command	Description
table-map	Enables metrics and tag values to be modified or enables selective route download when the IP routing table is updated with BGP learned routes.

clear ip bgp update-group

To reset Border Gateway Protocol (BGP) connections for all the members of a BGP update group, use the **clear ip bgp update-group** command in privileged EXEC mode.

Syntax Without Address Family Syntax

clear ip bgp [*vrf vrf-name*] **update-group** [*index-group*| *neighbor-address*]

Syntax With Address Family Syntax

clear ip bgp [*vrf vrf-name*] [**all**| **ipv4** {**multicast**| **mdt**| **unicast**}| **ipv6** {**multicast**| **unicast**}| **vpn4** **unicast**| **vpn6** **unicast**] **update-group** [*index-group*| *neighbor-address*]

Syntax Description

vrf	(Optional) Specifies an instance of a routing table.
<i>vrf-name</i>	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
<i>index-group</i>	(Optional) Specifies that the update group with the specified index number will be reset. The range of update group index numbers is from 1 to 4294967295.
<i>neighbor-address</i>	(Optional) Specifies the IP address of a single peer that will be reset. The value for this argument can be an IPv4 or IPv6 address.
all	(Optional) Specifies the reset of update group members in all address families.
ipv4	(Optional) Specifies the reset of update group members in IPv4 address family sessions.
multicast	(Optional) Specifies the reset of update group members in multicast address family sessions.
mdt	(Optional) Specifies the reset of update group members in multicast distribution tree (MDT) address family sessions.
unicast	(Optional) Specifies the reset of update group members in unicast address family sessions.
ipv6	(Optional) Specifies the reset of update group members in IPv6 address family sessions.

vpnv4	(Optional) Specifies the reset of update group members in Virtual Private Network Version 4 (VPNv4) address family sessions.
vpnv6	(Optional) Specifies the reset of update group members in Virtual Private Network Version 6 (VPNv6) address family sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.0(29)S	The mdt keyword was added.
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.
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(2)T	This command was modified. The vrf keyword and <i>vrf-name</i> argument were added.

Usage Guidelines

The **clear ip bgp update-group** command is used to clear BGP update group member sessions. If no keywords or arguments are specified, entering this command will recalculate all update groups. Specific index numbers for update groups and information about update-group membership is displayed in the output of the **show ip bgp update-group** and **debug ip bgp groups** commands.

When a change to outbound policy occurs, the BGP routing process will automatically recalculate update-group memberships and apply changes by triggering an outbound soft reset after a 1-minute timer expires. This behavior is designed to provide the network operator with time to change the configuration before the soft reset is initiated. You can immediately initiate the outbound soft reset before the timer expires by entering the **clear ip bgp ip-address soft out** command or immediately initiate a hard reset by entering the **clear ip bgp ip-address** command.

**Note**

In Cisco IOS Release 12.0(25)S, 12.3(2)T, and prior releases, the update group recalculation delay timer is set to 3 minutes.

Examples

In the following example, a hard reset is initiated for the peer 10.0.0.1:

```
Router# clear ip bgp 10.0.0.1
```

In the following example, all peers are cleared from the update group 10.0.0.1:

```
Router# clear ip bgp update-group 10.0.0.1
```

In the following example, update-group information for all peers in the index 1 update group is cleared:

```
Router# clear ip bgp update-group 1
```

In the following example, update-group information for all MDT address family session peers in the index 6 update group is cleared:

```
Router# clear ip bgp ipv4 mdt update-group 6
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection or session.
debug ip bgp groups	Displays information related to the processing of BGP update groups.
show ip bgp replication	Displays BGP update-group replication statistics.
show ip bgp update-group	Displays information about BGP update groups.

clear ip bgp vpnv4

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration for IPv4 Virtual Private Network (VPNv4) address family sessions, use the **clear ip bgp vpnv4** command in privileged EXEC mode.

clear ip bgp [*vrf vrf-name*] **vpnv4 unicast** *autonomous-system-number* [**in** [**prefix-filter**]] [**out**] [**slow**] [**soft** [**in** [**prefix-filter**]] **out** **slow**]]

Syntax Description

vrf	(Optional) Specifies an instance of a routing table.
<i>vrf-name</i>	(Optional) Name of the Virtual Private Network (VPN) routing and forwarding (VRF) table to use for storing data.
unicast	Specifies the reset of unicast address family sessions.
<i>autonomous-system-number</i>	Specifies that sessions with BGP peers in the specified autonomous system will be reset. Number in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the router bgp command.
in	(Optional) Initiates inbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.

out	(Optional) Initiates inbound or outbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.
slow	(Optional) Clears slow-peer status forcefully and moves it to original update group.
soft	(Optional) Initiates a soft reset. Does not tear down the session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(22)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.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
15.1(2)T	This command was modified. The vrf keyword and <i>vrf-name</i> argument were added.

Usage Guidelines

The **clear ip bgp vpnv4** command can be used to initiate a hard reset or soft reconfiguration of VPNv4 address family sessions. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

Generating Updates from Stored Information

To generate new inbound updates from stored update information (rather than dynamically) without resetting the BGP session, you must preconfigure the local BGP router using the **neighbor soft-reconfiguration inbound** command. This preconfiguration causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy. Storing updates is memory intensive and should be avoided if possible.

Outbound BGP soft configuration has no memory overhead and does not require any preconfiguration. You can trigger an outbound reconfiguration on the other side of the BGP session to make the new inbound policy take effect.

Use this command whenever any of the following changes occur:

- Additions or changes to the BGP-related access lists
- Changes to BGP-related weights
- Changes to BGP-related distribution lists
- Changes to BGP-related route maps

Dynamic Inbound Soft Reset

The route refresh capability, as defined in RFC 2918, allows the local router to reset inbound routing tables dynamically by exchanging route refresh requests to supporting peers. The route refresh capability does not store update information locally for non-disruptive policy changes. It instead relies on dynamic exchange with supporting peers. Route refresh is advertised through BGP capability negotiation. All BGP routers must support the route refresh capability.

To determine if a BGP router supports this capability, use the **show ip bgp neighbors** command. The following message is displayed in the output when the router supports the route refresh capability:

```
Received route refresh capability from peer.
```

If all BGP routers support the route refresh capability, use the **clear ip bgp vpnv4** command with the **in** keyword. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.

**Note**

After configuring a soft reset (inbound or outbound), it is normal for the BGP routing process to hold memory. The amount of memory that is held depends on the size of routing tables and the percentage of the memory chunks that are utilized. Partially used memory chunks will be used or released before more memory is allocated from the global router pool.

Examples

In the following example, a soft reconfiguration is initiated for the inbound sessions for BGP neighbors in VPNv4 unicast address family sessions, and the outbound session is unaffected:

```
Router#
clear ip bgp vpnv4 unicast soft in
```

In the following example, the route refresh capability is enabled on the VPNv4 unicast address family BGP neighbors and a soft reconfiguration is initiated for all inbound session with the VPNv4 multicast address family neighbors, and the outbound session is unaffected:

```
Router#
clear ip bgp vpnv4 unicast in
```

In the following example, a hard reset is initiated for neighbor sessions with all VPNv4 unicast address family routers in the autonomous system numbered 35700:

```
Router#
clear ip bgp vpnv4 unicast 35700
```

In the following example, a hard reset is initiated for BGP neighbors in IPv4 unicast address family sessions in the 4-byte autonomous system numbered 65538 in asplain notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Router#
clear ip bgp vpnv4 unicast 65538
```

In the following example, a hard reset is initiated for BGP neighbors in IPv4 unicast address family sessions in the 4-byte autonomous system numbered 1.2 in asdot notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, and Cisco IOS XE Release 2.3, or a later release.

```
Router#
clear ip bgp vpnv4 unicast 1.2
```

Related Commands

Command	Description
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.

clear ip bgp vpnv4 unicast dampening

To reset Border Gateway Protocol (BGP) route flap dampening for a particular IPv4 Virtual Private Network version 4 (VPNv4) address family prefix on a device that has no VRF concept, use the **clear ip bgp vpnv4 unicast dampening** command in privileged EXEC mode.

clear ip bgp vpnv4 unicast dampening *rd route-distinguisher* [*network-address* [*network-mask*]]

Syntax Description

rd <i>route-distinguisher</i>	(Optional) VPN route distinguisher (RD) is either an autonomous system number (ASN)-relative RD, in which case it is composed of an autonomous system number and an arbitrary number, or it is an IP-address-relative RD, in which case it is composed of an IP address and an arbitrary number. You can enter a <i>route-distinguisher</i> in either of these formats: 16-bit autonomous system number: your 32-bit number. For example, 10:1. 32-bit IP address: your 16-bit number. For example, 192.168.122.15:1.
<i>network-address</i>	(Optional) IPv4 address for which the flap statistics are cleared.
<i>network-mask</i>	(Optional) IPv4 network mask.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Use this command on a device that has no VRF concept, such as an ASBR for Option B or a route reflector for Option C. Do not use this command on a Provider Edge (PE) router.

You can use the **clear ip bgp vpnv4 unicast dampening** command to clear stored route dampening information for the VPNv4 address family from the global VPN table. If you specify a route-distinguisher in the command, the command clears all the prefixes that contain the particular route-distinguisher. If you specify a VPNv4 address in the command, the command clears the route dampening information for that particular network address.

**Note**

On a PE router that has VRF concept, you can use the **clear ip bgp vrf *vrf name* dampening** command to clear the dampening information for all the routes in the same VRF. Use the **clear ip bgp vrf *vrf name* dampening *network-address*** command to clear the dampening information for a specific route belonging to a particular VRF.

Examples

The following example shows how to reset the flap dampening for a particular VPNv4 prefix:

```
Router# clear ip bgp vpnv4 unicast dampening rd 10:1 192.168.2.1 255.255.255.0
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or configures BGP route dampening parameters.
clear ip bgp flap-statistics	Resets BGP route dampening flap-statistics.
set dampening	Sets route dampening parameters in a route map.
show ip bgp dampened-paths	Displays BGP dampened routes.

clear ip bgp vpnv6

To reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration for IPv6 Virtual Private Network (VPNv6) address family sessions, use the **clear ip bgp vpnv6** command in privileged EXEC mode.

clear ip bgp vpnv6 unicast *autonomous-system-number* [**in** [**prefix-filter**]] [**out**] [**slow**] [**soft** [**in** [**prefix-filter**]] **out**] **slow**]]

Syntax Description

unicast	Specifies the reset of unicast address family sessions.
<i>autonomous-system-number</i>	Specifies that sessions with BGP peers in the specified autonomous system will be reset. Number in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the router bgp command.
in	(Optional) Initiates inbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the existing outbound route filter (ORF) prefix list to trigger a new route refresh or soft reconfiguration, which updates the ORF prefix list.
out	(Optional) Initiates inbound or outbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.
slow	(Optional) Clears slow-peer status forcefully and moves it to original update group.

soft	(Optional) Initiates a soft reset. Does not tear down the session.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(2)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.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

The **clear ip bgp vpnv6** command can be used to initiate a hard reset or soft reconfiguration of VPNv6 address family sessions. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information,

at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

Generating Updates from Stored Information

To generate new inbound updates from stored update information (rather than dynamically) without resetting the BGP session, you must preconfigure the local BGP router using the **neighbor soft-reconfiguration inbound** command. This preconfiguration causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy. Storing updates is memory intensive and should be avoided if possible.

Outbound BGP soft configuration has no memory overhead and does not require any preconfiguration. You can trigger an outbound reconfiguration on the other side of the BGP session to make the new inbound policy take effect.

Use this command whenever any of the following changes occur:

- Additions or changes to the BGP-related access lists
- Changes to BGP-related weights
- Changes to BGP-related distribution lists
- Changes to BGP-related route maps

Dynamic Inbound Soft Reset

The route refresh capability, as defined in RFC 2918, allows the local router to reset inbound routing tables dynamically by exchanging route refresh requests to supporting peers. The route refresh capability does not store update information locally for non-disruptive policy changes. It instead relies on dynamic exchange with supporting peers. Route refresh is advertised through BGP capability negotiation. All BGP routers must support the route refresh capability.

To determine if a BGP router supports this capability, use the **show ip bgp neighbors** command. The following message is displayed in the output when the router supports the route refresh capability:

```
Received route refresh capability from peer.
```

If all BGP routers support the route refresh capability, use the **clear ip bgp vpnv6** command with the **in** keyword. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.



Note

After configuring a soft reset (inbound or outbound), it is normal for the BGP routing process to hold memory. The amount of memory that is held depends on the size of routing tables and the percentage of the memory chunks that are utilized. Partially used memory chunks will be used or released before more memory is allocated from the global router pool.

Examples

In the following example, a soft reconfiguration is initiated for the inbound sessions for BGP neighbors in VPNv6 unicast address family sessions, and the outbound session is unaffected:

```
Router#  
clear ip bgp vpnv6 unicast soft in
```

In the following example, the route refresh capability is enabled on the VPNv6 unicast address family BGP neighbors and a soft reconfiguration is initiated for all inbound session with the IPv6 multicast address family neighbors, and the outbound session is unaffected:

```
Router#
clear ip bgp vpnv6 unicast in
```

In the following example, a hard reset is initiated for neighbor sessions with all VPNv6 unicast address family routers in the autonomous system numbered 35700:

```
Router#
clear ip bgp vpnv6 unicast 35700
```

In the following example, a hard reset is initiated for BGP neighbors in VPNv6 unicast address family sessions in the 4-byte autonomous system numbered 65538 in asplain notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
Router#
clear ip bgp vpnv6 unicast 65538
```

In the following example, a hard reset is initiated for BGP neighbors in VPNv6 unicast address family sessions in the 4-byte autonomous system numbered 1.2 in asdot notation. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, 12.4(24)T, and Cisco IOS XE Release 2.3, or a later release.

```
Router#
clear ip bgp vpnv6 unicast 1.2
```

Related Commands

Command	Description
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.

clear ip bgp vpnv6 unicast dampening

To reset Border Gateway Protocol (BGP) route flap dampening for a particular IPv6 Virtual Private Network version 6 (VPNv6) address family prefix, use the **clear ip bgp vpnv6 unicast dampening** command in privileged EXEC mode.

clear ip bgp vpnv6 unicast dampening [*rd route-distinguisher* [*network-address*]]

Syntax Description

rd <i>route-distinguisher</i>	(Optional) The VPN route distinguisher (RD) is either an autonomous system number (ASN)-relative RD, in which case it is composed of an autonomous system number and an arbitrary number, or it is an IP-address-relative RD, in which case it is composed of an IP address and an arbitrary number. You can enter a <i>route-distinguisher</i> in either of these formats: • 16-bit autonomous system number: your 32-bit number. For example, 10:1. • 32-bit IP address: your 16-bit number. For example, 192.168.122.15:1.
<i>network-address</i>	(Optional) VPNv6 address for which the flap statistics are cleared.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

You can use the **clear ip bgp vpnv6 unicast dampening** command to clear stored route dampening information for the VPNv6 address family. If you specify a route-distinguisher in the command, the command clears all the prefixes that contain the particular route-distinguisher. If you specify a VPNv6 address in the command, the command clears the route dampening information for that particular network address.

Examples

The following example shows how to reset the flap dampening for a particular VPNv6 prefix:

```
Router# clear ip bgp vpnv6 unicast dampening rd 1:0 2001:1000::0/64
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or configures BGP route dampening parameters.
clear ip bgp flap-statistics	Resets BGP route dampening flap-statistics.
set dampening	Sets route dampening parameters in a route map.
show ip bgp dampened-paths	Displays BGP dampened routes.

clear ip prefix-list

To reset IP prefix-list counters, use the **clear ip prefix-list** command in privileged EXEC mode.

clear ip prefix-list*[prefix-list-name][network/length]*

Syntax Description

<i>prefix-list-name</i>	(Optional) Name of the prefix list from which the hit count is to be cleared.
<i>network / length</i>	(Optional) Network number and length (in bits) of the network mask. The slash mark must precede the bit length value.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0	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 **clear ip prefix-list** command is used to clear prefix-list hit counters. The hit count is a value indicating the number of matches to a specific prefix list entry.

Examples

In the following example, the prefix-list counters are cleared for the prefix list named FIRST_LIST that matches the 10.0.0.0/8 prefix:

```
Router# clear ip prefix-list FIRST_LIST 10.0.0.0/8
```

Related Commands

Command	Description
distribute-list in (IP)	Filters networks received in updates.
distribute-list out (IP)	Suppresses networks from being advertised in updates.

Command	Description
ip prefix-list	Creates an entry in a prefix list.
ip prefix-list description	Adds a text description of a prefix list.
ip prefix-list sequence-number	Enables the generation of sequence numbers for entries in a prefix list.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
show ip bgp regexp	Displays information about a prefix list or prefix list entries.

continue

To configure a route map to go to a route-map entry with a higher sequence number, use the **continue** command in route-map configuration mode. To remove a continue clause from a route map, use the **no** form of this command.

continue [*sequence-number*]

no continue

Syntax Description

<i>sequence-number</i>	(Optional) Route-map sequence number. If a route-map sequence number is not specified when configuring a continue clause, the continue clause will continue to the route-map entry with the next sequence number. This behavior is referred to as an “implied continue.”

Command Default

If the sequence number argument is not configured when this command is entered, the continue clause will go to the route-map entry with the next default sequence number.

If a route-map entry contains a continue clause and no match clause, the continue clause will be executed automatically.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(31)S	Support for outbound route maps 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 **continue** command supports inbound route maps only in Cisco IOS Release 12.2(18)S and prior releases. Support for both inbound and outbound route maps was introduced in Cisco IOS Release 12.0(31)S and later releases.

Route Map Operation Without Continue Clauses

A route map evaluates match clauses until a successful match occurs. After the match occurs, the route map stops evaluating match clauses and starts executing set clauses, in the order in which they were configured. If a successful match does not occur, the route map “falls through” and evaluates the next sequence number of the route map until all configured route-map entries have been evaluated or a successful match occurs. Each route-map sequence is tagged with a sequence number to identify the entry. Route-map entries are evaluated in order starting with the lowest sequence number and ending with the highest sequence number. If the route map contains only set clauses, the set clauses will be executed automatically, and the route map will not evaluate any other route-map entries.

Route Map Operation With Continue Clauses

When a continue clause is configured, the route map will continue to evaluate and execute match clauses in the specified route-map entry after a successful match occurs. The continue clause can be configured to go to (or jump to) a specific route-map entry by specifying the sequence number, or if a sequence number is not specified, the continue clause will go to the next sequence number. This behavior is called an “implied continue.” If a match clause exists, the continue clause is executed only if a match occurs. If no successful matches occur, the continue clause is ignored.

Match Operations With Continue Clauses

If a match clause does not exist in the route-map entry but a continue clause does, the continue clause will be automatically executed and go to the specified route-map entry. If a match clause exists in a route-map entry, the continue clause is executed only when a successful match occurs. When a successful match occurs and a continue clause exists, the route map executes the set clauses and then goes to the specified route-map entry. If the next route map contains a continue clause, the route map will execute the continue clause if a successful match occurs. If a continue clause does not exist in the next route map, the route map will be evaluated normally. If a continue clause exists in the next route map but a match does not occur, the route map will not continue and will “fall through” to the next sequence number if one exists.

Set Operations With Continue Clauses

Set clauses are saved during the match clause evaluation process and executed after the route-map evaluation is completed. The set clauses are evaluated and executed in the order in which they were configured. Set clauses are only executed after a successful match occurs, unless the route map does not contain a match clause. The continue statement proceeds to the specified route-map entry only after configured set actions are performed. If a set action occurs in the first route map and then the same set action occurs again, with a different value, in a subsequent route-map entry, the last set action will override any previous set actions that were configured with the same **set** command.

**Note**

A continue clause can be executed, without a successful match, if a route-map entry does not contain a match clause.

Examples

In the following example, continue clause configuration is shown.

The first continue clause in route-map entry 10 indicates that the route map will go to route-map entry 30 if a successful matches occurs. If a match does not occur, the route map will “fall through” to route-map entry 20. If a successful match occurs in route-map entry 20, the set action will be executed and the route-map will not evaluate any additional route-map entries. Only the first successful **match ip address** clause is supported.

If a successful match does not occur in route-map entry 20, the route-map will “fall through” to route-map entry 30. This sequence does not contain a match clause, so the set clause will be automatically executed and the continue clause will go to the next route-map entry because a sequence number is not specified.

If there are no successful matches, the route-map will “fall through” to route-map entry 30 and execute the set clause. A sequence number is not specified for the continue clause so route-map entry 40 will be evaluated.

```
Router(config)# route-map ROUTE-MAP-NAME permit 10
Router(config-route-map)# match ip address 1
Router(config-route-map)# match metric 10
Router(config-route-map)# set as-path prepend 10
Router(config-route-map)# continue 30
Router(config-route-map)# exit
Router(config)# route-map ROUTE-MAP-NAME permit 20
Router(config-route-map)# match ip address 2
Router(config-route-map)# match metric 20
Router(config-route-map)# set as-path prepend 10 10
Router(config-route-map)# exit
Router(config)# route-map ROUTE-MAP-NAME permit 30
Router(config-route-map)# set as-path prepend 10 10 10
Router(config-route-map)# continue
Router(config-route-map)# exit
Router(config)# route-map ROUTE-MAP-NAME permit 40
Router(config-route-map)# match community 10:1
Router(config-route-map)# set local-preference 104
Router(config-route-map)# exit
```

Related Commands

Command	Description
aggregate-address	Creates an aggregate entry in a BGP or multicast BGP database.
match as-path	Match BGP autonomous system path access lists.
match community	Matches a BGP community.
match extcommunity	Matches a BGP extended community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address permitted by a standard or extended access list, or performs policy routing on packets.

Command	Description
match ip next-hop	Redistributes any routes that have a next-hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match length	Bases policy routing on the Level 3 length of a packet.
match metric (IP)	Redistributes routes with the metric specified.
match mpls-label	Redistributes routes that include MPLS labels if the routes meet the conditions specified in the route map.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
neighbor default-originate	Allows a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route.
neighbor route-map	Applies a route map to incoming or outgoing routes.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol to another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value in a route-map configuration.
set comm-list delete	Removes communities from the community attribute of an inbound or outbound update.
set community	Sets the BGP communities attribute.
set dampening	Sets the BGP route dampening factors.

Command	Description
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and have no explicit route to the destination.
set extcommunity	Sets the BGP extended communities attribute.
set interface	Indicates where to output packets that pass a match clause of route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.
set ip default next-hop verify-availability	Configures a router to check the CDP database for the availability of an entry for the default next hop that is specified by the set ip default next-hop command.
set ip next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ip next-hop verify-availability	Configures policy routing to verify if the next hops of a route map are CDP neighbors before policy routing to those next hops.
set ip precedence	Sets the precedence value in the IP header.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set mpls-label	Enables a route to be distributed with an MPLS label if the route matches the conditions specified in the route map.
set next-hop	Specifies the address of the next hop.
set nlri	This command was replaced by the address-family ipv4 and address-family vpnv4 commands.
set origin (BGP)	Sets the BGP origin code.
set qos-group	Sets a group ID that can be used later to classify packets.
set tag (IP)	Sets the value of the destination routing protocol.

Command	Description
set traffic-index	Defines where to output packets that pass a match clause of a route map for BGP policy accounting.
set weight	Specifies the BGP weight for the routing table.
show ip bgp	Displays entries in the BGP routing table.
show route-map	Displays all route maps configured or only the one specified.

debug ip bgp event rpki

To display information related to the BGP—Origin AS Validation feature and the process of connecting to a Resource Public Key Infrastructure (RPKI) server to download prefix information, use the **debug ip bgp event rpki** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip bgp event rpki

no debug ip bgp event rpki

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.5S	This command was introduced.
	15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.
	15.2(4)S	This command was implemented on the Cisco 7200 series routers.

Usage Guidelines This command provides details about the following events:

- Gain/loss of connectivity to cache server
- Receipt of serial notify
- Sending of serial query
- Sending of reset query
- Receipt of End of Data
- Receipt of cache reset
- Error report sent or received
- Expiration of stale path timer

Examples The following example enables debugging of events related to the BGP—Origin AS Validation feature:

```
Router# debug ip bgp event rpki
```

Related Commands

Command	Description
bgp rpki server	Connects to an RPKI server and enables the validation of BGP prefixes based on the AS from which the prefix originates.

debug ip bgp igp-metric ignore

To display information related to the system ignoring the Interior Gateway Protocol (IGP) metric during best path selection, use the **debug ip bgp igp-metric ignore** command in privileged EXEC mode. To disable such debugging output, use the **no** form of this command.

debug ip bgp igp-metric ignore

no debug ip bgp igp-metric ignore

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.
	15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
	15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines You might use this command if the path you expected to be chosen as the best path at the shadow route reflector was not chosen as such. That could be because the **bgp bestpath igp-metric ignore** command makes the best path algorithm choose the same best path as the primary route reflector if they are not colocated.

Examples The following example shows how to enable debugging of events related to the system ignoring the IGP metric during best path selection:

```
Router# debug ip bgp igp-metric ignore
```

Related Commands	Command	Description
	bgp bestpath igp-metric ignore	Specifies that the system ignore the IGP metric during best path selection.

debug ip bgp import

To display debugging information related to importing IPv4 prefixes from the BGP global routing table into a VRF table or exporting from a VRF table into the BGP global table, use the **debug ip bgp import** command in privileged EXEC mode. To disable the display of such debugging information, use the **no** form of this command.

debug ip bgp import {events| updates [*access-list*| *expanded-access-list*]}

no debug ip bgp import {events| updates [*access-list*| *expanded-access-list*]}

Syntax Description

events	Displays messages related to IPv4 prefix import events.
updates	Displays messages related to IPv4 prefix import updates.
<i>access-list</i>	(Optional) Number of the access list used to filter debugging messages. The range is from 1 to 199.
<i>expanded-access-list</i>	(Optional) Number of the expanded access list used to filter debugging messages. The range is from 1300 to 2699.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.2(4)S	This command was modified. The output now includes information for the BGP Support for IP Prefix Export from a VRF to the Global Table feature.
Cisco IOS XE Release 3.7S	This command was modified. The output now includes information for the BGP Support for IP Prefix Export from a VRF to the Global Table feature.

Usage Guidelines

Use this command to display debugging information related to the BGP Support for IP Prefix Import from Global Table into a VRF Table feature or the BGP Support for IP Prefix Export from a VRF Table into Global Table feature. The former feature provides the capability to import IPv4 unicast prefixes from the global routing table into a Virtual Private Network (VPN) routing/forwarding (VRF) instance table using an import route map. The latter feature provides the capability to export IPv4 or IPv6 prefixes from a VRF table into the global table using an export route map.

Examples

The following example configures IPv4 prefix import debugging messages for both import events and import updates to be displayed on the console of the router:

```
Router# debug ip bgp import events

BGP import events debugging is on
Router# debug ip bgp import updates
BGP import updates debugging is on for access list 3
00:00:50: %BGP-5-ADJCHANGE: neighbor 10.2.2.2 Up
00:01:06: BGP: reevaluate IPv4 Unicast routes in VRF academic
00:01:06: BGP: 0 routes available (limit: 1000)
00:01:06: BGP: import IPv4 Unicast routes to VRF academic
00:01:06: BGP(2)-VRF(academic): import pfx 100:1:10.30.1.0/24 via 10.2.2.2
00:01:06: BGP: accepted 8 routes (limit: 1000)
00:01:06: BGP: reevaluate IPv4 Multicast routes in VRF multicast
00:01:06: BGP: 0 routes available (limit: 2)
00:01:06: BGP: import IPv4 Multicast routes to VRF multicast
00:01:06: %BGP-4-AFIMPORT: IPv4 Multicast prefixes imported to multicast vrf reached the
limit 2
00:01:06: BGP: accepted 2 routes (limit: 2)
00:01:06: BGP: reevaluate IPv4 Unicast routes in VRF BLUE
00:01:06: BGP: 0 routes available (limit: 1000)
00:01:06: BGP: import IPv4 Unicast routes to VRF BLUE
00:01:06: BGP: accepted 3 routes (limit: 1000)
```

The table below describes the significant fields shown in the display.

Table 6: debug ip bgp import Field Descriptions

Field	Description
BGP: accepted 2 routes (limit: 2)	Number of routes imported into the VRF, and the default or user-defined prefix import limit.
BGP: reevaluate IPv4 Unicast routes in VRF BLUE	Prefix was imported during BGP convergence and is being reevaluated for the next scan cycle.
BGP: 0 routes available (limit: 1000)	Number of routes available from the import source, and the default or user-defined prefix import limit.
BGP: import IPv4 Unicast routes to VRF BLUE	Import map and prefix type (unicast or multicast) that is being imported into the specified VRF.

The following is a sample debug message for the IP prefix export from a VRF table to global table:

```
Device# debug ip bgp import events
```

```
*Jul 12 10:06:48.357: BGP GBL-IMP: vpn1:VPNv4 Unicast:base 1:1:192.168.4.0/24
-> global:IPv4 Unicast:base Creating importing net.
  4.4.4.4 (metric 11) from 4.4.4.4 (4.4.4.4)
    Origin IGP, metric 0, localpref 100, valid, internal, best
    Extended Community: RT:1:1
    mpls labels in/out nolabel/16
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection.
export map (VRF table to global table)	Exports IP prefixes from a VRF table to the global routing table based on a route map.
import map	Imports IP prefixes from the global routing table to a VRF table based on a route map.

debug ip bgp route-server

To turn on debugging for a BGP route server, use the **debug ip bgp route-server** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip bgp route-server {client| context| event| import| policy} [detail]

no debug ip bgp route-server {client| context| event| import| policy} [detail]

Syntax Description

client	Displays information about BGP route server clients.
context	Displays information about BGP route server contexts.
event	Displays information about route server events, such as importing into the virtual RS table.
import	Displays information about BGP route server import maps.
policy	Displays information about the policy path process.
detail	(Optional) Displays detailed debugging information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 3.3S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

Use this command to turn on debugging of a BGP router server.



Caution

The **detail** keyword is used for complex issues and should only be turned on when you are debugging with a Cisco representative.

Examples

In the following example, BGP route server client debugging is turned on:

```
Router# debug ip bgp route-server client
```

Related Commands

Command	Description
import-map	Configures flexible policy handling by a BGP route server.
neighbor route-server-client	Specifies on a BGP route server that a neighbor is a route server client.
route-server-context	Creates a route-server context in order to provide flexible policy handling for a BGP route server.

default (bmp)

To enable the default form of a command used to configure BGP Monitoring Protocol (BMP) servers, use the **default** command in BMP server configuration mode.

default {**activate** | **address** {*ipv4-addr* | *ipv6-addr*} **port-number** *port-number* | **description** **LINE** *server-description* | **exit-bmp-server-mode** | **failure-retry-delay** | **flapping-delay** | **initial-delay** | **set ip dscp** *dscp-value* | **stats-reporting-period** | **update-source** *interface-type interface-number*}

Syntax Description

activate	Sets the default connection between the BMP servers and BGP BMP neighbors.
address	Sets the default IP address on the BMP servers.
<i>ipv4-addr</i>	Specifies the default IPv4 address for the BMP servers.
<i>ipv6-addr</i>	Specifies the default IPv6 address for the BMP servers.
port-number <i>port-number</i>	Sets the default port number for the listening BMP servers. The port number of the listening BMP servers range from 1 to 65535. The value specified for the BMP server in this range becomes the default port number.
description LINE <i>server-description</i>	Sets the default description of the BMP servers. The text defined for the <i>server-description</i> argument becomes the default line description for specific BMP servers.
exit-bmp-server-mode	Sets the default exit flag from BMP server configuration mode.
failure-retry-delay	Sets the default delay for retries upon failures when sending BMP server updates.
flapping-delay	Sets the default delay for flapping when sending BMP server updates.
initial-delay	Sets the default delay when sending the initial BMP server updates.
set ip dscp <i>dscp-value</i>	Sets the default IP Differentiated Services Code Point (DSCP) values for BMP servers. The value specified for the <i>dscp-value</i> argument, which ranges from 0 to 7, becomes the default value.
stats-reporting-period	Sets the default reporting period for the statistics of BMP servers.
update-source <i>interface-type interface-number</i>	Sets the default interface source of routing updates on a BMP server. The interface specified for the <i>interface-type interface-number</i> argument becomes the default value.

Command Default

The default form of the commands used to configure BMP servers is not set.

Command Modes

BMP server configuration

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use the **bmp server** command to enter BMP server configuration mode and configure a specific BMP server. To configure BGP BMP neighbors to which the BMP servers establish a connection, use the **neighbor bmp-activate** command in router configuration mode. Use the **show ip bgp bmp** command to verify default forms and values of the commands and parameters, respectively, that have been configured.

Examples

The following example show how to enter BMP server configuration mode and assign default value to the **set ip dscp** command:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp server 1
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 10.1.1.1 port-number 8000
Device(config-router-bmpsrvr)# default set ip dscp 6
Device(config-router-bmpsrvr)# exit-bmp-server-mode
Device(config-router)# bmp server 2
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 20.1.1.1 port-number 9000
Device(config-router-bmpsrvr)# default set ip dscp 6
Device(config-router-bmpsrvr)# end
```

The following is sample output from the **show ip bgp bmp server detail** command for BMP server number 1 and 2. The “IP Precedence value” field in the output displays the default IP DSCP value (indicating Internetwork control) set for BMP servers 1 and 2:

```
Device# show ip bgp bmp server detail | include IP Precedence

IP Precedence value : 6
IP Precedence value : 6
```

Related Commands

Command	Description
bmp server	Enters BMP server configuration mode to configure specific BMP servers.
neighbor bmp-activate	Activates BMP monitoring for BGP neighbors.

Command	Description
show ip bgp bmp	Displays information about BMP servers and neighbors.

default-information originate (BGP)

To configure a Border Gateway Protocol (BGP) routing process to distribute a default route (network 0.0.0.0), use the **default-information originate** command in address family or router configuration mode. To disable the advertisement of a default route, use the **no** form of this command.

default-information originate

no default-information originate

Syntax Description This command has no arguments or keywords.

Command Default No default behavior or values

Command Modes Address family configuration (config-router-af)
Router configuration (config-router)

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(7)T	Address family configuration mode support 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.

Usage Guidelines The **default-information originate** command is used to configure a BGP routing process to advertise a default route (network 0.0.0.0). A redistribution statement must also be configured to complete this configuration or the default route will not be advertised.

The configuration of the **default-information originate** command in BGP is similar to the configuration of the **network (BGP)** command. The **default-information originate** command, however, requires explicit redistribution of the route 0.0.0.0. The **network** command requires only that the route 0.0.0.0 is present in the Interior Gateway Protocol (IGP) routing table. For this reason, the **network** command is preferred.



Note

The **default-information originate** command should not be configured with the **neighbor default-originate** command on the same router. You should configure one or the other.

Examples

In the following example, the router is configured to redistribute a default route from OSPF into the BGP routing process:

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 unicast

Router(config-router-af)# default-information originate

Router(config-router-af)# redistribute ospf 100

Router(config-router-af)# end
```

Related Commands

Command	Description
neighbor default-originate	Configures a BGP routing process to send a default route (network 0.0.0.0) to a neighbor.
network (BGP)net	Specifies the list of networks for the BGP routing process.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

default-metric (BGP)

To set a default metric for routes redistributed into Border Gateway Protocol (BGP), use the **default-metric** command in address family or router configuration mode. To remove the configured value and return BGP to default operation, use the **no** form of this command.

default-metric *number*

no default-metric *number*

Syntax Description

<i>number</i>	Default metric value applied to the redistributed route. The range of values for this argument is from 1 to 4294967295.

Command Default

The following is default behavior if this command is not configured or if the **no** form of this command is entered:

- The metric of redistributed interior gateway protocol (IGP) routes is set to a value that is equal to the interior BGP (iBGP) metric.
- The metric of redistributed connected and static routes is set to 0.

When this command is enabled, the metric for redistributed connected routes is set to 0.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode support 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.

Usage Guidelines

The **default-metric** command is used to set the metric value for routes redistributed into BGP and can be applied to any external BGP (eBGP) routes received and subsequently advertised internally to iBGP peers.

This value is the Multi Exit Discriminator (MED) that is evaluated by BGP during the best path selection process. The MED is a non-transitive value that is processed only within the local autonomous system and adjacent autonomous systems. The default metric is not set if the received route has a MED value.

**Note**

When enabled, the **default-metric** command applies a metric value of 0 to redistributed connected routes. The **default-metric** command does not override metric values that are applied with the **redistribute** command.

Examples

In the following example, a metric of 1024 is set for routes redistributed into BGP from OSPF:

```
Router(config)# router bgp 50000
Router(config-router)# address-family ipv4 unicast
```

```
Router(config-router-af)# default-metric 1024
Router(config-router-af)# redistribute ospf 10
Router(config-router-af)# end
```

In the following configuration and output examples, a metric of 300 is set for eBGP routes received and advertised internally to an iBGP peer.

```
Router(config)# router bgp 65501
Router(config-router)# no synchronization
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# network 172.16.1.0 mask 255.255.255.0
Router(config-router)# neighbor 172.16.1.1 remote-as 65501
Router(config-router)# neighbor 172.16.1.1 soft-reconfiguration inbound
Router(config-router)# neighbor 192.168.2.2 remote-as 65502
Router(config-router)# neighbor 192.168.2.2 soft-reconfiguration inbound
Router(config-router)# default-metric 300
Router(config-router)# no auto-summary
```

After the above configuration, some routes are received from the eBGP peer at 192.168.2.2 as shown in the output from the **show ip bgp neighbors received-routes** command.

```
Router# show ip bgp neighbors 192.168.2.2 received-routes
```

```
BGP table version is 7, local router ID is 192.168.2.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
*> 172.17.1.0/24   192.168.2.2               0      100      0 65502 i
```

After the received routes from the eBGP peer at 192.168.2.2 are advertised internally to iBGP peers, the output from the **show ip bgp neighbors received-routes** command shows that the metric (MED) has been set to 300 for these routes.

```
Router# show ip bgp neighbors 172.16.1.2 received-routes
BGP table version is 2, local router ID is 172.16.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
* i172.16.1.0/24   172.16.1.2               0      100      0 i
* i172.17.1.0/24   192.168.2.2             300     100      0 65502 i
Total number of prefixes 2
```

Related Commands

Command	Description
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

description (bmp)

To configure a textual description of a BMP server, use the **description** command in BMP server configuration mode. To remove the description, use the **no** form of the command.

description *LINE* *server-description*

no description *LINE* *server-description*

Syntax Description

LINE	Sets a textual line describing a BMP server.
<i>server-description</i>	Specifies the line describing a BMP server upto a maximum limit of 80 characters.

Command Default

Line description is not configured for the BMP servers.

Command Modes

BMP server configuration (config-router-bmpsrvr)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use the **bmp server** command to enter BMP server configuration mode and configure a specific BMP server. To configure BGP BMP neighbors to which the BMP servers establish a connection, use the **neighbor bmp-activate** command in router configuration mode. Use the **show ip bgp bmp** command to verify that the line description of the BMP server has been configured.

Examples

The following example show how to enter BMP server configuration mode and assign a textual description for BMP servers 1 and 2:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp server 1
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 10.1.1.1 port-number 8000
Device(config-router-bmpsrvr)# description LINE SERVER1
Device(config-router-bmpsrvr)# exit-bmp-server-mode
Device(config-router)# bmp server 2
Device(config-router-bmpsrvr)# activate
```

description (bmp)

```
Device(config-router-bmpsrvr)# address 20.1.1.1 port-number 9000
Device(config-router-bmpsrvr)# description LINE SERVER2
Device(config-router-bmpsrvr)# end
```

The following is sample output from the **show ip bgp bmp server** command for BMP server number 1 and 2. The “description” field in the output displays the line description assigned to BMP servers 1 and 2:

```
Device# show ip bgp bmp server 1
```

```
Print detailed info for 1 server number 1.
```

```
bmp server 1
address: 10.1.1.1      port 8000
description SERVER1
up time 00:06:22
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
activated
```

```
Device# show ip bgp bmp server 2
```

```
Print detailed info for 1 server number 2.
```

```
bmp server 2
address: 20.1.1.1      port 9000
description SERVER2
up time 00:06:23
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
activated
```

Related Commands

Command	Description
bmp server	Enters BMP server configuration mode to configure specific BMP servers.
neighbor bmp-activate	Activates BMP monitoring for BGP neighbors.
show ip bgp bmp	Displays information about BMP servers and neighbors.

description (route server context)

To specify a description for a BGP route server context, use the **description** command in route server context configuration mode. To remove the description, use the **no** form of this command.

description *string*

no description

Syntax Description

<i>string</i>	Description of the route server context. The string can be up to 80 characters long.

Command Default

No description for a route server context exists.

Command Modes

Route server context configuration (config-router-rsctx)

Command History

Release	Modification
Cisco IOS XE 3.3S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

Create a route server context if you want your BGP route server to support customized, flexible policies. The routes needing flexible policy handling are selected for import into a route server context by an import map that you configure. The import map references a route map, where the actual policy is defined.

The **description** command allows an optional description of a route server context to remind you of the purpose of the context or policy, for example. This is more user-friendly and scannable than trying to interpret the route map commands when looking at a configuration file or **show** output.

Examples

In the following example, the description is a user-friendly way to see the purpose of the context, without having to interpret the import map and route map:

```
Router(config)# router bgp 65000
Router(config-router)# route-server-context only_AS27_context
Router(config-router-rsctx)# description Context references route map permitting only routes
with AS 27 in AS path.
```

Related Commands

Command	Description
import-map	Configures flexible policy handling by a BGP route server.
route-server-context	Creates a route-server context in order to provide flexible policy handling for a BGP route server.

distance bgp

To configure the administrative distance for BGP routes, use the **distance bgp** command in address family or router configuration mode. To return to the administrative distance to the default value, use the **no** form of this command.

distance bgp *external-distance internal-distance local-distance*
no distance bgp

Syntax Description

<i>external-distance</i>	Administrative distance for external BGP routes. Routes are external when learned from an external autonomous system. The range of values for this argument are from 1 to 255.
<i>internal-distance</i>	Administrative distance for internal BGP routes. Routes are internal when learned from peer in the local autonomous system. The range of values for this argument are from 1 to 255.
<i>local-distance</i>	Administrative distance for local BGP routes. Local routes are those networks listed with a network router configuration command, often as back doors, for the router or for the networks that is being redistributed from another process. The range of values for this argument are from 1 to 255.

Command Default

The following values are used if this command is not configured or if the no form is entered:

external-distance : 20 *internal-distance*: 200 *local-distance*: 200

Routes with a distance of 255 are not installed in the routing table.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode support was added.
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

The **distance bgp** command is used to configure a rating of the trustworthiness of a routing information source, such as an individual router or a group of routers. Numerically, an administrative distance is a positive integer from 1 to 255. In general, the higher the value, the lower the trust rating. An administrative distance of 255 means the routing information source cannot be trusted at all and should be ignored. Use this command if another protocol is known to be able to provide a better route to a node than was actually learned via external BGP (eBGP), or if some internal routes should be preferred by BGP.



Caution

Changing the administrative distance of internal BGP routes is considered dangerous and is not recommended. Improper configuration can introduce routing table inconsistencies and break routing.

The **distance bgp** command replaces the **distance mbgp** command.

Examples

In the following example, the external distance is set to 10, the internal distance is set to 50, and the local distance is set to 100:

```
Router(config)# router bgp 50000
Router(config-router)# address family ipv4 multicast
Router(config-router-af)# network 10.108.0.0

Router(config-router-af)# neighbor 192.168.6.6 remote-as 123

Router(config-router-af)# neighbor 172.16.1.1 remote-as 47
Router(config-router-af)# distance bgp 10 50 100

Router(config-router-af)# end
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.

distribute-list in (BGP)

To filter routes or networks received in incoming Border Gateway Protocol (BGP) updates, use the **distribute-list in** command in router configuration mode. To delete the distribute list and remove it from the running configuration file, use the **no** form of this command.

distribute-list {*acl-number*| **prefix** *list-name*} **in**
no distribute-list {*acl-number*| **prefix** *list-name*} **in**

Syntax Description

<i>acl-number</i>	IP access list number. The access list defines which networks are to be received and which are to be suppressed in routing updates.
prefix <i>list-name</i>	Name of a prefix list. The prefix list defines which networks are to be received and which are to be suppressed in routing updates, based upon matching prefixes.

Command Default

If this command is configured without a predefined access list or prefix list, the distribute list will default to permitting all traffic.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
11.2	The <i>acl-number</i> arguments was added.
12.0	The prefix keyword and <i>list-name</i> argument were 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.

Usage Guidelines

The **distribute-list in** command is used to filter incoming BGP updates. An access list or prefix list must be defined prior to configuration of this command. Standard and expanded access lists are supported. IP prefix lists are used to filter based on the bit length of the prefix. An entire network, subnet, supernet, or single host route can be specified. Prefix list and access list configuration is mutually exclusive when configuring a

distribute list. The session must be reset with the **clear ip bgp** command before the distribute list will take effect.

**Note**

Interface type and number arguments may be displayed in the CLI depending on the version of Cisco IOS software you are using. However, the interface arguments are not supported in any Cisco IOS software release.

**Note**

We recommend that you use IP prefix lists (configured with the **ip prefix-list** command in global configuration mode) instead of distribute lists. IP prefix lists provide improved performance and are simpler to configure. Distribute list configuration will be removed from the CLI at a future date.

To suppress networks from being advertised in updates, use the **distribute-list out** command.

Examples

In the following example, a prefix list and distribute list are defined to configure the BGP routing process to accept traffic from only network 10.1.1.0/24, network 192.168.1.0, and network 10.108.0.0. An inbound route refresh is initiated to activate the distribute-list.

```
Router(config)# ip prefix-list RED permit 10.1.1.0/24
Router(config)# ip prefix-list RED permit 10.108.0.0/16

Router(config)# ip prefix-list RED permit 192.168.1.0/24

Router(config)# router bgp 50000

Router(config-router)# network 10.108.0.0

Router(config-router)# distribute-list prefix RED in

Router(config-router)# end
Router# clear ip bgp in
```

In the following example, an access list and distribute list are defined to configure the BGP routing process to accept traffic from only network 192.168.1.0 and network 10.108.0.0. An inbound route refresh is initiated to activate the distribute-list.

```
Router(config)# access-list 1 permit 192.168.1.0

Router(config)# access-list 1 permit 10.108.0.0

Router(config)# router bgp 50000

Router(config-router)# network 10.108.0.0
Router(config-router)# distribute-list 1 in
Router(config-router)# end
Router# clear ip bgp in
```

Related Commands

Command	Description
access-list	Defines an IP access list.
clear ip bgp	Resets a BGP connection or session.

Command	Description
distribute-list out (BGP)	Suppresses networks from being advertised in outbound BGP updates.
ip prefix-list	Creates an entry in a prefix list.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

distribute-list out (BGP)

To suppress networks from being advertised in outbound Border Gateway Protocol (BGP) updates, use the **distribute-list out** command in router configuration mode. To delete the distribute list and remove it from the running configuration file, use the **no** form of this command.

distribute-list {*acl-number*| **prefix** *list-name*} **out** [*protocol process-number*| **connected**| **static**]

no distribute-list {*acl-number*| **prefix** *list-name*} **out** [*protocol process-number*| **connected**| **static**]

Syntax Description

<i>acl-number</i>	IP access list number. The access list defines which networks are to be received and which are to be suppressed in routing updates.
prefix <i>list-name</i>	Name of a prefix list. The list defines which networks are to be received and which are to be suppressed in routing updates, based upon matching prefixes in the prefix list.
<i>protocol process-number</i>	Specifies the routing protocol to apply the distribution list. BGP, EIGRP, OSPF, and RIP are supported. The process number is entered for all routing protocols, except RIP. The process number is a value from 1 to 65535.
connected	Specifies peers and networks learned through connected routes.
static	Specifies peers and networks learned through static routes.

Command Default

If this command is configured without a predefined access list or prefix list, the distribute list will default to permitting all traffic.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
11.2	The <i>acl-number</i> argument was added.
12.0	The prefix keyword and <i>list-name</i> argument were added.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Command History

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 **distribute-list out** command is used to filter outbound BGP updates. An access list or prefix list must be defined prior to configuration of this command. Standard and expanded access lists are supported. IP prefix lists are used to filter based on the bit length of the prefix. An entire network, subnet, supernet, or single host route can be specified. Prefix list and access list configuration is mutually exclusive when configuring a distribute list. The session must be reset with the **clear ip bgp** command before the distribute list will take effect.



Note

Interface type and number arguments may be displayed in the CLI depending on the version of Cisco IOS software you are using. However, the interface arguments are not supported in any Cisco IOS software release.



Note

We recommend that you use IP prefix lists (configured with the **ip prefix-list** command in global configuration mode) instead of distribute lists. IP prefix lists provide improved performance and are simpler to configure. Distribute list configuration will be removed from the CLI at a future date.

Entering a *protocol* and/or *process-number* arguments causes the distribute list to be applied to only routes derived from the specified routing process. Addresses not specified in the distribute-list command will not be advertised in outgoing routing updates after a distribute list is configured.

To suppress networks or routes from being received in inbound updates, use the **distribute-list in** command.

Examples

In the following example, a prefix list and distribute list are defined to configure the BGP routing process to advertise only network 192.168.0.0. An outbound route refresh is initiated to activate the distribute-list.

```
Router(config)# ip prefix-list BLUE permit 192.168.0.0/16
Router(config)# router bgp 50000
Router(config-router)# distribute-list prefix BLUE out
Router(config-router)# end
```

```
Router# clear ip bgp out
```

In the following example, an access list and a distribute list are defined to configure the BGP routing process to advertise only network 192.168.0.0. An outbound route refresh is initiated to activate the distribute-list.

```
Router(config)# access-list 1 permit 192.168.0.0 0.0.255.255
Router(config)# access-list 1 deny 0.0.0.0 255.255.255.255
```

distribute-list out (BGP)

```

Router(config)# router bgp 50000

Router(config-router)# distribute-list 1 out
Router(config-router)# end
Router# clear ip bgp out

```

Related Commands

Command	Description
access-list	Defines an IP access list.
clear ip bgp	Resets a BGP connection or session.
distribute-list in (BGP)	Filters routes and networks received in updates.
ip prefix-list	Creates an entry in a prefix list.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.

exit-bmp-server-mode (bmp)

To exit from BGP Monitoring Protocol (BMP) server configuration mode and return to router configuration mode, use the **exit-bmp-server-mode** command in BMP server configuration mode. To disable exit from BMP server configuration mode, use the **no** form of the command.

exit-bmp-server-mode

no exit-bmp-server-mode

Command Default Configuration of the specified BMP server continues in BMP server configuration mode.

Command Modes BMP server configuration (config-router-bmpsrvr)

Command History	Release	Modification
	15.4(1)S	This command was introduced.
	Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines Use the **bmp server** command to enter BMP server configuration mode and configure a specific BMP server. To configure BGP BMP neighbors to which the BMP servers establish a connection, use the **neighbor bmp-activate** command in router configuration mode. Use the **show running-config** command to display the configuration of different BMP servers.

Examples The following example show how to enter BMP server configuration mode and assign IP address and port number for BMP server 1 and 2:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp server 1
Device(config-router-bmpsrvr)# address 10.1.1.1 port-number 8000
Device(config-router-bmpsrvr)# description SERVER1
Device(config-router-bmpsrvr)# initial-delay 20
Device(config-router-bmpsrvr)# failure-retry-delay 40
Device(config-router-bmpsrvr)# flapping-delay 120
Device(config-router-bmpsrvr)# update-source Ethernet0/0
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# exit-bmp-server-mode
Device(config-router)# bmp server 2
Device(config-router-bmpsrvr)# address 20.1.1.1 port-number 9000
Device(config-router-bmpsrvr)# description SERVER2
Device(config-router-bmpsrvr)# initial-delay 20
Device(config-router-bmpsrvr)# failure-retry-delay 40
Device(config-router-bmpsrvr)# flapping-delay 120
Device(config-router-bmpsrvr)# update-source Ethernet2/0
```

exit-bmp-server-mode (bmp)

```
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# exit-bmp-server-mode
Device(config-router)#
```

The following is sample output from the **show ip bgp bmp server** command for BMP server number 1 and 2. The “address” and the “port” field in the output display the IP address and the port number of the listening BMP servers 1 and 2:

```
Device# show running-config | section bmp
```

```

bmp server 1
address 10.1.1.1 port-number 8000
description SERVER1
initial-delay 20
failure-retry-delay 40
flapping-delay 120
update-source Ethernet0/0
activate
exit-bmp-server-mode
bmp server 2
address 20.1.1.1 port-number 9000
description SERVER2
initial-delay 20
failure-retry-delay 40
flapping-delay 120
update-source Ethernet2/0
activate
exit-bmp-server-mode

```

Related Commands

Command	Description
bmp server	Enters BMP server configuration mode to configure specific BMP servers.
neighbor bmp-activate	Activates BMP monitoring for BGP neighbors.
show running-config	Displays running configuration on a device.

exit-peer-policy

To exit policy-template configuration mode and enter router configuration mode, use the **exit-peer-policy** command in policy-template configuration mode.

exit-peer-policy

Syntax Description This command has no keywords or arguments.

Command Default No default behavior or values

Command Modes Policy-template configuration (config-router-ptmp)

Command History	Release	Modification
	12.0(24)S	This command was introduced.
	12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
	12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
	12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
	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 router is configured to exit policy-template configuration mode and enter router configuration mode:

```
Router(config-router-ptmp) # exit-peer-policy
Router(config-router) #
```

Related Commands

Command	Description
template peer-policy	Creates a peer policy template and enters policy-template configuration mode.

exit-peer-session

To exit session-template configuration mode and enter router configuration mode, use the **exit-peer-session** command in session-template configuration mode.

exit-peer-session

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Session-template configuration (config-router-stmp)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
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 router is configured to exit session-template configuration mode and enter router configuration mode:

```
Router(config-router-stmp) # exit-peer-session
Router(config-router) #
```

Related Commands

Command	Description
template peer-session	Creates a peer session template and enters session-template configuration mode.

exit-route-server-context

To exit a route server context and return to router configuration mode, use the **exit-route-server-context** command in route server context configuration mode.

exit-route-server-context

Syntax Description This command has no arguments or keywords.

Command Modes Route server context configuration (config-router-rsctx)

Command History	Release	Modification
	Cisco IOS XE 3.3S	This command was introduced.
	15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines When you configure a BGP route server with a flexible policy, you create a route server context with an import map, which is when you might use the **exit-route-server-context** command. The **exit-route-server-context** command is one of the commands that will be displayed in system help if you enter a ? at the Router(config-router-rsctx)# prompt. However, the **exit** command performs the same function as the **exit-route-server-context** command.

Examples In the following example, a route server context is created and the **exit-route-server-context** command is used to exit route server context configuration mode:

```
router bgp 65000
  route-server-context ONLY_AS27_CONTEXT
  address-family ipv4 unicast
    import-map only_AS27_routemap
  exit-address-family
  exit-route-server-context
!
```

Router(config)#

Related Commands	Command	Description
	route-server-context	Creates a route-server context in order to provide flexible policy handling for a BGP route server.

export map (VRF table to global table)

To export IP prefixes from a VRF table into the global table, use the **export map** command in IP VRF configuration or in address family configuration mode. To remove the export map, use the **no** form of this command.

export {ipv4| ipv6} {unicast| multicast} [*prefix-limit*] **map** *map-name*

no export {ipv4| ipv6} {unicast| multicast} [*prefix-limit*] **map** *map-name*

Syntax Description

ipv4	Specifies that IPv4 prefixes will be exported.
ipv6	Specifies that IPv6 prefixes will be exported.
unicast	Specifies that unicast prefixes will be exported.
multicast	Specifies that multicast prefixes will be exported.
<i>prefix-limit</i>	(Optional) Limits the number of prefixes that will be exported. The default limit is 1000 prefixes. The range is from 1 to 2147483647 prefixes.
<i>map-name</i>	Identifies the map to be used as an export map.

Command Default

No IP prefixes are exported from a VRF table into the global table.

Command Modes

Address family configuration (config-router-af)
IP VRF configuration (config-vrf)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines

Use this command to implement the BGP Support for IP Prefix Export from a VRF Table into the Global Table feature.

You can access the **export map** command by using the **vrf definition** global configuration command followed by the **address-family** configuration command. You can also access the **export map** command by using the **ip vrf** global configuration command.

Examples

In the following example, an export map (route map) named OnlyNet2000 is configured under the IPv6 address family. The route map matches on routes that pass the prefix list named net2000, which permits IPv6 routes with the prefix 2000::/16.

```
vrf definition vrfname1
 rd 100:100
  address-family ipv6
   export ipv6 unicast map OnlyNet2000
   route-target import 100:100
   route-target export 100:100
 !
ipv6 prefix-list net2000 permit 2000::/16
!
route-map OnlyNet2000 permit 10
 match ipv6 address prefix-list net2000
```

In the following example, an export map named OnlyNet200 is configured under the IPv4 address family. The route map matches on routes that pass the prefix list named net200, which permits IPv4 routes with the prefix 200.0.0.0/8.

```
vrf definition vrfname2
 rd 100:100
  address-family ipv4
   export ipv4 unicast map OnlyNet200
   route-target import 100:100
   route-target export 100:100
 !
ip prefix-list net200 permit 200.0.0.0/8
!
route-map OnlyNet200 permit 10
 match ip address prefix-list net200
```

In the following example, an export map named OnlyNet200 is configured under the **ip vrf** command. The route map matches on routes that pass the prefix-list named net200, which permits IPv4 routes with the prefix 200.0.0.0/8.

```
ip vrf vrfname
 rd 100:100
  export ipv4 unicast map OnlyNet200
  route-target import 100:100
  route-target export 100:100
 !
ip prefix-list net200 permit 200.0.0.0/8
!
route-map OnlyNet200 permit 10
 match ip address prefix-list net200
```

Related Commands

Command	Description
address-family	Selects an address family type and enters address family configuration mode.
ip vrf	Configures a VRF routing table.

Command	Description
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

failure-retry-delay (bmp)

To configure delay in the retry requests during failures when sending BGP Monitoring Protocol (BMP) server updates, use the **failure-retry-delay** command in BMP server configuration mode. To disable configuration of delays in failure retry requests, use the **no** form of the command.

failure-retry-delay *failure-retry-delay*

no failure-retry-delay

Syntax Description

<i>failure-retry-delay</i>	Specifies the delay, in seconds, in retry requests during failures when sending BMP server updates. The delay value that can be configured ranges from 1 to 3600 seconds.

Command Default

There is no delay in retry requests upon failures in sending BMP server updates.

Command Modes

BMP server configuration (config-router-bmpsrvr)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use the **bmp server** command to enter BMP server configuration mode and configure a specific BMP server. To configure BGP BMP neighbors to which the BMP servers establish a connection, use the **neighbor bmp-activate** command in router configuration mode. Use the **show ip bgp bmp** command to verify the failure retry delay configured for a specific BMP server.

Examples

The following example show how to enter BMP server configuration mode and configure the failure retry delay for BMP servers 1 and 2:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp server 1
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 10.1.1.1 port-number 8000
Device(config-router-bmpsrvr)# failure-retry-delay 40
Device(config-router-bmpsrvr)# exit-bmp-server-mode
Device(config-router)# bmp server 2
Device(config-router-bmpsrvr)# activate
```

```
Device(config-router-bmpsrvr)# address 20.1.1.1 port-number 9000
Device(config-router-bmpsrvr)# failure-retry-delay 40
Device(config-router-bmpsrvr)# end
```

The following is sample output from the **show ip bgp bmp server** command for BMP server number 1 and 2. The “failure-retry-delay” field in the output displays the failure retry delay configured for BMP servers 1 and 2:

```
Device# show ip bgp bmp server 1
```

Print detailed info for 1 server number 1.

```
bmp server 1
address: 10.1.1.1      port 8000
description SERVER1
up time 00:06:22
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
activated
```

```
Device# show ip bgp bmp server 2
```

Print detailed info for 1 server number 2.

```
bmp server 2
address: 20.1.1.1      port 9000
description SERVER2
up time 00:06:23
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
activated
```

Related Commands

Command	Description
bmp server	Enters BMP server configuration mode to configure specific BMP servers.
neighbor bmp-activate	Activates BMP monitoring for BGP neighbors.
show ip bgp bmp	Displays information about BMP servers and neighbors.

flapping-delay (bmp)

To configure delays in flapping when sending BGP Monitoring Protocol (BMP) server updates, use the **flapping-delay** command in BMP server configuration mode. To disable configuration of flapping delays, use the **no** form of the command.

flapping-delay *flap-delay*

no flapping-delay

Syntax Description

<i>flap-delay</i>	Configures delay, in seconds, caused due to flaps during connection establishment between BMP servers and BGP BMP neighbors. The value for flap delay that can be configured ranges from 1 to 3600 seconds.

Command Default

There is no delay configured for flapping during BMP session establishment.

Command Modes

BMP server configuration (config-router-bmpsrvr)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use the **bmp server** command to enter BMP server configuration mode and configure a specific BMP server. To configure BGP BMP neighbors to which the BMP servers establish a connection, use the **neighbor bmp-activate** command in router configuration mode. Use the **show ip bgp bmp** command to verify the flapping delay configured for the BMP servers.

Examples

The following example show how to enter BMP server configuration mode and configure flapping delay for BMP servers 1 and 2:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp server 1
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 10.1.1.1 port-number 8000
Device(config-router-bmpsrvr)# flapping-delay 40
Device(config-router-bmpsrvr)# exit-bmp-server-mode
Device(config-router)# bmp server 2
Device(config-router-bmpsrvr)# activate
```

```
Device(config-router-bmpsrvr)# address 20.1.1.1 port-number 9000
Device(config-router-bmpsrvr)# flapping-delay 80
Device(config-router-bmpsrvr)# end
```

The following is sample output from the **show ip bgp bmp server** command for BMP server number 1 and 2. The “address” and the “port” field in the output display the IP address and the port number of the listening BMP servers 1 and 2:

```
Device# show ip bgp bmp server 1
```

Print detailed info for 1 server number 1.

```
bmp server 1
address: 10.1.1.1    port 8000
description SERVER1
up time 00:06:22
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 40
activated
```

```
Device# show ip bgp bmp server 2
```

Print detailed info for 1 server number 2.

```
bmp server 2
address: 20.1.1.1    port 9000
description SERVER2
up time 00:06:23
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 80
activated
```

Related Commands

Command	Description
bmp server	Enters BMP server configuration mode to configure specific BMP servers.
neighbor bmp-activate	Activates BMP monitoring for BGP neighbors.
show ip bgp bmp	Displays information about BMP servers and neighbors.

ha-mode graceful-restart

To enable or disable the Border Gateway Protocol (BGP) graceful restart capability for a BGP peer session template, use the **ha-mode graceful-restart** command in peer session template configuration mode. To remove from the configuration the BGP graceful restart capability for a BGP peer session template, use the **no** form of this command.

ha-mode graceful-restart [disable]

no ha-mode graceful-restart [disable]

Syntax Description

disable	(Optional) Disables BGP graceful restart capability for a neighbor.

Command Default

BGP graceful restart is disabled.

Command Modes

Peer session template configuration (config-router-stmp)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

The **ha-mode graceful-restart** command is used to enable or disable the graceful restart capability for a BGP peer session template. Use the **disable** keyword to disable the graceful restart capability when graceful restart has been previously enabled for the BGP peer.

The graceful restart capability is negotiated between nonstop forwarding (NSF)-capable and NSF-aware peers in OPEN messages during session establishment. If the graceful restart capability is enabled after a BGP session has been established, the session will need to be restarted with a soft or hard reset.

The graceful restart capability is supported by NSF-capable and NSF-aware routers. A router that is NSF-capable can perform a stateful switchover (SSO) operation (graceful restart) and can assist restarting peers by holding routing table information during the SSO operation. A router that is NSF-aware functions like a router that is NSF-capable but cannot perform an SSO operation.

Peer session templates are used to group and apply the configuration of general BGP session commands to groups of neighbors that share session configuration elements. General session commands that are common for neighbors that are configured in different address families can be configured within the same peer session

template. Peer session templates are created and configured in peer session configuration mode. Only general session commands can be configured in a peer session template.

General session commands can be configured once in a peer session template and then applied to many neighbors through the direct application of a peer session template or through indirect inheritance from a peer session template. The configuration of peer session templates simplifies the configuration of general session commands that are commonly applied to all neighbors within an autonomous system.

To enable the BGP graceful restart capability globally for all BGP neighbors, use the **bgp graceful-restart** command. Use the **show ip bgp neighbors** command to verify the BGP graceful restart configuration for BGP neighbors.

Examples

The following example enables the BGP graceful restart capability for the BGP peer session template named S1 and disables the BGP graceful restart capability for the BGP peer session template named S2. The external BGP neighbor at 192.168.1.2 inherits peer session template S1, and the BGP graceful restart capability is enabled for this neighbor. Another external BGP neighbor, 192.168.3.2, is configured with the BGP graceful restart capability disabled after inheriting peer session template S2.

```
router bgp 45000
 template peer-session S1
  remote-as 40000
  ha-mode graceful-restart
 exit-peer-session
 template peer-session S2
  remote-as 50000
  ha-mode graceful-restart disable
 exit-peer-session
 bgp log-neighbor-changes
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 inherit peer-session S1
 neighbor 192.168.3.2 remote-as 50000
 neighbor 192.168.3.2 inherit peer-session S2
 end
```

Related Commands

Command	Description
bgp graceful-restart	Enables the BGP graceful restart capability globally for all BGP neighbors.
neighbor ha-mode graceful-restart	Enables or disables the BGP graceful restart capability for a BGP neighbor or peer group.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

import ipv4

To configure an import map to import IPv4 prefixes from the global routing table to a VRF table, use the **import ipv4** command in VRF configuration or in VRF address family configuration mode. To remove the import map, use the **no** form of this command.

import ipv4 {unicast| multicast} [*prefix-limit*] **map** *route-map*

no import ipv4 {unicast| multicast} [*prefix-limit*] **map** *route-map*

Syntax Description

unicast	Specifies IPv4 unicast prefixes to import.
multicast	Specifies IPv4 multicast prefixes to import.
<i>prefix-limit</i>	(Optional) Number of prefixes to import. The range is from 1 to 2147483647. Default is 1000.
map <i>route-map</i>	Specifies the route map to be used as an import route map for the VRF.

Command Default

No import map is configured.

Command Modes

VRF configuration (config-vrf)

VRF address family configuration (config-vrf-af)

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

IP prefixes that are defined for import are processed through a match clause in a route map. The prefixes that pass through the route map are imported into the Virtual Private Network (VPN) routing/forwarding (VRF) instance. A maximum of five VRFs per router can be configured to import IPv4 prefixes from the global routing table. 1000 prefixes per VRF are imported by default. You can manually configure from 1 to 2,147,483,647 prefixes for each VRF. We recommend that you use caution if you manually configure the prefix import limit. Configuring the router to import too many prefixes can interrupt normal router operation. Only IPv4 unicast and multicast prefixes can be imported to a VRF with this feature. IPv4 prefixes imported into a VRF using this feature cannot be imported into a VPNv4 VRF.

You can access the **import ipv4** command by using the **ip vrf** global configuration command. You can also access the **import ipv4** command by using the **vrf definition** global configuration command followed by the **address-family** VRF configuration command.

No MPLS or Route Target Configuration Is Required

No MPLS or route target (import/export) configuration is required.

Import Behavior

Import actions are triggered when a new routing update is received or when routes are withdrawn. During the initial BGP update period, the import action is postponed to allow BGP to converge more quickly. Once BGP converges, incremental BGP updates are evaluated immediately and qualified prefixes are imported as they are received.

Examples

The following example, beginning in global configuration mode, imports all unicast prefixes from the 10.24.240.0/22 subnet into the VRF named GREEN. An IP prefix list is used to define the imported IPv4 prefixes. The route map is attached to the Ethernet interface 0, and unicast RPF verification for VRF GREEN is enabled.

```
ip prefix-list COLORADO permit 10.24.240.0/22
!
ip vrf GREEN
  rd 100:10
  import ipv4 unicast 1000 map UNICAST
  exit
route-map UNICAST permit 10
  match ip address prefix-list ACCOUNTING
  exit
interface Ethernet 0
  ip policy route-map UNICAST
  ip verify unicast vrf GREEN permit
end
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
ip verify unicast vrf	Enables Unicast Reverse Path Forwarding verification for the specified VRF.
ip vrf	Configures a VRF routing table.
rd	Creates routing and forwarding tables for a VRF.

Command	Description
show ip bgp	Displays entries in the BGP routing table.
show ip bgp vpnv4	Displays VPN address information from the BGP table.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

import map

To configure an import route map for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **import map** command in VRF configuration or in VRF address family configuration mode. To remove the import map, use the **no** form of this command.

import [**ipv4**] [**unicast**|**multicast**] [*prefix-limit*] **map** *map-name*

no import [**ipv4**] [**unicast**|**multicast**] [*prefix-limit*] **map** *map-name*

Syntax Description

ipv4	(Optional) Specifies that IPv4 prefixes will be imported.
unicast	(Optional) Specifies that unicast prefixes will be imported.
multicast	(Optional) Specifies that multicast prefixes will be imported.
<i>prefix-limit</i>	(Optional) Limits the number of prefixes that will be imported. The default limit is 1000 prefixes. The range is from 1 to 2147483647 prefixes.
<i>map-name</i>	Identifies the route map to be used as an import route map for the VRF.

Command Default

A VRF has no import route map unless one is configured using the **import map** command.

Command Modes

VRF configuration (config-vrf) VRF address family configuration (config-vrf-af)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS 12.2(14)S.

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.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use an import route map when an application requires finer control over the routes imported into a VRF than provided by the import and export extended communities configured for the importing and exporting VRF. You can also use the **import map** command to implement the BGP Support for IP Prefix Import from Global Table into a VRF Table feature.

The **import map** command associates a route map with the specified VRF. You can use a route map to filter routes that are eligible for import into a VRF, based on the route target extended community attributes of the route. The route map might deny access to selected routes from a community that is on the import list.

The **import map** command does not replace the need for a route-target import in the VRF configuration. You use the **import map** command to further filter prefixes that match a route-target import statement in that VRF.

You can access the **import map** command by using the **ip vrf** global configuration command. You can also access the **import map** command by using the **vrf definition** global configuration command followed by the **address-family** VRF configuration command.

Examples

The following example shows how to configure an import route map for a VRF:

```
Router(config)# ip vrf vrf1
Router(config-vrf)# import map importmap1
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
export map	Exports IP prefixes from a VRF table into the global table.
ip vrf	Configures a VRF routing table.
route-target	Creates a route-target extended community for a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

Command	Description
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

import path limit

To specify the maximum number of Border Gateway Protocol (BGP) paths, per VPN routing and forwarding (VRF) importing net, that can be imported from an exporting net, use the **import path limit** command in address family configuration mode. To reset the BGP path import limit to the default value, use the **no** form of this command.

import path limit *number-of-import-paths*

no import path limit *number-of-import-paths*

Syntax Description

<i>number-of-import-paths</i>	Maximum number of BGP paths, per importing net, that can be imported from an exporting net.

Command Default

BGP, by default, installs only one best path in the routing table.

Command Modes

Address family configuration--IPv4 VRF only (config-router-af)

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.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.

Usage Guidelines

Use the **import path limit** command to control memory utilization when importing paths using the BGP Event-Based VPN Import feature. A maximum limit of the number of paths imported from an exporting net can be specified, per importing net. When a selection is made of paths to be imported from one or more exporting net, the first selection priority is a bestpath, the next selection priority is for multipaths, and the lowest selection priority is for nonmultipaths. The import path policy is set using the **import path selection** command.

The BGP Event-Based VPN Import feature introduces a modification to the existing BGP path import process. BGP Virtual Private Network (VPN) import provides importing functionality for BGP paths where BGP paths are imported from the BGP VPN table into a BGP virtual routing and forwarding (VRF) topology. In the existing path import process, when path updates occur, the import updates are processed during the next scan time which is a configurable interval of 5 to 15 seconds. The scan time adds a delay in the propagation of routes. The enhanced BGP path import is driven by events; when a BGP path changes, all of its imported copies are updated as soon as processing is available.

Using the BGP Event-Based VPN Import feature, convergence times are significantly reduced because provider edge (PE) routers can propagate VPN paths to customer edge (CE) routers without the scan time delay. Configuration changes such as adding imported route-targets to a VRF are not processed immediately, and are still handled during the 60-second periodic scanner pass.

Examples

The following example shows how to specify a maximum number of BGP paths to import from an exporting net for each importing net. Two BGP neighbors are configured in BGP router configuration mode and are activated in VPNv4 address family configuration mode. In IPv4 VRF address family configuration mode, the import path selection is set to all, and the number of import paths is set to 3.

```
Router(config)# router bgp 45000
Router(config-router)# neighbor 192.168.1.2 remote-as 40000
Router(config-router)# neighbor 192.168.3.2 remote-as 50000
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 192.168.1.2 activate
Router(config-router-af)# neighbor 192.168.3.2 activate
Router(config-router-af)# exit-address-family
Router(config-router)# address-family ipv4 vrf vrf-A
Router(config-router-af)# import path selection all
Router(config-router-af)# import path limit 3
Router(config-router-af)# end
```

Related Commands

Command	Description
import path selection	Specifies the BGP import path selection policy for a specific VRF instance.
show ip bgp vpnv4	Displays VPNv4 address information from the BGP table.

import path selection

To specify the Border Gateway Protocol (BGP) import path selection policy for a specific VPN routing and forwarding (VRF) instance, use the **import path selection** command in address family configuration mode. To remove the BGP import path selection policy for a VRF, use the **no** form of this command.

import path selection {**all**| **bestpath** [**strict**]| **multipaths** [**strict**]}

no import path selection {**all**| **bestpath** [**strict**]| **multipaths** [**strict**]}

Syntax Description

all	Imports all available paths from the exporting net that match any route targets (RTs) associated with the importing VRF instance. The number of paths imported per importing net must not exceed the import path limit set using the import path limit command.
bestpath	Imports the best available path that matches the RT of the VRF instance. If the best path in the exporting net does not match the RT of the VRF instance, a best available path that matches the RT of the VRF instance, is imported.
multipaths	Imports the bestpath and all paths marked as multipaths that match the RT of the VRF instance. If there are no bestpath or multipath matches, the best available path is selected. The number of paths imported per importing net must not exceed the import path limit set using the import path limit command.
strict	(Optional) Disables the fall back safety option of choosing the best available path for the bestpath and multipath keywords. If there are no paths appropriate to the configured option--bestpath or multipath--in the exporting net that match the RT of the VRF instance, then no paths are imported. This behavior matches the behavior of the software before the BGP Event-Based VPN Import feature was introduced.

Command Default BGP, by default, installs only one best path in the routing table.

Command Modes Address family configuration--IPv4 VRF only (config-router-af)

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.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.

Usage Guidelines

Use the **import path selection** command to set the import path policy for the BGP Event-Based VPN Import feature. Use the **import path limit** command to control memory utilization when importing paths by limiting the number of paths imported from an exporting net into each importing net.

The BGP Event-Based VPN Import feature introduces a modification to the existing BGP path import process. BGP Virtual Private Network (VPN) import provides importing functionality for BGP paths where BGP paths are imported from the BGP VPN table into a BGP virtual routing and forwarding (VRF) topology. In the existing path import process, when path updates occur, the import updates are processed during the next scan time which is a configurable interval of 5 to 15 seconds. The scan time adds a delay in the propagation of routes. The enhanced BGP path import is driven by events; when a BGP path changes, all of its imported copies are updated as soon as processing is available.

Using the BGP Event-Based VPN Import feature, convergence times are significantly reduced because provider edge (PE) routers can propagate VPN paths to customer edge (CE) routers without the scan time delay. Configuration changes such as adding imported route-targets to a VRF are not processed immediately, and are still handled during the 60-second periodic scanner pass.

Examples

The following example shows how to specify a BGP import path selection policy for a specific VRF instance. Two BGP neighbors are configured in BGP router configuration mode and are activated in VPNv4 address family configuration mode. In IPv4 VRF address family configuration mode, the import path selection is set to all, and the number of import paths is set to 3. In this example, up to three paths from an exporting net that match any of the route targets associated with the VRF of the importing net, can be imported.

```
Router(config)# router bgp 45000
Router(config-router)# neighbor 192.168.1.2 remote-as 40000
Router(config-router)# neighbor 192.168.3.2 remote-as 50000
Router(config-router)# address-family vpnv4
Router(config-router-af)# neighbor 192.168.1.2 activate
Router(config-router-af)# neighbor 192.168.3.2 activate
Router(config-router-af)# exit-address-family
Router(config-router)# address-family ipv4 vrf vrf-A
Router(config-router-af)# import path selection all
Router(config-router-af)# import path limit 3
Router(config-router-af)# end
```

Related Commands

Command	Description
import path limit	Specifies the maximum number of BGP paths, per VRF importing net, that can be imported from an exporting net.
show ip bgp vpnv4	Displays VPNv4 address information from the BGP table.

import-map

To configure flexible policy handling by a BGP route server, use the **import-map** command in route server context address family configuration mode. To remove the route server's flexible policy handling, use the **no** form of this command.

import-map *route-map-name*

no import-map *route-map-name*

Syntax Description

route-map-name

Name of the route map that controls which routes will be added to the route server client virtual table.

Command Default

No import map exists and no flexible policy handling by a route server exists.

Command Modes

Route server context address family configuration (config-router-rsctx-af)

Command History

Release	Modification
Cisco IOS XE 3.3S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

Use this command if your BGP route server needs to support flexible policies.

In order to configure flexible policy handling, you must create a route server context, which includes an import map. The import map references a standard route map. You may match on nexthop, AS path, communities, and extended communities.



Note

Do not confuse the **import-map** command with the **import map** command in VRF configuration submode, which configures an import route map for a VPN routing and forwarding (VRF) instance.

Examples

In the following example, the local router is a BGP route server. Its neighbors at 10.10.10.12 and 10.10.10.13 are its route server clients. A route server context named ONLY_AS27_CONTEXT is created and applied to the neighbor at 10.10.10.13. The context uses an import map that references a route map named only_AS27_routemap. The route map matches routes permitted by access list 27. Access list 27 permits routes that have 27 in the autonomous system path.

```
router bgp 65000
```

```

route-server-context ONLY_AS27_CONTEXT
  address-family ipv4 unicast
    import-map only_AS27_routemap
  exit-address-family
exit-route-server-context
!
neighbor 10.10.10.12 remote-as 12
neighbor 10.10.10.12 description Peer12
neighbor 10.10.10.13 remote-as 13
neighbor 10.10.10.13 description Peer13
neighbor 10.10.10.21 remote-as 21
neighbor 10.10.10.27 remote-as 27
!
address-family ipv4
  neighbor 10.10.10.12 activate
  neighbor 10.10.10.12 route-server-client
  neighbor 10.10.10.13 activate
  neighbor 10.10.10.13 route-server-client context ONLY_AS27_CONTEXT
  neighbor 10.10.10.21 activate
  neighbor 10.10.10.27 activate
exit-address-family
!
ip as-path access-list 27 permit 27
!
route-map only_AS27_routemap permit 10
  match as-path 27
!

```

Related Commands

Command	Description
description (route server context)	Describes a route server context for a user-friendly way to see the purpose of the route server context.
route-map	Enables policy routing.
route-server-context	Creates a route-server context in order to provide flexible policy handling for a BGP route server.

inherit peer-policy

To configure a peer policy template to inherit the configuration from another peer policy template, use the **inherit peer-policy** command in policy-template configuration mode. To remove an inherit statement from a peer policy template, use the **no** form of this command.

inherit peer-policy *policy-template sequence-number*

no inherit peer-policy *policy-template sequence-number*

Syntax Description

<i>policy-template</i>	Name of the peer policy template to be inherited.
<i>sequence-number</i>	Sequence number that sets the order in which the peer policy template is evaluated. Like a route-map sequence number, the lowest sequence number is evaluated first.

Command Default

No inherit statements are configured.

Command Modes

Policy-template configuration (config-router-ptmp)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
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 **inherit peer-policy** command is used to configure a peer policy template to inherit the configuration of another peer policy template. Peer policy templates support inheritance and a peer can directly and indirectly inherit up to seven peer policy templates. Inherited peer policy templates are configured with sequence numbers like route maps. An inherited peer policy template, like a route map, is evaluated starting with the inherit statement with the lowest sequence number. However, peer policy templates do not fall through. Every sequence is evaluated. If a BGP policy command is reapplied with a different value, it will overwrite any previous value from a lower sequence number.

**Note**

A Border Gateway Protocol (BGP) routing process cannot be configured to be a member of a peer group and to use peer templates for group configurations. You must use one method or the other. We recommend peer templates because they provide improved performance and scalability.

Examples

In the following example, a peer policy template named CUSTOMER-A is created. This peer policy template is configured to inherit the configuration from the peer policy templates named PRIMARY-IN and GLOBAL.

```
Router(config-router)# template peer-policy CUSTOMER-A
Router(config-router-ptmp)# route-map SET-COMMUNITY in
Router(config-router-ptmp)# filter-list 20 in

Router(config-router-ptmp)# inherit peer-policy PRIMARY-IN 20
Router(config-router-ptmp)# inherit peer-policy GLOBAL 10
Router(config-router-ptmp)# exit-peer-policy
Router(config-router)#
```

Related Commands

Command	Description
exit peer-policy	Exits policy-template configuration mode and enters router configuration mode.
neighbor inherit peer-policy	Configures a router to send a peer policy template to a neighbor so that the neighbor can inherit the configuration.
show ip bgp template peer-policy	Displays locally configured peer policy templates.
template peer-policy	Creates a peer policy template and enters policy-template configuration mode.

inherit peer-session

To configure a peer session template to inherit the configuration from another peer session template, use the **inherit peer-session** command in session-template configuration mode. To remove an inherit statement from a peer session template, use the **no** form of this command.

inherit peer-session *template-name*

no inherit peer-session *template-name*

Syntax Description

<i>template-name</i>	Name of the peer session template to inherit.

Command Default

No inherit statements are configured.

Command Modes

Session-template configuration (config-router-stmp)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
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 **inherit peer-session** command is used to configure a peer session template to inherit the configuration of another peer session template. A peer can be configured with only one peer session template at a time, and that peer session template can contain only one indirectly inherited peer session template. However, each indirectly inherited session template can also contain an indirectly inherited template. So, a peer can directly inherit only one peer session template and indirectly inherit up to seven additional indirectly inherited peer session templates, allowing you to apply up to a maximum of eight inherited peer session configurations.



Note

If you attempt to configure more than one inherit statement with a single peer session template, an error message will be displayed.

Indirectly inherited peer session templates are evaluated first, and the directly applied (locally configured) peer session template is evaluated last. If a general session command is reapplied with a different value, the subsequent value will have priority and overwrite the previous value that was configured in the indirectly inherited template. In other words, an overlapping statement from a local configuration will override the statement from the inherited configuration.

Examples

In the following example, a peer session template named CORE1 is created. This example inherits the configuration of the peer session template named INTERNAL-BGP.

```
Router(config-router)# template peer-session CORE1
Router(config-router-stmp)# description CORE-123
Router(config-router-stmp)# update-source loopback 1
Router(config-router-stmp)# inherit peer-session INTERNAL-BGP
Router(config-router-stmp)# exit-peer-session

Router(config-router)#
```

Related Commands

Command	Description
exit peer-session	Exits session-template configuration mode and enters router configuration mode.
neighbor inherit peer-session	Configures a router to send a peer session template to a neighbor so that the neighbor can inherit the configuration.
show ip bgp template peer-session	Displays locally configured peer session templates.
template peer-session	Creates a peer session template and enters session-template configuration mode.

initial-delay (bmp)

To configure delays in sending initial requests for updates from the BGP Monitoring Protocol (BMP) server, use the **initial-delay** command in BMP server configuration mode. To disable configuration of delays in sending initial requests, use the **no** form of the command.

initial-delay *initial-delay-time*

no initial-delay

Syntax Description

<i>initial-delay-time</i>	Configures the delay timer, in seconds, in sending initial requests for updates from the BMP server. The value for the configuration of the delay timer ranges from 1 to 3600 seconds.

Command Default

There is no delay in sending initial requests for updates from the BMP servers.

Command Modes

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use the **bmp server** command to enter BMP server configuration mode and configure a specific BMP server. To configure BGP BMP neighbors to which the BMP servers establish a connection, use the **neighbor bmp-activate** command in router configuration mode. Use the **show ip bgp bmp** command to verify the initial delay configured for sending BMP server updates.

Examples

The following example show how to enter BMP server configuration mode and configure initial delay timer for BMP servers 1 and 2:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp server 1
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 10.1.1.1 port-number 8000
Device(config-router-bmpsrvr)# initial-delay 20
Device(config-router-bmpsrvr)# exit-bmp-server-mode
Device(config-router)# bmp server 2
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 20.1.1.1 port-number 9000
```

```
Device(config-router-bmpsrvr)# initial-delay 20
```

```
Device(config-router-bmpsrvr)# end
```

The following is sample output from the **show ip bgp bmp server** command for BMP server number 1 and 2. The “initial-delay” field in the output displays the time configured for initial delay requests:

```
Device# show ip bgp bmp server 1
```

Print detailed info for 1 server number 1.

```
bmp server 1  
address: 10.1.1.1    port 8000  
description SERVER1  
up time 00:06:22  
session-startup route-refresh  
initial-delay 20  
failure-retry-delay 40  
flapping-delay 120  
activated
```

```
Device# show ip bgp bmp server 2
```

Print detailed info for 1 server number 2.

```
bmp server 2  
address: 20.1.1.1    port 9000  
description SERVER2  
up time 00:06:23  
session-startup route-refresh  
initial-delay 20  
failure-retry-delay 40  
flapping-delay 120  
activated
```

Related Commands

Command	Description
bmp server	Enters BMP server configuration mode to configure specific BMP servers.
neighbor bmp-activate	Activates BMP monitoring for BGP neighbors.
show ip bgp bmp	Displays information about BMP servers and neighbors.

ip as-path access-list

To configure an autonomous system path filter using a regular expression, use the **ip as-path access-list** command in global configuration mode. To delete the autonomous system path filter and remove it from the running configuration file, use the **no** form of this command.

ip as-path access-list *acl-number* {**permit**|**deny**} *regex*

no ip as-path access-list *acl-number*

Syntax Description

<i>acl-number</i>	Number from 1 to 500 that specifies the AS-path access-list number.
permit	Permits advertisement based on matching conditions.
deny	Denies advertisement based on matching conditions.
<i>regex</i>	Regular expression that defines the AS-path filter. The autonomous system number is expressed in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXII, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the router bgp command. Note See the “Regular Expressions” appendix in the <i>Cisco IOS Terminal Services Configuration Guide</i> for information about configuring regular expressions.

Command Default No autonomous system path filter is created.

Command Modes Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	This command was modified. The range of values that can be entered for the <i>acl-number</i> argument was increased from 199 to 500 in Cisco IOS Release 12.0(22)S.
12.2(15)T	This command was modified. The range values that can be entered for the <i>acl-number</i> argument was increased from 199 to 500 in Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS Release 15.1(1)SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

Use the **ip as-path access-list** command to configure an autonomous system path filter. You can apply autonomous system path filters to both inbound and outbound BGP paths. Each filter is defined by the regular expression. If the regular expression matches the representation of the autonomous system path of the route as an ASCII string, then the **permit** or **deny** condition applies. The autonomous system path should not contain the local autonomous system number.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain--65538 for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command. When the asdot format is enabled as the default, any regular expressions to match 4-byte autonomous system numbers must be written using the asdot format, or the regular expression match will fail.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot--1.2 for example--as the only configuration format, regular expression match, and output display, with no asplain support.

Examples

In the following example, an autonomous system path access list (number 500) is defined to configure the router to not advertise any path through or from autonomous system 65535 to the 10.20.2.2 neighbor:

```
ip as-path access-list 500 deny _65535_
ip as-path access-list 500 deny ^65535$
router bgp 50000
 neighbor 192.168.1.1 remote-as 65535
 neighbor 10.20.2.2 remote-as 40000
 neighbor 10.20.2.2 filter-list 500 out
end
```

In the following example, the router is configured to deny all updates with private autonomous system paths:

```
ip as-path access-list 1 deny (_64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_)
ip as-path access-list 1 permit .*
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, shows BGP path filtering by neighbor using 4-byte autonomous system numbers in asplain format. Only the routes that pass autonomous system path access list 2 will be sent to 192.168.3.2.

```
ip as-path access-list 2 permit ^65536$
router bgp 65538
 neighbor 192.168.3.2 remote-as 65550
 address-family ipv4 unicast
 neighbor 192.168.3.2 filter-list 2 in
end
```

The following example shows BGP path filtering by neighbor using 4-byte autonomous system numbers in asdot format. The dot notation is the only format for 4-byte autonomous system numbers in Cisco IOS Release 12.0(32)S12, 12.4(24)T, or Cisco IOS XE Release 2.3. This example can also be configured using Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or later releases. after the **bgp asnotation dot** command has been entered to allow matching of 4-byte autonomous system numbers in regular expressions in asdot notation. The dot in the asdot notation is a special

character for regular expressions and a backslash must precede it, as shown in the example. Only the routes that pass autonomous system path access list 2 will be sent to 192.168.3.2.

```
ip as-path access-list 2 permit ^1\.0$
router bgp 1.2
 neighbor 192.168.3.2 remote-as 1.14
 address-family ipv4 unicast
  neighbor 192.168.3.2 filter-list 2 in
end
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
neighbor distribute-list	Distributes BGP neighbor information as specified in an access list.
neighbor filter-list	Applies a filter list to the specified neighbor.
neighbor prefix-list	Applies a prefix list to the specified neighbor.
router bgp	Configures the BGP routing process.

ip bgp fast-external-fallover

To configure per-interface fast external fallover, use the **ip bgp fast-external-fallover** command in interface configuration mode. To remove a per-interface fast external fallover configuration, use the **no** form of this command.

ip bgp fast-external-fallover [permit| deny]

no ip bgp fast-external-fallover [permit| deny]

Syntax Description

permit	(Optional) Allows per-interface fast external fallover.
deny	(Optional) Prevents per-interface fast external fallover.

Command Default

Global fast external fallover is enabled by default in Cisco IOS software.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0ST	This command was introduced.
12.1	This command was integrated into Cisco IOS Release 12.1.
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 **ip bgp fast-external-fallover** command is used to configure per-interface fast external fallover, overriding the global configuration. Entering the **permit** keyword enables fast external fallover. Entering the **deny** keyword disables fast external fallover. Entering the **no** form of this command, returns the router to the global configuration.

Examples

The following example enables per-interface fast-external-fallover on interface Ethernet 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ip bgp fast-external-fallover permit
```


Related Commands

Command	Description
bgp fast-external-fallover	Configures global BGP fast external fall over.

ip bgp-community new-format

To configure BGP to display communities in the format AA:NN (autonomous system:community number/4-byte number), use the **ip bgp-community new-format** command in global configuration mode. To configure BGP to display communities as a 32-bit number, use the **no** form of this command.

ip bgp-community new-format

no ip bgp-community new-format

Syntax Description

This command has no argument or keywords.

Command Default

BGP communities (also when entered in the AA:NN format) are displayed as a 32-bit numbers if this command is not enabled or if the **no** form is entered.

Command Modes

Global configuration

Command History

Release	Modification
12.0	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 **ip bgp-community new-format** command is used to configure the local router to display BGP communities in the AA:NN format to conform with RFC-1997. This command only affects the format in which BGP communities are displayed; it does not affect the community or community exchange. However, expanded IP community lists that match locally configured regular expressions may need to be updated to match on the AA:NN format instead of the 32-bit number.

RFC 1997, BGP Communities Attribute, specifies that a BGP community is made up of two parts that are each 2 bytes long. The first part is the autonomous system number and the second part is a 2-byte number defined by the network operator. For example, according to RFC 1997, an AS number 640100, in hexadecimal, specified in the NN:AA format, is represented in decimal as 100:256 in the AA:NN format.

In Cisco software, you can configure BGP communities in three different formats namely, decimal (NN:AA format), hexadecimal, and AA:NN. BGP community attribute is a numerical value that can be assigned to a specific prefix and advertised to other neighbors. Although the community attribute can be represented in decimal, hexadecimal, or AA:NN, it is still a 32-bit number. For example, you can configure the **set community** command to specify the community 30:20 (AS 30, number 20) in the old and the new formats:

- **set community 30:20**

- **set community** 0x1e0014
- **set community** 1966100

Use the **ip bgp-community new-format** command to change the NN:AA format to AA:NN format, such that the device configuration file and the BGP table displays 30:20.

Examples

In the following example, a router that uses the 32-bit number community format is upgraded to use the AA:NN format:

```
Router(config)# ip bgp-community new-format
```

The following sample output shows how BGP community numbers are displayed when the **ip bgp-community new-format** command is enabled:

```
Router# show ip bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/8, version 4
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to non peer-group peers:
    10.0.33.35
    35
    10.0.33.35 from 10.0.33.35 (192.168.3.3)
      Origin incomplete, metric 10, localpref 100, valid, external
      Community: 30:20
  Local
    0.0.0.0 from 0.0.0.0 (10.0.33.34)
      Origin incomplete, metric 0, localpref 100, weight 32768, valid, sourced, best
```

Related Commands

Command	Description
set community	Configures the BGP community value.
show ip bgp	Displays entries in the BGP routing table.

ip community-list

To configure a BGP community list and to control which routes are permitted or denied based on their community values, use the **ip community-list** command in global configuration mode. To delete the community list, use the **no** form of this command.

Standard Community Lists

ip community-list {*standard*| **standard** *list-name*} {**deny**| **permit**} [*community-number*] [*AA:NN*] [**internet**] [**local-as**] [**no-advertise**] [**no-export**] [**gshut**]

no ip community-list {*standard*| **standard** *list-name*}

Expanded Community Lists

ip community-list {*expanded*| **expanded** *list-name*} {**deny**| **permit**} *regex*

no ip community-list {*expanded*| **expanded** *list-name*}

Syntax Description

<i>standard</i>	Standard community list number from 1 to 99 to identify one or more permit or deny groups of communities.
standard <i>list-name</i>	Configures a named standard community list.
deny	Denies routes that match the specified community or communities.
permit	Permits routes that match the specified community or communities.
<i>community-number</i>	(Optional) 32-bit number from 1 to 4294967200. A single community can be entered or multiple communities can be entered, each separated by a space.

<i>AA :NN</i>	(Optional) Autonomous system number and network number entered in the 4-byte new community format. This value is configured with two 2-byte numbers separated by a colon. A number from 1 to 65535 can be entered for each 2-byte number. A single community can be entered or multiple communities can be entered, each separated by a space.
internet	(Optional) Specifies the Internet community. Routes with this community are advertised to all peers (internal and external).
local-as	(Optional) Specifies the local-as community. Routes with community are advertised to only peers that are part of the local autonomous system or to only peers within a subautonomous system of a confederation. These routes are not advertised to external peers or to other subautonomous systems within a confederation.
no-advertise	(Optional) Specifies the no-advertise community. Routes with this community are not advertised to any peer (internal or external).
no-export	(Optional) Specifies the no-export community. Routes with this community are advertised to only peers in the same autonomous system or to only other subautonomous systems within a confederation. These routes are not advertised to external peers.

gshut	(Optional) Specifies the Graceful Shutdown (GSHUT) community.
<i>expanded</i>	Expanded community list number from 100 to 500 to identify one or more permit or deny groups of communities.
expanded <i>list-name</i>	Configures a named expanded community list.
<i>regex</i>	Regular expression that is used to specify a pattern to match against an input string. Note Regular expressions can be used only with expanded community lists.

Command Default BGP community exchange is not enabled by default.

Command Modes Global configuration (config)

Command History	Release	Modification
	10.3	This command was introduced.
	12.0	This command was modified. The local-as keyword was added.
	12.0(10)S	This command was modified. Named community list support was added.
	12.0(16)ST	This command was modified. Named community list support was introduced.
	12.1(9)E	Named community list support was integrated into Cisco IOS Release 12.1(9)E.
	12.2(8)T	Named community list support was integrated into Cisco IOS Release 12.2(8)T.
	12.0(22)S	This command was modified. The maximum number of expanded community list numbers was increased from 199 to 500.
	12.2(14)S	This command was modified. The maximum number of expanded community list numbers was increased from 199 to 500 and named community list support were integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.2(15)T	This command was modified. The maximum number of expanded community list numbers was increased from 199 to 500.
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.
15.2(2)S	This command was modified. The gshut keyword was added.
Cisco IOS XE Release 3.6S	This command was modified. The gshut keyword was added.
Cisco IOS XE Release 3.7S	This command was implemented on the Cisco ASR 903 router.
15.2(4)S	This command was implemented on the Cisco ASR 7200 router.

Usage Guidelines

The **ip community-list** command is used to filter BGP routes based on one or more community values. BGP community values are configured as a 32-bit number (old format) or as a 4-byte number (new format). The new community format is enabled when the **ip bgp-community new-format** command is entered in global configuration mode. The new community format consists of a 4-byte value. The first two bytes represent the autonomous system number, and the trailing two bytes represent a user-defined network number. Named and numbered community lists are supported.

BGP community exchange is not enabled by default. The exchange of BGP community attributes between BGP peers is enabled on a per-neighbor basis with the **neighbor send-community** command. The BGP community attribute is defined in [RFC 1997](#) and [RFC 1998](#).

The Internet community is applied to all routes or prefixes by default, until any other community value is configured with this command or the **set community** command.

Use a route map to reference a community list and thereby apply policy routing or set values.

Community List Processing

Once a **permit** value has been configured to match a given set of communities, the community list defaults to an implicit deny for all other community values. Unlike an access list, it is feasible for a community list to contain only **deny** statements.

- When multiple communities are configured in the same **ip community-list** statement, a logical AND condition is created. All community values for a route must match the communities in the community list statement to satisfy an AND condition.
- When multiple communities are configured in separate **ip community-list** statements, a logical OR condition is created. The first list that matches a condition is processed.

Standard Community Lists

Standard community lists are used to configure well-known communities and specific community numbers. A maximum of 16 communities can be configured in a standard community list. If you attempt to configure

more than 16 communities, the trailing communities that exceed the limit are not processed or saved to the running configuration file.

Expanded Community Lists

Expanded community lists are used to filter communities using a regular expression. Regular expressions are used to configure patterns to match community attributes. The order for matching using the * or + character is longest construct first. Nested constructs are matched from the outside in. Concatenated constructs are matched beginning at the left side. If a regular expression can match two different parts of an input string, it will match the earliest part first. For more information about configuring regular expressions, see the “Regular Expressions” appendix of the *Terminal Services Configuration Guide*.

Examples

In the following example, a standard community list is configured that permits routes from network 10 in autonomous system 50000:

```
Router(config)# ip community-list 1 permit 50000:10
```

In the following example, a standard community list is configured that permits only routes from peers in the same autonomous system or from subautonomous system peers in the same confederation:

```
Router(config)# ip community-list 1 permit no-export
```

In the following example, a standard community list is configured to deny routes that carry communities from network 40 in autonomous system 65534 and from network 60 in autonomous system 65412. This example shows a logical AND condition; all community values must match in order for the list to be processed.

```
Router(config)# ip community-list 2 deny 65534:40 65412:60
```

In the following example, a named, standard community list is configured that permits all routes within the local autonomous system or permits routes from network 20 in autonomous system 40000. This example shows a logical OR condition; the first match is processed.

```
Router(config)# ip community-list standard RED permit local-as
Router(config)# ip community-list standard RED permit 40000:20
```

In the following example, a standard community list is configured that denies routes with the GSHUT community and permits routes with the local-AS community. This example shows a logical OR condition; the first match is processed.

```
Router(config)# ip community-list 18 deny gshut
Router(config)# ip community-list 18 permit local-as
```

In the following example, an expanded community list is configured that denies routes that carry communities from any private autonomous system:

```
Router(config)# ip community-list 500 deny _64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_
```

In the following example, a named expanded community list is configured that denies routes from network 1 to 99 in autonomous system 50000:

```
Router(config)# ip community-list expanded BLUE deny 50000:[0-9][0-9]_
```

Related Commands

Command	Description
match community	Defines a BGP community that must match the community of a route.
neighbor send-community	Allows BGP community exchange with a neighbor.

Command	Description
neighbor shutdown graceful	Configures the BGP Graceful Shutdown feature.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set community	Sets the BGP communities attribute.
set comm-list delete	Removes communities from the community attribute of an inbound or outbound update.
show ip bgp community	Displays routes that belong to specified BGP communities.
show ip bgp regexp	Displays routes that match a locally configured regular expression.

ip extcommunity-list

To create an extended community list to configure Virtual Private Network (VPN) route filtering, use the **ip extcommunity-list** command in global configuration mode. To delete the extended community list, use the **no** form of this command.

To enter IP Extended community-list configuration mode to create or configure an extended community-list, use the **ip extcommunity-list** command in global configuration mode. To delete the entire extended community list, use the **no** form of this command. To delete a single entry, use the **no** form in IP Extended community-list configuration mode.

Global Configuration Mode CLI

ip extcommunity-list {*expanded-list* [**permit**|**deny**] [*regular-expression*] || **expanded** *list-name* [**permit**|**deny**] [*regular-expression*] || *standard-list* [**permit**|**deny**] [*rt value*] [*soo value*] || **standard** *list-name* [**permit**|**deny**] [*rt value*] [*soo value*] }

no ip extcommunity-list {*expanded-list* | **expanded** *list-name* | *standard-list* | **standard** *list-name* }

ip extcommunity-list {*expanded-list* | **expanded** *list-name* | *standard-list* | **standard** *list-name* }

no ip extcommunity-list {*expanded-list* | **expanded** *list-name* | *s* *tandard-list* | **standard** *list-name* }

Expanded IP Extended Community-List Configuration Mode CLI

[*sequence-number*] {**deny** [*regular-expression*] || **permit** [*regular-expression*] || **resequence** [*starting-sequence*] [*sequence-increment*] }

default {*sequence-number* | **deny** [*regular-expression*] || **permit** [*regular-expression*] || **resequence** [*starting-sequence*] [*sequence-increment*] }

no {*sequence-number* | **deny** [*regular-expression*] || **permit** [*regular-expression*] || **resequence** [*starting-sequence*] [*sequence-increment*] }

Standard IP Extended Community-List Configuration Mode CLI

default {*sequence-number* | **deny** [*rt value*] [*soo value*] || **permit** [*rt value*] [*soo value*] || **resequence** [*starting-sequence*] [*sequence-increment*] }

no {*sequence-number* | **deny** [*rt value*] [*soo value*] || **permit** [*rt value*] [*soo value*] || **resequence** [*starting-sequence*] [*sequence-increment*] }

Syntax Description

<i>expanded-list</i>	An expanded list number from 100 to 500 that identifies one or more permit or deny groups of extended communities.
<i>standard-list</i>	A standard list number from 1 to 99 that identifies one or more permit or deny groups of extended communities.

expanded <i>list-name</i>	Creates an expanded named extended community list and enters IP Extended community-list configuration mode.
standard <i>list-name</i>	Creates a standard named extended community list and enters IP Extended community-list configuration mode.
permit	Permits access for a matching condition. Once a permit value has been configured to match a given set of extended communities, the extended community list defaults to an implicit deny for all other values.
deny	Denies access for a matching condition.
<i>regular-expression</i>	(Optional) An input string pattern to match against.
rt	(Optional) Specifies the route target (RT) extended community attribute. The rt keyword can be configured only with standard extended community lists and not expanded community lists.
soo	(Optional) Specifies the site of origin (SOO) extended community attribute. The soo keyword can be configured only with standard extended community lists and not expanded community lists.
<i>value</i>	Specifies the route target or site of origin extended community value. This value can be entered in one of the following formats: • autonomous-system-number : network-number • ip-address : network-number
<i>sequence-number</i>	(Optional) The sequence number of a named or numbered extended community list. This value can be a number from 1 to 2147483647.
resequence	(Optional) Changes the sequences of extended community list entries to the default sequence numbering or to the specified sequence numbering. Extended community entries are sequenced by ten number increments by default.
<i>starting-sequence</i>	(Optional) Specifies the number for the first entry in an extended community list.
<i>sequence-increment</i>	(Optional) Specifies the increment range for each subsequent extended community entry.

Command Default

Extended community exchange is not enabled by default.

Command Modes

Global configuration (config)

IP Extended community-list configuration (config-extcom-list)

Command History

Release	Modification
12.1	This command was introduced.
12.0(22)S	The maximum number of expanded community list numbers was increased from 199 to 500.
12.2(15)T	The maximum number of expanded community list numbers was increased from 199 to 500.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(25)S	Support for the following was added in Cisco IOS Release 12.2(25)S: • Extended community-list sequencing • IP Extended community configuration mode • Named extended community lists
12.3(11)T	Support for the following was added in Cisco IOS Release 12.3(11)T: • Extended community-list sequencing • IP Extended community configuration mode • Named extended community lists
12.2(27)SBC	This command was integrated into the Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	This command was integrated into the Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.

Release	Modification
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS Release 15.1(1)SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.2(1)E	This command was integrated into the Cisco IOS Release 15.2(1)E.

Usage Guidelines

The **ip extcommunity-list** command is used to configure named or numbered extended community lists. Extended community attributes are used to filter routes for VPN routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs). All of the standard rules of access lists apply to the configuration of extended community lists. The route target (RT) and site of origin (SOO) extended community attributes are supported by the standard range of extended community lists. Extended community list entries start with the number 10 and increment by ten for each subsequent entry when no sequence number is specified, when default behavior is configured, and when an extended community list is resequenced without specifying the first entry number or the increment range for subsequent entries. Regular expressions are supported in expanded extended community lists. For information about configuring regular expressions, see the “Regular Expressions” appendix of the Cisco IOS Terminal Services Configuration Guide.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain--65538 for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot--1.2 for example--as the only configuration format, regular expression match, and output display, with no asplain support.

Route Target Extended Community Attribute

The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.

Site of Origin Extended Community Attribute

The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the provider edge (PE) router learned the route. All routes learned from a particular site must be assigned the same site of origin extended community attribute, regardless if a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO should not be configured for stub sites or sites that are not multihomed.

IP Extended Community-List Configuration Mode

Named and numbered extended community lists can be configured in IP Extended community-list configuration mode. To enter IP Extended community-list configuration mode, enter the **ip extcommunity-list** command with either the **expanded** or **standard** keyword followed by the extended community list name. This configuration mode supports all of the functions that are available in global configuration mode. In addition, you can perform the following operations:

- Configure sequence numbers for extended community list entries
- Resequence existing sequence numbers for extended community list entries
- Configure an extended community list to use default values

Extended Community List Processing

When multiple values are configured in the same extended community list statement, a logical AND condition is created. All extended community values must match to satisfy an AND condition. When multiple values are configured in separate extended community list statements, a logical OR condition is created. The first list that matches a condition is processed.

Examples

Examples

In the following example, an extended community list is configured that permits routes from route target 64512:10 and site of origin 65400:20 and denies routes from route target 65424:30 and site of origin 64524:40. List 1 shows a logical OR condition; the first match is processed. List 2 shows a logical AND condition; all community values must match in order for list 2 to be processed.

```
Router(config)# ip extcommunity-list 1 permit rt 64512:10
Router(config)# ip extcommunity-list 1 permit soo 65400:20
Router(config)# ip extcommunity-list 2
deny rt 65424:30 soo 64524:40
```

Examples

In the following example, an expanded extended community list is configured to deny advertisements from any path through or from autonomous system 65534 from being advertised to the 192.168.1.2 neighbor:

```
Router(config)# ip extcommunity-list 500 deny _65412_
Router(config)# router bgp 50000
Router(config-router)# address-family vpnv4
```

```
Router(config-router-af)# neighbor 172.16.1.1 remote-as 65412
Router(config-router-af)# neighbor 172.16.1.1
  neighbor send-community extended
Router(config-router-af)# neighbor 192.168.1.2 remote-as 65534
Router(config-router-af)# neighbor 192.168.1.2
  neighbor send-community extended
Router(config-router-af)# end
```

Examples

In the following example, a named extended community list is configured that will permit routes only from route target 65505:50. All other routes are implicitly denied.

```
Router(config)# ip extcommunity-list standard NAMED_LIST permit rt 65505:50
```

Examples

In the following example, an expanded named extended community list is configured in IP Extended community-list configuration mode. A list entry is created with a sequence number 10 that will permit a route target or route origin pattern that matches any network number extended community from autonomous system 65412.

```
Router(config)# ip extcommunity-list RED
Router(config-extcom-list)# 10 permit 65412:[0-9][0-9][0-9][0-9][0-9]_
Router(config-extcom-list)# exit
```

Examples

In the following example, the first list entry is resequenced to the number 50 and each subsequent entry is configured to increment by 100:

```
Router(config)# ip extcommunity-list BLUE
Router(config-extcom-list)# resequence 50 100
Router(config-extcom-list)# exit
```

Examples

The following example shows how to filter traffic by creating an extended BGP community list to control outbound routes. In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, extended BGP communities support 4-byte autonomous system numbers in the regular expressions in asplain format. In this task, the router is configured with an extended named community list to specify that the BGP peer at 192.168.1.2 is not sent advertisements about any path through or from the 4-byte autonomous system 65550. The IP extended community-list configuration mode is used, and the ability to resequence entries is shown.

```
Router(config)# ip extcommunity-list expanded DENY65550
Router(config-extcomm-list)# 10 deny _65550_
Router(config-extcomm-list)# 20 deny ^65550 .*
Router(config-extcomm-list)# resequence 50 100
Router(config-extcomm-list)# exit
Router(config)# router bgp 65538
Router(config-router)# network 172.17.1.0 mask 255.255.255.0
```

```
Router(config-router)# neighbor 192.168.3.2 remote-as 65550
Router(config-router)# neighbor 192.168.1.2 remote-as 65536
Router(config-router)# neighbor 192.168.3.2 activate
Router(config-router)# neighbor 192.168.1.2 activate
Router(config-router)# end
Router# show ip extcommunity-list DENY65550
```

In Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, 12.4(24)T, and Cisco IOS XE Release 2.3, or a later releases, extended BGP communities support 4-byte autonomous system numbers in the regular expressions in asdot format. In this task, the router is configured with an extended named community list to specify that the BGP peer at 192.168.1.2 is not sent advertisements about any path

through or from the 4-byte autonomous system 1.14. The IP extended community-list configuration mode is used, and the ability to resequence entries is shown.

```
Router(config)# ip extcommunity-list expanded DENY114
Router(config-extcomm-list)# 10 deny _1\.14_
Router(config-extcomm-list)# 20 deny ^1\.14_.*
Router(config-extcomm-list)# resequence 50 100
Router(config-extcomm-list)# exit
Router(config)# router bgp 1.2
Router(config-router)# network 172.17.1.0 mask 255.255.255.0
Router(config-router)# neighbor 192.168.3.2 remote-as 1.14
Router(config-router)# neighbor 192.168.1.2 remote-as 1.0
Router(config-router)# neighbor 192.168.3.2 activate
Router(config-router)# neighbor 192.168.1.2 activate
Router(config-router)# end
Router# show ip extcommunity-list DENY114
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
export map	Configures an export route map for a VRF.
match extcommunity	Matches a BGP VPN extended community list.
router bgp	Configures the BGP routing process.
set extcommunity	Sets BGP extended community attributes.
show ip extcommunity-list	Displays routes that are permitted by the extended community list.
show route-map	Displays configured route maps.

ip policy-list

To create a Border Gateway Protocol (BGP) policy list, use the **ip policy-list** command in global configuration mode. To remove a policy list, use the **no** form of this command.

ip policy-list *policy-list-name* {**permit**|**deny**}

no ip policy-list *policy-list-name*

Syntax Description

<i>policy-list-name</i>	Name of the configured policy list.
permit	Permits access for matching conditions.
deny	Denies access to matching conditions.

Command Default

This command is not enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into 12.2(15)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

When a policy list is referenced within a route map, all the match statements within the policy list are evaluated and processed. Two or more policy lists can be configured with a route map. Policy- lists configured within a route map are evaluated with AND semantics or OR semantics. A policy list can also coexist with any other preexisting match and set statements that are configured within the same route map but outside of the policy list. When multiple policy lists perform matching within a route map entry, all policy lists match on the incoming attribute only.

Examples

In the following example, a policy list is configured that permits all network prefixes that match AS 1 and metric 10:

```
Router(config)# ip policy-list POLICY-LIST-NAME-1 permit
Router(config-policy-list)# match as-path 1
Router(config-policy-list)# match metric 10
Router(config-policy-list)# end
```

In the following example, a policy list is configured that permits traffic that matches community 20 and metric 10:

```
Router(config)# ip policy-list POLICY-LIST-NAME-2 permit
Router(config-policy-list)# match community 20
Router(config-policy-list)# match metric 10
Router(config-policy-list)# end
```

In the following example, a policy list is configured that denies traffic that matches community 20 and metric 10:

```
Router(config)# ip policy-list POLICY-LIST-NAME-3 deny
Router(config-policy-list)# match community 20
Router(config-policy-list)# match metric 10
Router(config-policy-list)# end
```

Related Commands

Command	Description
match as-path	References a policy list within a route map for evaluation and processing.
show ip policy-list	Displays configured policy lists.
show route-map	Displays configured route maps and information about referenced policy maps.

ip prefix-list

To create a prefix list or to add a prefix-list entry, use the **ip prefix-list** command in global configuration mode. To delete a prefix-list entry, use the **no** form of this command.

ip prefix-list *{list-name [seq number] {deny|permit} network/length [ge ge-length] [le le-length]}* **description** *description* **sequence-number**

no ip prefix-list *{list-name [seq number] [{deny|permit} network/length [ge ge-length] [le le-length]]}* **description** *description* **sequence-number**

Syntax Description

<i>list-name</i>	Configures a name to identify the prefix list. Do not use the word “detail” or “summary” as a list name because they are keywords in the show ip prefix-list command.
seq	(Optional) Applies a sequence number to a prefix-list entry.
<i>number</i>	(Optional) Integer from 1 to 4294967294. If a sequence number is not entered when configuring this command, default sequence numbering is applied to the prefix list. The number 5 is applied to the first prefix entry, and subsequent unnumbered entries are incremented by 5.
deny	Denies access for a matching condition.
permit	Permits access for a matching condition.
<i>network / length</i>	Configures the network address and the length of the network mask in bits. The network number can be any valid IP address or prefix. The bit mask can be a number from 1 to 32.
ge	(Optional) Specifies the lesser value of a range (the “from” portion of the range description) by applying the <i>ge-length</i> argument to the range specified. Note The ge keyword represents the greater than or equal to operator.
<i>ge-length</i>	(Optional) Represents the minimum prefix length to be matched.

le	(Optional) Specifies the greater value of a range (the “to” portion of the range description) by applying the <i>le-length</i> argument to the range specified. Note The le keyword represents the less than or equal to operator.
<i>le-length</i>	(Optional) Represents the maximum prefix length to be matched.
description	(Optional) Configures a descriptive name for the prefix list.
<i>description</i>	(Optional) Descriptive name of the prefix list, from 1 to 80 characters in length.
sequence-number	(Optional) Enables or disables the use of sequence numbers for prefix lists.

Command Default No prefix lists or prefix-list entries are created.

Command Modes Global configuration (config)

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 Use the **ip prefix-list** command to configure IP prefix filtering. Prefix lists are configured with **permit** or **deny** keywords to either permit or deny a prefix based on a matching condition. An implicit deny is applied to traffic that does not match any prefix-list entry.

A prefix-list entry consists of an IP address and a bit mask. The IP address can be for a classful network, a subnet, or a single host route. The bit mask is a number from 1 to 32.

Prefix lists are configured to filter traffic based on a match of an exact prefix length or a match within a range when the **ge** and **le** keywords are used. The **ge** and **le** keywords are used to specify a range of prefix lengths and provide more flexible configuration than using only the *network / length* argument. A prefix list is processed using an exact match when neither the **ge** nor **le** keyword is specified. If only the **ge** value is specified, the range is the value entered for the **ge ge-length** argument to a full 32-bit length. If only the **le** value is specified, the range is from the value entered for the *network / length* argument to the **le le-length** argument. If both the

ge *ge-length* and **le** *le-length* keywords and arguments are entered, the range is between the values used for the *ge-length* and *le-length* arguments.

The following formula shows this behavior:

$$length < \text{ge } ge\text{-length} < \text{le } le\text{-length} \leq 32$$

If the **seq** keyword is configured without a sequence number, the default sequence number is 5. In this scenario, the first prefix-list entry is assigned the number 5 and subsequent prefix list entries increment by 5. For example, the next two entries would have sequence numbers 10 and 15. If a sequence number is entered for the first prefix list entry but not for subsequent entries, the subsequent entry numbers increment by 5. For example, if the first configured sequence number is 3, subsequent entries will be 8, 13, and 18. Default sequence numbers can be suppressed by entering the **no ip prefix-list** command with the **seq** keyword.

Evaluation of a prefix list starts with the lowest sequence number and continues down the list until a match is found. When an IP address match is found, the permit or deny statement is applied to that network and the remainder of the list is not evaluated.



Tip

For best performance, the most frequently processed prefix list statements should be configured with the lowest sequence numbers. The **seq number** keyword and argument can be used for resequencing.

A prefix list is applied to inbound or outbound updates for a specific peer by entering the **neighbor prefix-list** command. Prefix list information and counters are displayed in the output of the **show ip prefix-list** command. Prefix-list counters can be reset by entering the **clear ip prefix-list** command.

Examples

In the following example, a prefix list is configured to deny the default route 0.0.0.0/0:

```
Router(config)# ip prefix-list RED deny 0.0.0.0/0
```

In the following example, a prefix list is configured to permit traffic from the 172.16.1.0/24 subnet:

```
Router(config)# ip prefix-list BLUE permit 172.16.1.0/24
```

In the following example, a prefix list is configured to permit routes from the 10.0.0.0/8 network that have a mask length that is less than or equal to 24 bits:

```
Router(config)# ip prefix-list YELLOW permit 10.0.0.0/8 le 24
```

In the following example, a prefix list is configured to deny routes from the 10.0.0.0/8 network that have a mask length that is greater than or equal to 25 bits:

```
Router(config)# ip prefix-list PINK deny 10.0.0.0/8 ge 25
```

In the following example, a prefix list is configured to permit routes from any network that have a mask length from 8 to 24 bits:

```
Router(config)# ip prefix-list GREEN permit 0.0.0.0/0 ge 8 le 24
```

In the following example, a prefix list is configured to deny any route with any mask length from the 10.0.0.0/8 network:

```
Router(config)# ip prefix-list ORANGE deny 10.0.0.0/8 le 32
```

Related Commands

Command	Description
clear ip prefix-list	Resets the prefix list entry counters.
ip prefix-list description	Adds a text description of a prefix list.
ip prefix-list sequence	Enables or disables default prefix-list sequencing.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
neighbor prefix-list	Filters routes from the specified neighbor using a prefix list.
show ip prefix-list	Displays information about a prefix list or prefix list entries.

ip prefix-list description

To add a text description of a prefix list, use the **ip prefix-list description** command in global configuration mode. To remove the text description, use the **no** form of this command.

ip prefix-list *list-name* **description** *text*

no ip prefix-list *list-name* **description**

Syntax Description

<i>list-name</i>	Identifies the prefix-list that is being described.
<i>text</i>	Adds a text description. Up to 80 characters can be entered.

Command Default

No default behavior or values

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

Use the **ip prefix-list description** command to add a helpful description to an IP prefix list, which you can see in the configuration file and in the **show ip prefix-list** output to remind you what the prefix list is for. The description can be up to 80 characters in length.

Examples

In the following example, a description is added to the prefix list named RED, which indicates that the prefix list is to permit routes from network A:

```
Router(config)# ip prefix-list RED description Permit routes from network A
```

Related Commands

Command	Description
clear ip prefix-list	Resets the prefix list entry counters.

Command	Description
ip prefix-list	Creates an entry in a prefix list.
ip prefix-list sequence	Enables or disables default prefix-list sequencing.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
neighbor prefix-list	Filters routes from the specified neighbor using a prefix list.
show ip prefix-list	Displays information about a prefix list or prefix list entries.

ip prefix-list sequence-number

To enable the generation of default sequence numbers for entries in a prefix list, use the **ip prefix-list sequence-number** command in global configuration mode. To suppress default generation of sequence numbers, use the **no** form of this command.

ip prefix-list sequence-number

no ip prefix-list sequence-number

Syntax Description This command has no arguments or keywords.

Command Default Default sequence numbers are generated when an IP prefix list is configured.

Command Modes Global configuration (config)

Command History	Release	Modification
	12.0	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 The following example suppresses the automatic generation of default sequence numbers for prefix list entries:

```
Router(config)# no ip prefix-list sequence-number
```

Related Commands	Command	Description
	clear ip prefix-list	Resets the prefix list entry counters.
	ip prefix-list	Creates an entry in a prefix list.
	ip prefix-list description	Adds a text description of a prefix list.
	match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.

Command	Description
neighbor prefix-list	Filters routes from the specified neighbor using a prefix list.
show ip prefix-list	Displays information about a prefix list or prefix list entries.

ip verify unicast vrf

To enable Unicast Reverse Path Forwarding (Unicast RPF) verification for a specified VRF, use the **ip verify unicast vrf** command in interface configuration mode. To disable the Unicast RPF check for a VRF, use the **no** form of this command.

ip verify unicast vrf *vrf-name* {**deny**|**permit**}

no ip verify unicast vrf *vrf-name* {**deny**|**permit**}

Syntax Description

<i>vrf-name</i>	Virtual Private Network (VPN) routing and forwarding (VRF) instance name.
deny	Specifies that traffic associated with the specified VRF is dropped after it passes the Unicast RPF verification.
permit	Specifies that traffic associated with the specified VRF is forwarded after it passes the Unicast RPF verification.

Command Default

Unicast RPF verification is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Unicast RPF is configured to verify that the source address is in the Forwarding Information Base (FIB). The **ip verify unicast vrf** command is configured in interface configuration mode and is enabled for each VRF.

This command has **permit** and **deny** keywords that are used to determine if traffic is forwarded or dropped after Unicast RPF verification.

Examples

The following example configures Unicast RPF verification for VRF1 and VRF2. VRF1 traffic is forwarded. VRF2 traffic is dropped.

```
Router(config)# interface Ethernet 0
Router(config-if)# ip verify unicast vrf vrf1 permit
Router(config-if)# ip verify unicast vrf vrf2 deny
Router(config-if)# end
```

Related Commands

Command	Description
import ipv4	Configures an import map to import IPv4 prefixes from the global routing table to a VRF table.
ip vrf	Configures a VRF routing table.
rd	Creates routing and forwarding tables for a VRF.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp vpnv4	Displays VPN address information from the BGP table.
show ip vrf	Displays the set of defined VRFs and associated interfaces.



BGP Commands: M through N

- [match additional-paths advertise-set, page 348](#)
- [match as-path, page 352](#)
- [match community, page 355](#)
- [match extcommunity, page 358](#)
- [match local-preference, page 360](#)
- [match policy-list, page 362](#)
- [match rpki, page 364](#)
- [match source-protocol, page 366](#)
- [maximum-paths eibgp, page 369](#)
- [maximum-paths ibgp, page 372](#)
- [mvpn single-forwarder-selection highest-ip-address, page 376](#)
- [neighbor accept-route-legacy-rt, page 377](#)
- [neighbor activate, page 379](#)
- [neighbor additional-paths, page 383](#)
- [neighbor advertise additional-paths, page 386](#)
- [neighbor advertise best-external, page 389](#)
- [neighbor advertise diverse-path, page 392](#)
- [neighbor advertise-map, page 395](#)
- [neighbor advertisement-interval, page 399](#)
- [neighbor allow-policy, page 401](#)
- [neighbor announce rpki state, page 403](#)
- [neighbor bmp-activate, page 406](#)
- [neighbor capability orf prefix-list, page 408](#)
- [neighbor cluster-id, page 410](#)

- [neighbor default-originate, page 412](#)
- [neighbor description, page 414](#)
- [neighbor disable-connected-check, page 416](#)
- [neighbor distribute-list, page 418](#)
- [neighbor dmzlink-bw, page 422](#)
- [neighbor ebgp-multihop, page 424](#)
- [neighbor fall-over, page 426](#)
- [neighbor filter-list, page 430](#)
- [neighbor ha-mode graceful-restart, page 433](#)
- [neighbor ha-mode sso, page 435](#)
- [neighbor inherit peer-policy, page 437](#)
- [neighbor inherit peer-session, page 439](#)
- [neighbor internal-vpn-client, page 441](#)
- [neighbor local-as, page 443](#)
- [neighbor maximum-prefix \(BGP\), page 450](#)
- [neighbor next-hop-self, page 453](#)
- [neighbor next-hop-unchanged, page 455](#)
- [neighbor password, page 458](#)
- [neighbor path-attribute discard, page 461](#)
- [neighbor path-attribute treat-as-withdraw, page 463](#)
- [neighbor peer-group \(assigning members\), page 465](#)
- [neighbor peer-group \(creating\), page 467](#)
- [neighbor prefix-list, page 470](#)
- [neighbor remote-as, page 474](#)
- [neighbor remove-private-as, page 480](#)
- [neighbor route-map, page 484](#)
- [neighbor route-reflector-client, page 487](#)
- [neighbor route-server-client, page 490](#)
- [neighbor send-community, page 492](#)
- [neighbor shutdown, page 495](#)
- [neighbor slow-peer detection, page 498](#)
- [neighbor slow-peer split-update-group dynamic, page 501](#)
- [neighbor slow-peer split-update-group static, page 504](#)

- [neighbor soft-reconfiguration](#), page 506
- [neighbor soo](#), page 508
- [neighbor suppress-signaling-protocol](#), page 511
- [neighbor timers](#), page 513
- [neighbor translate-update](#), page 515
- [neighbor transport](#), page 518
- [neighbor ttl-security](#), page 522
- [neighbor unsuppress-map](#), page 524
- [neighbor update-source](#), page 526
- [neighbor version](#), page 529
- [neighbor weight](#), page 531
- [network \(BGP and multiprotocol BGP\)](#), page 533
- [network backdoor](#), page 536

match additional-paths advertise-set

To match on paths that are marked (tagged) with a specific path-marking policy, use the **match additional-paths advertise-set** command in route-map configuration mode. To remove the **match additional-paths advertise-set** command from the configuration file, use the **no** form of this command.

match additional-paths advertise-set [*best number*] [*best-range range-start range-end*] [*group-best*] [*all*]
no match additional-paths advertise-set [*best number*] [*best-range range-start range-end*] [*group-best*] [*all*]

Syntax Description

best <i>number</i>	(Optional) Matches on paths that are tagged with best <i>number</i> tag. • The value can be 2 or 3. • The best <i>number</i> keyword and argument are mutually exclusive with the best-range <i>range-start range-end</i> keyword and arguments. That is, the configuration of one disallows the configuration of the other.
best-range <i>range-start</i>	(Optional) Matches on paths that are tagged with best <i>n</i> (this starting number or any number in the range specified). • The <i>range-start</i> value can be 1, 2, or 3. • The best <i>number</i> keyword and argument are mutually exclusive with the best-range <i>range-start range-end</i> keyword and arguments. That is, the configuration of one disallows the configuration of the other.
<i>range-end</i>	(Optional) Matches on paths that are tagged with best <i>n</i> (this ending number or any number in the range specified). • The <i>range-end</i> value can be 1, 2, or 3. • If the <i>range-start</i> equals the <i>range-end</i>, then one specific path (the <i>n</i>th best path) of the network is matched. Otherwise, the best paths in the range are matched.
group-best	(Optional) Matches on paths that are tagged with the group-best tag.

all	(Optional) Matches on paths that are tagged with the all tag.

Command Default No matching is performed on additional path advertise sets.

Command Modes Route-map configuration (config-route-map)

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines Use this command in a route map to filter the advertisement of additional paths. Paths that have the same path marking (tag) as the marking that is configured in the **match additional-paths advertise-set** command match the route map entry (and are permitted or denied). A tag is an advertise-set, as defined in the **bgp additional-paths select** command.

If **match additional-paths advertise-set best number** is configured, any path that has the tag **best number** or a lower number tag matches the route map entry.

You can specify more than one selection policy in one **match additional-paths advertise-set** command; you must specify at least one selection policy if you use this command.

The **best number** keyword and argument are mutually exclusive with the **best-range range-start range-end** keyword and arguments. That is, the configuration of one disallows the configuration of the other. For practical purposes, it is preferable to use **best number** rather than **best-range range-start range-end**.

You can configure only one **match additional-paths advertise-set** command in the route map. If you configure more than one **match additional-paths advertise-set** command, the latest command overwrites the previous **match additional-paths advertise-set** command.

You can optionally specify in the route map one or more **set** commands to set characteristics of a path.

Although you can specify a route map that matches on paths that have marking policies other than the paths you want to advertise, you will typically create a route map that matches on the paths that you want to advertise (specified by the **neighbor advertise additional-paths** command).

Examples In the following example, for every address family, there are one or more eBGP neighbors not shown in the configuration that are sending routes to the local device. The eBGP routes learned from these neighbors are advertised toward the neighbors shown in the configuration, and the path attributes are changed. The example configures that:

- The route map called `add_path1` specifies that all the paths are advertised toward neighbor 192.168.101.15, but any path that is marked with the **best 2** tag will have its metric set to 780 before being sent toward that neighbor.
- The route map called `add_path2` specifies that any path that is marked with the **best 3** tag will have its metric set to 640 and will be advertised toward neighbor 192.168.25.
- The route map called `add_path3` specifies that any path that is marked with the **group-best** tag will have its metric set to 825 and will be advertised toward neighbor 2001:DB8::1045.
- In the IPv6 multicast address family, all paths are candidates to be advertised and will be advertised toward neighbor 2001:DB8::1037.

For the rest of `advertise-set` (not specified in a given route-map), the routes will be denied. If this is not what you want, then you can add another configuration command to permit routes, such as `route-map add_pathX permit 20`, for example.

```
router bgp 1
 neighbor 192.168.101.15 remote-as 1
 neighbor 192.168.101.25 remote-as 1
 neighbor 2001:DB8::1045 remote-as 1
 neighbor 2001:DB8::1037 remote-as 1
!
 address-family ipv4 unicast
  bgp additional-paths send receive
  bgp additional-paths select all best 3 group-best
  neighbor 192.168.101.15 activate
  neighbor 192.168.101.15 route-map add_path1 out
  neighbor 192.168.101.15 advertise additional-paths best 2
 exit-address-family
!
 address-family ipv4 multicast
  bgp additional-paths send receive
  bgp additional-paths select all best 3 group-best
  neighbor 192.168.101.25 activate
  neighbor 192.168.101.25 route-map add_path2 out
  neighbor 192.168.101.25 advertise additional-paths best 3
 exit-address-family
!
 address-family ipv6 unicast
  bgp additional-paths send receive
  bgp additional-paths select group-best
  neighbor 2001:DB8::1045 activate
  neighbor 2001:DB8::1045 route-map add_path3 out
  neighbor 2001:DB8::1045 advertise additional-paths all group-best
 exit-address-family
!
 address-family ipv6 multicast
  bgp additional-paths send receive
  bgp additional-paths select all
  neighbor 2001:DB8::1037 activate
  neighbor 2001:DB8::1037 advertise additional-paths all
 exit-address-family
!
 route-map add_path1 permit 10
  match additional-paths advertise-set best 2
  set metric 780
 route-map add_path1 permit 20
!
 route-map add_path2 permit 10
  match additional-paths advertise-set best 3
  set metric 640
!
 route-map add_path3 permit 10
  match additional-paths advertise-set group-best
  set metric 825
!
```

Related Commands

Command	Description
bgp additional-paths	Configures BGP to send or receive additional paths for all neighbors in the address family.
bgp additional-paths select	Causes the system to calculate BGP additional paths that can be candidates for advertisement in addition to a bestpath.
neighbor advertise additional-paths	Advertises additional paths for a neighbor based on selection.
neighbor route-map	Applies a route map to incoming or outgoing routes.
route-map (IP)	Defines the conditions for policy routing or redistribution.

match as-path

To match a BGP autonomous system path that is specified by an access list, use the **match as-path** command in route-map configuration mode. To remove a path list entry, use the **no** form of this command.

match as-path *path-list-number*

no match as-path *path-list-number*

Syntax Description

<i>path-list-number</i>	Access list that specifies an autonomous system path. An integer from 1 to 199.

Command Default

No matching occurs on an autonomous system path specified by an access list.

Command Modes

Route-map configuration (config-route-map)

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

Use the **ip as-path access-list** command to create an access list that determines which AS path is specified. Then use the **match as-path** command to create a route map based on matching the access list that determined the AS path.

The values set by the combination of the **match as-path** and **set weight** commands override global values. For example, the weights assigned with the **match as-path** and **set weight** route-map configuration commands override the weight assigned using the **neighbor weight** command.

A route map can have several parts. Any route that does not match at least one **match** clause relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route-map section with an explicit match specified.

Examples

The following example configures a route map that matches on the autonomous system path specified by access list 20:

```
route-map IGP2BGP
 match as-path 20
```

Related Commands

Command	Description
ip as-path access-list	Configures an AS path filter using a regular expression.
match community	Matches a BGP community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
neighbor weight	Assigns weight to a neighbor connection.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set as-path	Modifies an autonomous system path for BGP routes.
set automatic-tag	Automatically computes the tag value in a route map configuration.
set community	Sets the BGP communities attribute.

Command	Description
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set next-hop	Specifies the address of the next hop.
set origin (BGP)	Sets the BGP origin code.
set tag (IP)	Sets the value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

match community

To match a Border Gateway Protocol (BGP) community, use the **match community** command in route-map configuration mode. To remove the **match community** command from the configuration file and restore the system to its default condition where the software removes the BGP community list entry, use the **no** form of this command.

match community {*standard-list-number*| *expanded-list-number*| *community-list-name* [**exact**]}

no match community {*standard-list-number*| *expanded-list-number*| *community-list-name* [**exact**]}

Syntax Description

<i>standard-list-number</i>	Specifies a standard community list number from 1 to 99 that identifies one or more permit or deny groups of communities.
<i>expanded-list-number</i>	Specifies an expanded community list number from 100 to 500 that identifies one or more permit or deny groups of communities.
<i>community-list-name</i>	The community list name.
exact	(Optional) Indicates that an exact match is required. All of the communities and only those communities specified must be present.

Command Default

No community list is matched by the route map.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.1	This command was introduced.
12.1(9)E	Named community list support was integrated into Cisco IOS Release 12.1(9)E.
12.2(8)T	Named community list support was integrated into Cisco IOS Release 12.2(8)T.
12.0(22)S	The maximum number of expanded extended community list numbers was changed from 199 to 500 in Cisco IOS Release 12.0(22)S.
12.2(14)S	The maximum number of expanded community lists was changed from 199 to 500 and named community list support were integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.2(15)T	The maximum number of expanded extended community list numbers was changed from 199 to 500 in Cisco IOS Release 12.2(15)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

A route map can have several parts. Any route that does not match at least one **match** command relating to a **route-map** command will be ignored; that is, the route will not be advertised for outbound route maps and will not be accepted for inbound route maps. If you want to modify only some data, you must configure a second route-map section with an explicit match specified.

Matching based on community list number is one of the types of **match** commands applicable to BGP.

Examples

The following example shows that the routes matching community list 1 will have the weight set to 100. Any route that has community 109 will have the weight set to 100.

```
Router(config)# ip community-list 1 permit 109
Router(config)# route-map set_weight
Router(config-route-map)# match community 1
Router(config-route-map)# set weight 100
```

The following example shows that the routes matching community list 1 will have the weight set to 200. Any route that has community 109 alone will have the weight set to 200.

```
Router(config)# ip community-list 1 permit 109
Router(config)# route-map set_weight
Router(config-route-map)# match community
1 exact
Router(config-route-map)# set weight 200
```

In the following example, the routes that match community list LIST_NAME will have the weight set to 100. Any route that has community 101 alone will have the weight set to 100.

```
Router(config)# ip community-list LIST_NAME permit 101
Router(config)# route-map set_weight
Router(config-route-map)# match community LIST_NAME
Router(config-route-map)# set weight 100
```

The following example shows that the routes that match expanded community list 500. Any route that has extended community 1 will have the weight set to 150.

```
Router(config)# ip community-list 500 permit [0-9]*
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match extcommunity 500
Router(config-route-map)# set weight 150
```


Related Commands

Command	Description
ip community-list	Creates a community list for BGP and controls access to it.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
set weight	Specifies the BGP weight for the routing table.

match extcommunity

To match Border Gateway Protocol (BGP) or Enhanced Interior Gateway Routing Protocol (EIGRP) extended community list attributes, use the **match extcommunity** command in route-map configuration mode. To remove the **match extcommunity** command from the configuration file and remove the BGP or EIGRP extended community list attribute entry, use the **no** form of this command.

match extcommunity *extended-community-list-name*

no match extcommunity *extended-community-list-name*

Syntax Description

<i>extended-community-list-name</i>	Name of an extended community list.

Command Default

BGP and EIGRP extended community list attributes are not matched.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.1	This command was introduced.
12.0(22)S	The maximum number of expanded extended community list numbers was changed from 199 to 500 in Cisco IOS Release 12.0(22)S.
12.2(15)T	The maximum number of expanded extended community list numbers was changed from 199 to 500 in Cisco IOS Release 12.2(15)T.
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 integrated into Cisco IOS XE Release 2.1.
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. Support for EIGRP was added.
12.2(33)SRE	This command was modified. Support for EIGRP was added.
Cisco IOS XE Release 2.5	This command was modified. Support for EIGRP was added.
12.2(33)XNE	This command was modified. Support for EIGRP was added.

Usage Guidelines

Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).

The **match extcommunity** command is used to configure match clauses that use extended community attributes in route maps. All of the standard rules of match and set clauses apply to the configuration of extended community attributes.

Examples

The following example shows that the routes that match extended community list 500 will have the weight set to 100. Any route that has extended community 1 will have the weight set to 100.

```
Router(config)# ip extcommunity-list 500 rt 100:2
Router(config-extcomm-list)# exit
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match extcommunity 1
Router(config-route-map)# set weight 100
```

Related Commands

Command	Description
ip extcommunity-list	Creates an extended community list for BGP and controls access to it.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
set extcommunity	Sets BGP extended community attributes.
set weight	Specifies the BGP weight for the routing table.
show ip extcommunity-list	Displays routes that are permitted by the extended community list.
show route-map	Displays configured route maps.

match local-preference

To configure a route map to match routes based on the Border Gateway Protocol (BGP) local-preference attribute, use the **match local-preference** command in route-map configuration mode. To remove the match clause entry from the route map, use the **no** form of this command.

match local-preference *value*

no match local-preference *value*

Syntax Description

<i>value</i>	The local preference value. This argument can be entered as a number from 0 to 4294967295.

Command Default

Cisco IOS software uses a default value of 100 for the local-preference attribute. However, a local-preference value must be entered when configuring a match clause with this command.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.

Usage Guidelines

The **match local-preference** command is used to filter routes based on the value of the local preference attribute. The local-preference attribute is a well-known discretionary attribute that is used to set the preference for an exit point within an autonomous system. The route with the highest local-preference value is preferred by the BGP best path selection process.

Redistributing OER Injected Routes

Optimized Edge Routing (OER) uses a local-preference value of 5000 (default) to move traffic to the preferred exit point in a BGP network (This value can be configured on the OER master controller). The **match local-preference** command can be used to redistribute OER injected routes within an autonomous system that is monitored and controlled by OER.

Examples

The following example configures the route-map name RED to match OER injected routes:

```
Router(config)#
route-map RED permit 10
Router(config-route-map)#
match local-preference 5000
```

Related Commands

Command	Description
bgp default local-preference	Changes the default local-preference value.
route-map (IP)	Defines conditions for redistributing routes.
set local-preference	Applies a local-preference value to routes that pass the match clause.

match policy-list

To configure a route map to evaluate and process a Border Gateway Protocol (BGP) policy list in a route map, use the **match policy-list command** in route-map configuration mode. To remove a path list entry, use the **no** form of this command.

match policy-list *policy-list-name*

no match policy-list *policy-list-name*

Syntax Description

<i>policy-list-name</i>	Name of the policy list to evaluate and process within the route map.

Command Default

This command is not enabled by default.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into 12.2(15)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

When a policy list is referenced within a route map, all the match statements within the policy list are evaluated and processed.

Two or more policy lists can be configured with a route map. Policy lists can be configured within a route map to be evaluated with AND semantics or OR semantics.

Policy lists can also coexist with any other preexisting match and set statements that are configured within the same route map but outside of the policy lists.

When multiple policy lists perform matching within a route map entry, all policy lists match on the incoming attribute only.

Examples

The following configuration example creates a route map that references policy lists and separate match and set clauses in the same configuration:

```
Router(config)# route-map MAP-NAME-1 10
Router(config-route-map)# match ip-address 1
Router(config-route-map)# match policy-list POLICY-LIST-NAME-1
```

```
Router(config-route-map)# set community 10:1
Router(config-route-map)# set local-preference 140
Router(config-route-map)# end
```

The following configuration example creates a route map that references policy lists and separate match and set clauses in the same configuration. This example processes the policy lists named POLICY-LIST-NAME-2 and POLICY-LIST-NAME-3 with OR semantics. A match is required from only one of the policy lists.

```
Router(config)# route-map MAP-NAME-2 10
Router(config-route-map)# match policy-list POLICY-LIST-NAME-2 POLICY-LIST-NAME-3
Router(config-route-map)# set community 10:1
Router(config-route-map)# set local-preference 140
Router(config-route-map)# end
```

Related Commands

Command	Description
ip policy-list	Creates a BGP policy list.
match as-path	References a policy list within a route map for evaluation and processing.
match community	Matches a BGP community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
neighbor weight	Assigns weight to a neighbor connection.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

match rpki

To match Border Gateway Protocol (BGP) routes that have the specified Resource Public Key Infrastructure (RPKI) state, use the **match rpki** command in route-map configuration mode. To remove the **match rpki** command from the route map, use the **no** form of this command.

match rpki {not-found| invalid| valid}

no match rpki {not-found| invalid| valid}

Syntax Description

not-found	Matches on the RPKI state Not Found.
invalid	Matches on the RPKI state Invalid.
valid	Matches on the RPKI state Valid.

Command Default

No RPKI state is matched by the route map.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
XE 3.5S	This command was introduced.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.
15.2(4)S	This command was implemented on the Cisco 7200 series routers.

Usage Guidelines

Use this command to create a custom policy for the treatment of valid, not-found, and invalid prefixes. We recommend that you also use the **bgp bestpath prefix-validate allow-invalid** command when configuring a route map to match on RPKI states.

By default, the router overrides all other preferences to reject routes that are in an invalid state. You must explicitly configure the **bgp bestpath prefix-validate allow-invalid** command if you want to use a route map to do something such as permit invalid prefixes, but with a non-default local preference.

Examples

In the following example, a route map named rtmmap-PEX1-3 sets a local preference of 50 for invalid prefix/AS pairs, 100 for not-found prefix/AS pairs, and 200 for valid prefix/AS pairs. The local preference values are

set for incoming routes from the neighbor at 10.0.102.1. The neighbor is an External Border Gateway Protocol (EBGP) peer.

```
router bgp 65000
 address-family ipv4 unicast
  neighbor 10.0.102.1 route-map rtmap-PEX1-3 in
  bgp bestpath prefix-validate allow-invalid
!
route-map rtmap-PEX1-3 permit 10
 match rpki invalid
 set local-preference 50
!
route-map rtmap-PEX1-3 permit 20
 match rpki not-found
 set local-preference 100
!
route-map rtmap-PEX1-3 permit 30
 match rpki valid
 set local-preference 200
!
route-map rtmap-PEX1-3 permit 40
```

Related Commands

Command	Description
bgp bestpath prefix-validate allow-invalid	Allows invalid prefixes to be used as the bestpath even if valid prefixes are available.
bgp rpki server	Connects to an RPKI server and enables the validation of BGP prefixes based on the AS from which the prefix originates.
neighbor announce rpki state	Sends and receives the RPKI state and prefix/AS pairs to and from an IBGP neighbor.
route-map	Defines the conditions for subjecting prefixes to policies.
show ip bgp rpki servers	Displays the current state of communication with RPKI servers.
show ip bgp rpki table	Displays the currently cached list of networks and associated AS numbers received from the RPKI server.

match source-protocol

To match Enhanced Interior Gateway Routing Protocol (EIGRP) external routes based on a source protocol and autonomous system number, use the **match source-protocol** command in route-map configuration mode. To remove the protocol to be matched, use the **no** form of this command.

match source-protocol *source-protocol* [*autonomous-system-number*]

no match source-protocol *source-protocol* [*autonomous-system-number*]

Syntax Description

<i>source-protocol</i>	Protocol to match. The valid keywords are bgp , connected , eigrp , isis , ospf , rip , and static . There is no default.
<i>autonomous-system-number</i>	(Optional) Autonomous system number. This argument is not applicable to the connected, rip, and static keywords. The range is from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXII, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the router bgp command.

Command Default

EIGRP external routes are not matched on a source protocol and autonomous system number.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

This command may not be useful with a redistribution operation that employs route maps because redistribution usually requires the configuration of a source protocol and an autonomous system value in order to redistribute. In many cases, it is more useful to configure a route map that includes matching the route type based on the source protocol and autonomous system using the **distribute-list** command for EIGRP.

Examples

The following example shows how to configure a route map to match a source protocol of BGP and an autonomous system 45000. When the match clause is true, the tag value of the destination routing protocol is set to 5. The route map is used to distribute incoming packets for an EIGRP process.

```
route-map metric_source
 match source-protocol bgp 45000
 set tag 5
!
router eigrp 1
 network 172.16.0.0
 distribute-list route-map metric_source in
```

The following example shows how to configure a route map to match a source protocol of BGP and a 4-byte autonomous system of 65538 in asplain format. When the match clause is true, the tag value of the destination routing protocol is set to 5. The route map is used to distribute incoming packets for an EIGRP process. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or a later release.

```
route-map metric_source
 match source-protocol bgp 65538
 set tag 5
!
router eigrp 1
 network 172.16.0.0
 distribute-list route-map metric_source in
```

The following example shows how to configure a route map to match a source protocol of BGP and a 4-byte autonomous system of 1.2 in asdot format. When the match clause is true, the tag value of the destination routing protocol is set to 5. The route map is used to distribute incoming packets for an EIGRP process. This example requires Cisco IOS Release 12.0(32)S12, 12.4(24)T, or Cisco IOS XE Release 2.3 where asdot notation is the only format for 4-byte autonomous system numbers. This configuration can also be performed using Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or a later release.

```
route-map metric_source
 match source-protocol bgp 1.2
 set tag 5
!
router eigrp 1
 network 172.16.0.0
 distribute-list route-map metric_source in
```

Related Commands

Command	Description
distribute-list	Filters networks received in updates.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
router bgp	Configures the BGP routing process.
set as-path	Modifies an autonomous system path for BGP routes.
set tag (IP)	Sets a tag value of the destination routing protocol.

maximum-paths eibgp

To enable multipath load sharing among external Border Gateway Protocol (eBGP) and internal BGP (iBGP) routes, use the **maximum-paths eibgp** command in address family configuration mode. To disable multipath load sharing for eBGP and iBGP routes, use the **no** form of this command.

maximum-paths eibgp *number-of-paths* [**import** *number-of-import-paths*]

no maximum-paths eibgp *number-of-paths* [**import** *number-of-import-paths*]

Syntax Description

<i>number-of-paths</i>	Number of routes to install into the routing table. See the “Usage Guidelines” section for the number of paths that can be configured with this argument.
import <i>number-of-import-paths</i>	(Optional) Specifies the number of redundant paths that can be configured as backup multipaths for a virtual routing and forwarding (VRF) table. This keyword can be configured only under a VRF instance in address family configuration mode. Note We recommend that this keyword is enabled only when needed and that the number of import paths be kept to the minimum (typically, not more than two paths). For more information, see the “Usage Guidelines” section of this command page.

Command Default

BGP, by default, will install only one best path in the routing table.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.0(25)S	This command was modified. The import keyword was added.
12.3(2)T	This command was modified. The maximum number of parallel routes was increased from 6 to 16.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was modified. The import keyword was replaced by the import path selection and import path limit commands.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
Cisco IOS XE 3.10S	This command was modified. The functionality to configure the command on non-VRF address families was added.
15.3(3)S	This command was modified. The functionality to configure the command on non-VRF address families was added.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

Usage Guidelines

The **maximum-paths eibgp** command is used to enable BGP multipath load sharing in a Multiprotocol Label Switching (MPLS) VPN using eBGP and iBGP routes. You can configure this command under VRF and non-VRF address families. The number of multipaths is configured separately for each VRF.

The number of paths that can be configured is determined by the version of Cisco IOS software as shown in the following list:

- Cisco IOS Release 12.0S-based software: 8 paths
- Cisco IOS Release 12.3T, 12.4, 12.4T, and 15.0-based software: 16 paths
- Cisco IOS Release 12.2S-based software: 32 paths

The **maximum-paths eibgp** command cannot be configured with the **maximum-paths** or **maximum-paths ibgp** command because the **maximum-paths eibgp** command is a superset of these commands.



Note

The configuration of this command does not override the existing outbound routing policy.

Configuring VRF Import Paths

A VRF will import only one path (best path) per prefix from the source VRF table, unless the prefix is exported with a different route target. If the best path goes down, the destination will not be reachable until the next import event occurs, and then a new best path will be imported into the VRF table. The import event runs every 15 seconds by default.

The **import** keyword allows the network operator to configure the VRF table to accept multiple redundant paths in addition to the best path. An import path is a redundant path, and it can have a next hop that matches an installed multipath. This keyword should be used when multiple paths with identical next hops are available to ensure optimal convergence times. A typical application of this keyword is to configure redundant paths in a network that has multiple route reflectors for redundancy.

The maximum number of import paths that can be configured in Cisco IOS Release 12.2SY-based software is 16.

**Note**

Configuring redundant paths with the **import** keyword can increase CPU and memory utilization significantly, especially in a network where there are many prefixes to learn and a large number of configured VRFs. We recommend that this keyword be configured only as necessary and that the minimum number of redundant paths be configured (typically, not more than two).

In Cisco IOS Releases 15.0(1)M and 12.2(33)SRE, and in later releases, the **import** keyword was replaced by the **import path selection** and **import path limit** commands. If the **import** keyword is configured, the configuration is converted to the new commands, as show in the following example:

```
Device(config-router-af)# maximum-paths eibgp import 3
```

```
%NOTE: Import option has been deprecated.
```

```
%      Converting to 'import path selection all; import path limit 3'.
```

Examples

In the following example, the router is configured to install six eBGP or iBGP routes into the VRF routing table:

```
Device(config)# router bgp 64496
Router(config-router)# address-family ipv4 vrf vrf-1
Router(config-router-af)# maximum-paths eibgp 6
```

The following example shows how to configure this command on a non-VRF address family.

```
Device(config)# router bgp 64498
Device(config-router)# address-family ipv4 unicast
Device(config-router-af)# maximum-paths eibgp 4
```

Related Commands

Command	Description
import path limit	Specifies the maximum number of BGP paths, per VRF importing net, that can be imported from an exporting net.
import path selection	Specifies the BGP import-path selection policy for a VRF instance.
maximum-paths	Controls the maximum number of parallel routes an IP routing protocol can support.
maximum-paths ibgp	Configures the number of equal-cost or unequal-cost routes that BGP will install in the routing table.
show ip bgp	Displays information about entries in the BGP routing table.
show ip bgp vpnv4	Displays VPNv4 address information from the BGP table entries in the BGP routing table.

maximum-paths ibgp

To control the maximum number of parallel internal Border Gateway Protocol (iBGP) routes that can be installed in a routing table, use the **maximum-paths ibgp** command in router or address family configuration mode. To restore the default value, use the **no** form of this command.

Router Configuration Mode

maximum-paths ibgp *number-of-paths*

no maximum-paths ibgp *number-of-paths*

Under VRF in Address Family Configuration Mode

maximum-paths ibgp {*number-of-paths* [**import** *number-of-import-paths*]} **unequal-cost** *number-of-import-paths*}

no maximum-paths ibgp {*number-of-paths* [**import** *number-of-import-paths*]} **unequal-cost** *number-of-import-paths*}

Syntax Description

<i>number-of-paths</i>	Number of routes to install to the routing table. See the “Usage Guidelines” section for the number of paths that can be configured with this argument.
import <i>number-of-import-paths</i>	(Optional) Specifies the number of redundant paths that can be configured as backup multipaths for a virtual routing and forwarding (VRF) instance. This keyword can be configured only under a VRF in address family configuration mode. Note We recommend that this keyword is enabled only where needed and that the number of import paths be kept to the minimum (typically, not more than two paths). For more information, see the related note in the “Usage Guidelines” section of this command page.
unequal-cost <i>number-of-import-paths</i>	Specifies the number of unequal-cost routes to install in the routing table. See the “Usage Guidelines” section for the number of paths that can be configured. This keyword can be configured only under a VRF instance in address family configuration mode.

Command Default

BGP, by default, will install only one best path in the routing table.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(25)S	This command was modified. The import keyword was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.3	This command was modified. The import keyword was added.
12.3(2)T	This command was modified. The maximum number of parallel routes was increased from 6 to 16.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S for use in IPv6.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was modified. The import keyword was replaced by the import path selection and import path limit commands.
12.2(33)SRE	This command was modified. The import keyword was replaced by the import path selection and import path limit commands.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.

Usage Guidelines

The **maximum-paths ibgp** command is used to configure equal-cost or unequal-cost multipath load sharing for iBGP peering sessions. In order for a route to be installed as a multipath in the BGP routing table, the route cannot have a next hop that is the same as another route that is already installed. The BGP routing process will still advertise a best path to iBGP peers when iBGP multipath load sharing is configured. For equal-cost routes, the path from the neighbor with the lowest router ID is advertised as the best path.

To configure BGP equal-cost multipath load sharing, all path attributes must be the same. The path attributes include weight, local preference, autonomous system path (entire attribute and not just the length), origin code, Multi Exit Discriminator (MED), and Interior Gateway Protocol (IGP) distance.

The number of paths that can be configured is determined by the version of Cisco IOS software as shown in the following list:

- Cisco IOS Release 12.0S-based software: 8 paths

- Cisco IOS Release 12.3T, 12.4, 12.4T, and 15.0-based software: 16 paths
- Cisco IOS Release 12.2S-based software: 32 paths

**Note**

In IPv6, the **maximum-paths ibgp** command does not work for prefixes learned from iBGP neighbors that have been configured to distribute a Multiprotocol Label Switching (MPLS) label with its IPv6 prefix advertisements. If multiple routes exist for such prefixes, all of them are inserted into the Routing Information Base (RIB) when the **maximum-paths ibgp** command is configured, but only one is used and no load balancing occurs between equal-cost paths. The **maximum-paths ibgp** command works with 6PE only in Cisco IOS Release 12.2(25)S and subsequent 12.2S releases.

Configuring VRF Import Paths

A VRF will import only one path (the best path) per prefix from the source VRF table, unless the prefix is exported with a different route target. If the best path goes down, the destination will not be reachable until the next import event occurs, and then a new best path will be imported into the VRF table. The import event runs every 15 seconds by default.

The **import** keyword allows the network operator to configure the VRF table to accept multiple redundant paths in addition to the best path. An import path is a redundant path, and it can have a next hop that matches an installed multipath. This keyword should be used when multiple paths with identical next hops are available to ensure optimal convergence times. A typical application of this keyword is to configure redundant paths in a network that has multiple route reflectors for redundancy.

The maximum number of import paths that can be configured in Cisco IOS Release 12.2SY-based software is 16.

**Note**

Configuring redundant paths with the **import** keyword can increase CPU and memory utilization significantly, especially in a network where there are many prefixes to learn and a large number of configured VRFs. It is recommended that this keyword be configured only as necessary and that the minimum number of redundant paths be configured (typically, not more than two).

In Cisco IOS Releases 15.0(1)M and 12.2(33)SRE, and in later releases, the **import** keyword was replaced by the **import path selection** and **import path limit** commands. If the **import** keyword is configured, the configuration is converted to the new commands, as show in the following example:

```
Router(config-router-af) # maximum-paths ibgp import 3

%NOTE: Import option has been deprecated.
%      Converting to 'import path selection all; import path limit 3'.
```

Examples

The following example configuration installs three parallel iBGP paths in a non-MPLS topology:

```
Router(config) # router bgp 100
Router(config-router) # maximum-paths ibgp 3
```

The following example configuration installs three parallel iBGP paths in an MPLS Virtual Private Network (VPN) topology:

```
Router(config) # router bgp 100
Router(config-router) # address-family ipv4 unicast vrf vrf-A
Router(config-route-af) # maximum-paths ibgp 3
```

The following example configuration installs two parallel routes in the VRF table:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf vrf-B
Router(config-router-af)# maximum-paths ibgp 2 import 2
Router(config-router-af)# end
```

The following example configuration installs two parallel routes in the VRF table:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv4 vrf vrf-C
Router(config-router-af)# maximum-paths ibgp import 2
Router(config-router-af)# end
```

Related Commands

Command	Description
import path limit	Specifies the maximum number of BGP paths, per VRF importing net, that can be imported from an exporting net.
import path selection	Specifies the BGP import path selection policy for a specific VRF instance.
maximum-paths	Controls the maximum number of parallel routes an IP routing protocol can support.
maximum-paths ibgp	Configures the number of equal-cost or unequal-cost routes that BGP will install in the routing table.
show ip bgp	Displays entries in the BGP routing table.
show ip bgp vpnv4	Displays VPNv4 address information from the BGP table entries in the BGP routing table.

mvpn single-forwarder-selection highest-ip-address

To configure the Border Gateway Protocol (BGP) Multicast VPN (MVPN) Upstream Multicast Hop (UMH) chosen via the highest ip address, use the **mvpn single-forwarder-selection highest-ip-address** command in address family configuration mode.

To disable the BGP MVPN hop, use the **no** form of this command.

mvpn single-forwarder-selection highest-ip-address

no mvpn single-forwarder-selection highest-ip-address

Command Default

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Release 3.10S	This command was introduced.

Usage Guidelines

BGP uses the Upstream Multicast Hop (UMH) algorithm to select Reverse Path Forwarding (RPF). To configure a UMH, the BGP neighbors must be activated under the appropriate address-family. By default, single path selection by BGP VPN is based on the BGP best path algorithm.

Examples

The following example shows how to configure a BGP MVPN UMH on the device:

```
Device(config)# configure terminal
Device(config)# router bgp 100
Device(config-router)# address-family ipv4 vrf test
Device(config-router-af)# mvpn single-forwarder-selection highest-ip-address
```

Related Commands

Command	Description
address-family mvpn	Enter address family configuration mode to configure a routing session using MVPN address information.
show bgp mvpn	Display entries in the BGP routing table for MVPN sessions.

neighbor accept-route-legacy-rt

To create Route Target Constrain (RTC) from the VPN prefix received from a legacy route target (RT) peer with special communities, use the **neighbor accept-route-legacy-rt** command in address family configuration mode. To remove the RT, use the **no** form of this command.

neighbor {*ip-address*|*peer-group-name*|*ipv6-address*} **accept-route-legacy-rt**

no neighbor {*ip-address*|*peer-group-name*|*ipv6-address*} **accept-route-legacy-rt**

Syntax Description

<i>ip-address</i>	IPv4 address for advertising the best external path.
<i>peer-group-name</i>	Name of the Boarder Gateway Protocol (BGP) peer group.
<i>ipv6-address</i>	IPv6 address for advertising the best external path.

Command Default

No legacy RT is configured.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use this command when you are configuring the BGP—RTC for Legacy PE feature.

The **neighbor accept-route-legacy-rt** command is configured on the route reflector (RR). RRs identify routes from legacy provider edge (PE) devices for retrieving RT membership information and filter VPN routes to legacy PE devices. The RR creates the RT filter list for each legacy client by collecting the entire set of route targets.

Examples

In the following example, the neighbor at 10.1.1.1 is configured as legacy RT:

```
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# address-family vpnv4 unicast
Device(config-router-af)# neighbor 10.1.1.1 activate
Device(config-router-af)# neighbor 10.1.1.1 accept-route-legacy-rt
Device(config-router-af)# exit address-family
```

Related Commands

Command	Description
address-family rtfilter unicast	Enables RTC with a BGP peer.
neighbor default-originate	Allows a BGP speaker (the local router) to send the default route 0:0:0:0 to a neighbor for use as a default route.
router bgp	Configures the BGP routing process.

neighbor activate

To enable the exchange of information with a Border Gateway Protocol (BGP) neighbor, use the **neighbor activate** command in address family configuration mode or router configuration mode. To disable the exchange of an address with a BGP neighbor, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name* | *ipv6-address* %} **activate**

no neighbor {*ip-address* | *peer-group-name* | *ipv6-address* %} **activate**

Syntax Description

<i>ip-address</i>	IP address of the neighboring router.
<i>peer-group-name</i>	Name of the BGP peer group.
<i>ipv6-address</i>	IPv6 address of the BGP neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.

Command Default

The exchange of addresses with BGP neighbors is enabled for the IPv4 address family. Enabling address exchange for all other address families is disabled.



Note

Address exchange for address family IPv4 is enabled by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-activate** command before configuring the **neighbor remote-as** command, or you disable address exchange for address family IPv4 with a specific neighbor by using the **no neighbor activate** command.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
11.0	This command was introduced.
12.0(5)T	Support for address family configuration mode and the IPv4 address family was added.
12.2(2)T	The <i>ipv6-address</i> argument and support for the IPv6 address family were added.

Release	Modification
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
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(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The % keyword was added
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 introduced on Cisco ASR 1000 Series Routers.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command to advertise address information in the form of an IP or IPv6 prefix. The address prefix information is known as Network Layer Reachability Information (NLRI) in BGP.

The % keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.



Note

The use of the **no** form of the **neighbor activate** command will remove all configurations associated with the neighbor both inside and outside address family configuration mode. This command is not the same as the **neighbor shutdown** command, and you should not use this command to disconnect a BGP adjacency.

Examples

The following example shows how to enable address exchange for address family vpnv4 for all neighbors in the BGP peer group named PEPEER and for the neighbor 10.0.0.44:

```
Router(config)# address-family vpnv4
Router(config-router-af)# neighbor PEPEER activate
Router(config-router-af)# neighbor 10.0.0.44 activate
Router(config-router-af)# exit-address-family
```

Examples

The following example shows how to enable address exchange for address family IPv4 unicast for all neighbors in the BGP peer group named group1 and for the BGP neighbor 172.16.1.1:

```
Device(config)# address-family ipv4 unicast
Device(config-router-af)# neighbor group1 activate
Device(config-router-af)# neighbor 172.16.1.1 activate
```


Examples

The following example shows how to enable address exchange for address family IPv6 for all neighbors in the BGP peer group named group2 and for the BGP neighbor 7000::2:

```
Device(config)# address-family ipv6
Device(config-router-af)# neighbor group2 activate
Device(config-router-af)# neighbor 7000::2 activate
```

The following example shows that the **no** command will remove all configurations associated with a neighbor both inside and outside the address family configuration mode. The first set of commands shows the configuration for a specific neighbor.

```
Device(config)# router bgp 64496
Device(config-router)# bgp log neighbor changes
Device(config-router)# neighbor 10.0.0.1 remote-as 64497
Device(config-router)# neighbor 10.0.0.1 update-source Loopback0
Device(config-router)# address-family ipv4
Device(config-router-af)# no synchronization
Device(config-router-af)# no neighbor 10.0.0.1 activate
Device(config-router-af)# no auto-summary
Device(config-router-af)# exit-address-family
Device(config-router)# address-family vpnv4
Device(config-router-af)# neighbor 10.0.0.1 activate
Device(config-router-af)# neighbor 10.0.0.1 send-community extended
Device(config-router-af)# exit-address-family
Device(config-router)# address-family ipv4 vrf vrf1
Device(config-router-af)# no synchronization
Device(config-router-af)# redistribute connected
Device(config-router-af)# neighbor 192.168.1.4 remote-as 100
Device(config-router-af)# neighbor 192.168.1.4 version 4
Device(config-router-af)# neighbor 192.168.1.4 activate
Device(config-router-af)# neighbor 192.168.1.4 weight 200
Device(config-router-af)# neighbor 192.168.1.4 prefix-list test out
Device(config-router-af)# exit-address-family
```

The following example shows the router configuration after the use of the **no** command.

```
Device(config)# router bgp 64496
Device(config-router)# address-family ipv4 vrf vrf1
Device(config-router-af)# no neighbor 192.168.1.4 activate
01:01:19: %BGP_SESSION-5-ADJCHANGE: neighbor 192.168.1.4 IPv4 Unicast vpn vrf vrf1 topology
base removed from session Neighbor deleted
01:01:19: %BGP-5-ADJCHANGE: neighbor 192.168.1.4 vpn vrf vrf1 Down Neighbor deleted
Device(config-router-af)# do show running-config | begin router bgp

router bgp 64496
bgp log-neighbor-changes
neighbor 10.0.0.1 remote-as 64496
neighbor 10.0.0.1 update-source Loopback0
!
address-family ipv4
  no synchronization
  no neighbor 10.0.0.1 activate
  no auto-summary
exit-address-family
!
address-family vpnv4
  neighbor 10.0.0.1 activate
  neighbor 10.0.0.1 send-community extended
exit-address-family
!
address-family ipv4 vrf vrf1
  no synchronization
  redistribute connected
exit-address-family
```

This example shows the router configuration when the neighbor is reactivated.

```
Device(config)# router bgp 64496
Device(config-router)# address-family ipv4 vrf vrf1
Device(config-router-af)# neighbor 192.168.1.4 activate
01:02:26: %BGP-5-ADJCHANGE: neighbor 192.168.1.4 vpn vrf vrf1 Up
Device(config-router-af)# do show running-config | begin router bgp

router bgp 64496
  bgp log-neighbor-changes
  neighbor 10.0.0.1 remote-as 64496
  neighbor 10.0.0.1 update-source Loopback0
  !
  address-family ipv4
    no synchronization
    no neighbor 10.0.0.1 activate
    no auto-summary
  exit-address-family
  !
  address-family vpnv4
    neighbor 10.0.0.1 activate
    neighbor 10.0.0.1 send-community extended
  exit-address-family
  !
  address-family ipv4 vrf vrf1
    no synchronization
    redistribute connected
    neighbor 192.168.1.4 remote-as 100
    neighbor 192.168.1.4 version 4
    neighbor 192.168.1.4 activate
  exit-address-family
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes.
exit-address-family	Exits from the address family submode.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.

neighbor additional-paths

To configure the local router with the ability to send and receive additional path information for a neighbor or peer group, use the **neighbor additional-paths** command in address family configuration mode. To remove the per-neighbor or per-peer group configuration of the sending and receiving of additional paths, use the **no** form of the command.

neighbor {*ip-address*|*ipv6-address*|*peer-group-name*} **additional-paths** {**send** [**receive**]|**receive**|**disable**}
no neighbor {*ip-address*|*ipv6-address*|*peer-group-name*} **additional-paths** {**send** [**receive**]|**receive**}

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>ipv6-address</i>	IPv6 address of the neighbor.
<i>peer-group-name</i>	Name of the peer group of peers.
send	(Optional) Specifies that the local device can send additional paths for the specified neighbor or peer group.
receive	(Optional) Specifies that the local device can receive additional paths for the specified neighbor or peer group.
disable	(Optional) Overrides template or address family configurations that enable the sending or receiving of additional paths. The disable keyword cannot be used with the send or receive keyword.

Command Default

Additional path capability per neighbor is not configured.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines

Use this command to allow the negotiation of the BGP Additional Paths send and receive capabilities for a specific neighbor or peer group. The ability to send and receive additional paths is negotiated between two BGP neighbors during session establishment.

The **bgp additional-paths {send [receive] | receive}** command controls whether the local device can send or receive additional paths to and from all neighbors within an address family. If the **neighbor additional-paths** command is configured, its send and receive configurations for that neighbor or peer group override the configuration for the address family or for a template.

To override template or address family configurations that enable the sending or receiving of additional paths, use the **neighbor additional-paths disable** command.

To remove the per-neighbor or per-peer group configuration of the sending and receiving of additional paths, use the **no neighbor additional-paths** command. That neighbor will then follow the policy of a peer-template (if it belongs to one) or follow the address family additional path configuration for sending and receiving.

Examples

In the following example, additional paths can be sent and received for the specified neighbor:

```
router bgp 65000
 address-family ipv4 unicast
  neighbor 192.168.1.2 additional-paths send receive
```

In the following example, the **no** form of the command configures that additional paths cannot be sent for the specified neighbor. Because the receive capability was previously configured for that neighbor, the receive capability remains in effect. Note that the **no neighbor 192.168.1.2 additional-paths send** command does not NVGEN (it is not shown in the configuration file. The display would indicate "additional-paths receive".)

```
router bgp 65000
 address-family ipv4 unicast
  neighbor 192.168.1.2 additional-paths send receive
  no neighbor 192.168.1.2 additional-paths send
```

In the following example, additional paths can be sent and received for the address family, but the specified neighbor is disabled from sending or receiving additional paths:

```
router bgp 65000
 address-family ipv4 unicast
  bgp additional-paths send receive
  neighbor 192.168.4.6 additional-paths disable
```

In the following example, the send and receive capability of the neighbor overrides the receive-only capability of the address family:

```
router bgp 65000
 address-family ipv6 multicast
  bgp additional-paths receive
  bgp additional-paths select group-best
  neighbor 2001:DB8::1037 additional-paths send receive
  neighbor 2001:DB8::1037 advertise additional-paths group-best
!
```

Related Commands

Command	Description
additional-paths	Uses a policy template to configure BGP to send or receive additional paths.
advertise additional-paths	Advertises additional paths for a BGP peer policy template based on selection.

Command	Description
bgp additional-paths	Configures the send and receive capabilities of additional path information for the address family.
bgp additional-paths select (additional paths)	Selects the types of additional paths that are calculated and available as candidates for advertisement.
neighbor advertise additional-paths	Advertises additional paths for a neighbor based on selection.

neighbor advertise additional-paths

To advertise additional paths for a neighbor based on selection, use the **neighbor advertise additional-paths** command in address family configuration mode. To prevent the advertisement of additional paths for a neighbor based on selection, use the **no** form of the command.

neighbor {*ip-address*|*ipv6-address*|*peer-group-name*} **advertise additional-paths** [*best number*] [*group-best*] [*all*]

no neighbor {*ip-address*|*ipv6-address*|*peer-group-name*} **advertise additional-paths** [*best number*] [*group-best*] [*all*]

Syntax Description

<i>ip-address</i>	IP address of the neighbor for which to advertise additional paths.
<i>ipv6-address</i>	IPv6 address of the neighbor for which to advertise additional paths.
<i>peer-group-name</i>	Name of the peer group of peers for which to advertise additional paths.
best number	(Optional) Advertises the paths tagged with the best 2 or best 3 tag as the best paths. The <i>number</i> value can be 2 or 3.
group-best	(Optional) Advertises the paths tagged with the group-best tag.
all	(Optional) Advertises the paths tagged with the all tag.

Command Default

Additional paths are not advertised for a neighbor.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines

Use this command to specify the neighbor for which additional paths are advertised. You can advertise additional paths based on any combination of the selection methods, but you must choose at least one selection method if you use this command. Otherwise, only the bestpath is advertised.

Examples

In the following example, for every address family, there are one or more eBGP neighbors not shown in the configuration that are sending routes to the local device. The eBGP routes learned from these neighbors are advertised toward the neighbors shown in the configuration, and the path attributes are changed. The example configures that:

- The route map called `add_path1` specifies that all the paths are advertised toward neighbor 192.168.101.15, but any path that is marked with the **best 2** tag will have its metric set to 780 before being sent toward that neighbor.
- The route map called `add_path2` specifies that any path that is marked with **best 3** will have its metric set to 640 and will be advertised toward neighbor 192.168.101.25.
- The route map called `add_path3` specifies that any path that is marked with **group-best** will have its metric set to 825 and will be advertised toward neighbor 2001:DB8::1045.
- In the IPv6 multicast address family, all paths are candidates to be advertised and will be advertised toward neighbor 2001:DB8::1037.

```
router bgp 1
 neighbor 192.168.101.15 remote-as 1
 neighbor 192.168.101.25 remote-as 1
 neighbor fec0::1045 remote-as 1
 neighbor fec0::1037 remote-as 1
!
 address-family ipv4 unicast
  bgp additional-paths send receive
  bgp additional-paths select all best 3 group-best
  neighbor 192.168.101.15 activate
  neighbor 192.168.101.15 route-map add_path1 out
  neighbor 192.168.101.15 advertise additional-paths best 2
 exit-address-family
!
 address-family ipv4 multicast
  bgp additional-paths send receive
  bgp additional-paths select all best 3 group-best
  neighbor 192.168.101.25 activate
  neighbor 192.168.101.25 route-map add_path2 out
  neighbor 192.168.101.25 advertise additional-paths best 3
 exit-address-family
!
 address-family ipv6 unicast
  bgp additional-paths send receive
  bgp additional-paths select group-best
  neighbor 2001:DB8::1045 activate
  neighbor 2001:DB8::1045 route-map add_path3 out
  neighbor 2001:DB8::1045 advertise additional-paths group-best
 exit-address-family
!
 address-family ipv6 multicast
  bgp additional-paths send receive
  bgp additional-paths select all
  neighbor 2001:DB8::1037 activate
  neighbor 2001:DB8::1037 advertise additional-paths all
 exit-address-family
!
 route-map add_path1 permit 10
  match additional-paths advertise-set best 2
```

neighbor advertise additional-paths

```

set metric 780
route-map add_path1 permit 20
!
route-map add_path2 permit 10
match additional-paths advertise-set best 3
set metric 640
!
route-map add_path3 permit 10
match additional-paths advertise-set group-best
set metric 825
!
```

Related Commands

Command	Description
additional-paths	Uses a policy template to configure BGP to send or receive additional paths.
advertise additional-paths	Advertises additional paths for a BGP peer policy template based on selection.
bgp additional-paths	Configures the send and receive capabilities of additional path information for the address family.
bgp additional-paths select (additional paths)	Specifies the selection methods for calculating additional paths.
neighbor additional-paths	Negotiates the send and receive capability of additional paths per neighbor.

neighbor advertise best-external

To specify that a neighbor receive the advertisement of the best external path, use the **neighbor advertise best-external** command in address family configuration mode. To remove the designation, use the **no** form of this command.

neighbor {*ip-address*|*ipv6-address*|*peer-group-name*|*policy-template-name*} **advertise best-external**
no neighbor {*ip-address*|*ipv6-address*|*peer-group-name*|*policy-template-name*} **advertise best-external**

Syntax Description

<i>ip-address</i>	Advertises the best external path to this IPv4 neighbor.
<i>ipv6-address</i>	Advertises the best external path to this IPv6 neighbor.
<i>peer-group-name</i>	Advertises the best external path to this peer group.
<i>policy-template-name</i>	Advertises the best external path to neighbors described by the policy template.

Command Default

This command is disabled by default; the Border Gateway Protocol (BGP) best path is advertised to neighbors.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

By default, the BGP best path is advertised to a peer. However, if the BGP Diverse Path feature is configured, you can use this command to specify that the best external path is advertised to the peer also.

This command does not enable the BGP Best External feature or the BGP Diverse Path feature. The **bgp additional-paths select best-external** command must be configured before the **neighbor advertise best-external** command can be configured. If the **neighbor advertise best-external** command is configured, but the **bgp additional-paths select best-external** command is not configured, an error message is generated.

This command can be configured for nonclient Internal Border Gateway Protocol (IBGP) peers only. It can be configured at the PE, ASBR, or route reflector. When it is configured at a route reflector, the best-external functionality is inter-cluster, best-external functionality.

When the **neighbor advertise best-external** command is configured:

- At the PE:
 - If the **bgp additional-paths select best-external** command (the new style command) is used to calculate the best external path, the best external path is advertised.
 - If the **bgp advertise-best-external** command (the old style command) is already present, the **neighbor advertise best-external** command cannot be configured and an error message is generated.
- At the route reflector:
 - The route reflector advertises the best internal path to nonclient IBGP peers only when the overall best path is a path learned from another cluster.

This command cannot be configured on a route reflector toward its clients; it can be configured only for nonclient route reflectors.

Examples

In the following example, the neighbor at 10.1.1.1 is configured to receive the advertisement of the best-external path:

```
router bgp 1
 neighbor 10.1.1.1 remote-as 1
 address-family ipv4 unicast
 neighbor 10.1.1.1 activate
 maximum-paths ibgp 4
 bgp bestpath igp-metric ignore
 bgp additional-paths select best-external
 bgp additional-paths install
 neighbor 10.1.1.1 advertise best-external
```

Related Commands

Command	Description
bgp additional-paths select best-external	Specifies that the system calculate a second BGP best path among those received from external neighbors.
bgp advertise-best-external	Enables BGP to calculate an external route as the best backup path for a given address family, to install it into the RIB and Cisco Express Forwarding, and to advertise the best external path to its neighbors.
bgp bestpath igp-metric ignore	Specifies that the system ignore the IGP metric during best path selection.
maximum-paths ebgp	Configures multipath load sharing for EBGp and IBGP routes.
maximum-paths ibgp	Controls the maximum number of parallel IBGP routes that can be installed in a routing table.

neighbor advertise diverse-path

To specify that an additional path (a backup path or multipath or both) is advertised to a peer in addition to the best path, use the **neighbor advertise diverse-path** command in address family configuration mode. To remove the designation, use the **no** form of this command.

neighbor {*ip-address*|*ipv6-address*|*peer-group-name*|*policy-template-name*} **advertise diverse-path** {**backup** [**mpath**]|**mpath**}

no neighbor {*ip-address*|*ipv6-address*|*peer-group-name*|*policy-template-name*} **advertise diverse-path** {**backup** [**mpath**]|**mpath**}

Syntax Description

<i>ip-address</i>	Advertises a diverse path to this IPv4 neighbor.
<i>ipv6-address</i>	Advertises a diverse path to this IPv6 neighbor.
<i>peer-group-name</i>	Advertises a diverse path to this peer group.
<i>policy-template-name</i>	Advertises a diverse path to neighbors described by the policy template?
backup	(Optional) Advertises the backup path. If backup is specified, but there is no backup path, the best path is advertised.
mpath	(Optional) Advertises the multipath, which is the second best path. If mpath is specified, but there is no multipath, the best path is advertised. If both backup and mpath are specified, the multipath is advertised.

Command Default

This command is disabled by default; the Border Gateway Protocol (BGP) best path is advertised to neighbors.

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

By default, the BGP best path is advertised to a peer. However, if the BGP Diverse Path feature is configured, you can use this command to specify that the backup path or multipath (or both) is advertised to the peer also. This command is not supported for VRFs.

This command does not enable the BGP Diverse Path feature. If this command is configured, but the BGP Diverse Path feature is not configured (by one of the commands in the Related Commands table), a warning message is generated.

If any of the Related Commands is configured, but there is no multipath or backup path (no additional path), then the specified neighbor will receive the best path in advertisements.

Neighbors for which this command is not specified will receive the best path in advertisements.

This command can be configured for route reflector clients only (because the BGP Diverse Path feature applies within an autonomous system (AS) and within a single cluster).

If the **bgp additional-paths select backup** command was configured and is subsequently removed from the configuration before the **neighbor advertise diverse-path backup** command is removed, then the specified neighbor will receive the best path in advertisements.

**Note**

If the old style command for BGP PIC or Best External is already configured (**bgp additional-paths install** or **bgp advertise-best-external**), the **neighbor advertise diverse-path** command cannot be configured; an error message is generated.

Either the **backup** keyword or the **mpath** keyword is required; both keywords can be specified.

Examples

In the following example, the neighbor at 10.1.1.1 will receive an advertisement for a backup path in addition to the bestpath:

```
router bgp 1
 neighbor 10.1.1.1 remote-as 1
 address-family ipv4 unicast
 neighbor 10.1.1.1 activate
 maximum-paths ibgp 4
 bgp bestpath igp-metric ignore
 bgp additional-paths select backup
 bgp additional-paths install
 neighbor 10.1.1.1 advertise diverse-path backup
```

Related Commands

Command	Description
bgp additional-paths install	Enables BGP to calculate a backup path for a given address and to install it into the RIB and CEF.
bgp additional-paths select backup	Specifies that the system calculate a second BGP best path as a backup path.
maximum-paths ebgp	Configures multipath load sharing for EBGp and IBGP routes.

Command	Description
maximum-paths ibgp	Controls the maximum number of parallel IBGP routes that can be installed in a routing table.

neighbor advertise-map

To advertise the routes in the BGP table matching the configured route-map, use the **neighbor advertise-map** command in router configuration mode. To disable route advertisement, use the **no** form of this command.

neighbor {*ipv4-address* | *ipv6-address*} **advertise-map** *map-name* {**exist-map** *map-name* | **non-exist-map** *map-name*} [**check-all-paths**]

no neighbor {*ipv4-address* | *ipv6-address*} **advertise-map** *map-name* {**exist-map** *map-name* | **non-exist-map** *map-name*} [**check-all-paths**]

Syntax Description

<i>ip-address</i>	Specifies the IPv4 address of the router that should receive conditional advertisements.
<i>ipv6-address</i>	Specifies the IPv6 address of the router that should receive conditional advertisements.
advertise-map <i>map-name</i>	Specifies the name of the route map that will be advertised if the conditions of the exist map or non-exist map are met.
exist-map <i>map-name</i>	Specifies the name of the exist-map that is compared with the routes in the BGP table to determine whether the advertise-map route is advertised or not.
non-exist-map <i>map-name</i>	Specifies the name of the non-exist-map that is compared with the routes in the BGP table to determine whether the advertise-map route is advertised or not.
check-all-paths	(Optional) Enables checking of all paths by the exist-map with a prefix in the BGP table.

Command Default

No default behavior or values.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
11.1CC	This command was introduced.
11.2	This command was integrated into Cisco IOS Release 11.2.
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.
15.3(2)S	This command was integrated into Cisco IOS Release 15.3(2)S.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.
15.0(02)SG	This command was integrated into Cisco IOS Release 15.0(02)SG. The check-all-paths keyword was introduced.

Usage Guidelines

Use the **neighbor advertise-map** command to conditionally advertise selected routes. The routes (prefixes) that will be conditionally advertised are defined in two route maps: an advertise map and either an exist map or non-exist map.

- The route map associated with the exist map or non-exist map specifies the prefix that the BGP speaker will track.
- The route map associated with the advertise map specifies the prefix that will be advertised to the specified neighbor when the condition is met.

If an exist map is configured, the condition is met when the prefix exists in both the advertise map and the exist map.

If a non-exist map is configured, the condition is met when the prefix exists in the advertise map, but does not exist in the non-exist map.

If the condition is not met, the route is withdrawn and conditional advertisement does not occur. All routes that may be dynamically advertised or not advertised need to exist in the BGP routing table for conditional advertisement to occur.

Examples

The following router configuration example configures BGP to check all

```
router bgp 5
address-family ipv4 unicast
neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
```

The following address family configuration example configures BGP to conditionally advertise a prefix to the 10.1.1.1 neighbor using a non-exist map. If the prefix exists in MAP3 but not MAP4, the condition is met and the prefix is advertised.

```
router bgp 5
address-family ipv4 unicast
neighbor 10.1.1.1 advertise-map MAP3 non-exist-map MAP4
```

The following peer group configuration example configures BGP to check all paths against the prefix to the BGP neighbor:

```
router bgp 5
address-family ipv4
redistribute static
```



```
neighbor route1 send-community both
neighbor route1 advertise-map MAP1 exist-map MAP2 check-all-paths
```

The following is sample output from the **show ip bgp** command where all paths are checked in the BGP table:

Device# **show ip bgp**

```
BGP table version is 12, local router ID is 192.168.10.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
*> 0.0.0.0           0.0.0.0              0         32768 i
*> 1.0.0.0/32        0.0.0.0              0         32768 ?
*> 192.168.10.1/8    0.0.0.0              0         32768 i
r> 192.168.20.1/8    192.168.20.2         0          0 65200 1 2 3 4 5 ?
r> 192.168.30.1/8    192.168.30.2         0          0 65200 ?
* 192.168.50.1       192.168.20.2         0          0 65200 1 2 3 4 5 ?
*>                   192.168.30.2         0          0 65200 ?
```

The following is sample output from the **show ip bgp advertised-routes** command to check the routes advertised for the BGP neighbors.

Device# **show ip bgp neighbors 192.168.20.2 advertised-routes**

```
BGP table version is 12, local router ID is 192.168.10.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
   Network          Next Hop          Metric LocPrf Weight Path
*> 0.0.0.0           0.0.0.0              0         32768 i
*> 167.84.96.5/32    0.0.0.0              0         32768 i
```

Total number of prefixes 2



Note

In the example above, 0.0.0.0 is the default network path that is advertised for the BGP neighbor 192.168.20.2.

The following debug logs indicate the prefix that matches the advertised exist-map after checking all paths from the BGP table.

```
*Sep 26 23:13:00.723: BGP(0): 192.168.20.2 0.0.0.0/0 matches advertise map MAP1,
state: Advertise
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.

Command	Description
address-family ipv6	Places router in address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

neighbor advertisement-interval

To set the minimum route advertisement interval (MRAI) between the sending of BGP routing updates, use the **neighbor advertisement-interval** command in address family or router configuration mode. To restore the default value, use the **no** form of this command.

neighbor {*ip-address*|*peer-group-name*} **advertisement-interval** *seconds*

no neighbor {*ip-address*|*peer-group-name*} **advertisement-interval** *seconds*

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>seconds</i>	Time (in seconds) is specified by an integer ranging from 0 to 600.

Command Default

eBGP sessions not in a VRF: 30 seconds

eBGP sessions in a VRF: 0 seconds

iBGP sessions: 0 seconds

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.3	This command was introduced.
12.0(7)T	Address family configuration mode 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.
12.4T, 12.2SB, 12.2SE, 12.2SG, 12.2SR, 12.2SX, Cisco IOS XE 2.1	This command was modified. The default value for eBGP sessions in a VRF and for iBGP sessions changed from .5 seconds to 0 seconds.

Usage Guidelines

When the MRAI is equal to 0 seconds, BGP routing updates are sent as soon as the BGP routing table changes.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

The following router configuration mode example sets the minimum time between sending BGP routing updates to 10 seconds:

```
router bgp 5
 neighbor 10.4.4.4 advertisement-interval 10
```

The following address family configuration mode example sets the minimum time between sending BGP routing updates to 10 seconds:

```
router bgp 5
 address-family ipv4 unicast
 neighbor 10.4.4.4 advertisement-interval 10
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
neighbor peer-group (creating)	Creates a BGP peer group.

neighbor allow-policy

To allow a route reflector to be configured to change iBGP attributes (policies) in updates for an iBGP session that has the iBGP Local-AS feature configured, use the **neighbor allow-policy** command in router or address family configuration mode. To disable the functionality, use the **no** form of this command.

neighbor {*ip-address*|*ipv6-address*|*peer-group*} **allow-policy**

no neighbor {*ip-address*|*ipv6-address*|*peer-group*} **allow-policy**

Syntax Description

<i>ip-address</i>	IPv4 address of the iBGP neighbor.
<i>ipv6-address</i>	IPv6 address of the iBGP neighbor.
<i>peer-group</i>	Name of a BGP peer group.

Command Default

A route reflector does not change iBGP policies in updates.

Command Modes

Router configuration (config-router)
Address family configuration (config-router-af)

Command History

Release	Modification
15.3(2)S	This command was introduced.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

This command is intended to be used when migrating or merging autonomous systems. Typically, a route reflector (RR) would not change iBGP attributes in updates to a peer. In a scenario where a network administrator is merging autonomous systems, the **neighbor allow-policy** command provides flexibility by allowing the administrator to configure the route reflector to change iBGP policies (by configuring a route map). The RR would have the **neighbor remote-as** command and the **neighbor local-as** command specify the same AS, thus enabling the iBGP Local-AS feature.

This command can be used in iIPv4, IPv6, VPNv4, or VPNv6 address family configuration mode.

Examples

The following example configures a route reflector in AS 4000 to treat BGP sessions with the neighbor in AS 2500 as iBGP sessions. That is, iBGP attributes (LOCAL_PREF, ORIGINATOR_ID, CLUSTER_ID, and CLUSTER_LIST) will not be dropped from routes in advertisements to and from the neighbor; the attributes will be preserved. AS 2500 will be prepended to the AS_PATH attribute in all routes to and from

the neighbor. Additionally, the **neighbor allow-policy** command enables the RR to be configured with a route map that changes iBGP policies.

```
router bgp 4000
 neighbor 192.168.1.1 remote-as 2500
 neighbor 192.168.1.1 local-as 2500
 neighbor 192.168.1.1 route-reflector-client
 address-family vpnv4
   neighbor 192.168.1.1 allow-policy
!
 address-family vpnv6
   neighbor 192.168.1.1 allow-policy
```

Related Commands

Command	Description
neighbor local-as	Customizes the AS_PATH attribute for routes received from an eBGP neighbor or enables the iBGP Local-AS feature.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
show ip bgp vpnv4 all neighbors	Displays information about VPNv4 sessions.
show ip bgp vpnv4 all update-group	Displays information about VPNv4 update groups.

neighbor announce rpki state

To cause the router to send the Resource Public Key Infrastructure (RPKI) state with prefixes to its Internal Border Gateway Protocol (IBGP) neighbor in the Border Gateway Protocol (BGP) extended community attribute, and to also receive the RPKI state with prefixes from that neighbor, use the **neighbor announce rpki state** command in router configuration mode or IPv4 unicast or IPv6 unicast address family configuration mode. To stop the router from sending and receiving the RPKI state, use the **no** form of this command.

neighbor {*ipv4-address*|*ipv6-address*} **announce rpki state**

no neighbor {*ipv4-address*|*ipv6-address*} **announce rpki state**

Syntax Description

<i>ipv4-address</i>	IPv4 address of the IBGP neighbor that will receive the prefixes and associated RPKI state, and from which the router will receive prefixes and the associated RPKI state.
<i>ipv6-address</i>	IPv6 address of the IBGP neighbor that will receive the prefixes and associated RPKI state, and from which the router will receive prefixes and the associated RPKI state.

Command Default

No RPKI state is announced to or received from IBGP neighbors.

Command Modes

Router configuration (config-router)

IPv4 unicast or IPv6 unicast address family configuration (config-router-af)

Command History

Release	Modification
XE 3.5S	This command was introduced.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.
15.2(4)S	This command was implemented on the Cisco 7200 series routers.

Usage Guidelines

Use this command if it is more convenient for the router to send the RPKI state to a neighbor than it is to configure the neighbor with the BGP—Origin AS Validation feature. Thus, the neighbor is spared from having to connect to an RPKI server. This command works in both directions. That is, the specified neighbor can send and receive the RPKI state. If this command is not configured, the local router ignores the extended community attribute if the neighbor sends it.

The extended community attribute announced is 0x4300 0x0000 (four bytes indicating the RPKI state). The four bytes indicating the state will be treated as a 32-bit unsigned integer having one of the following values:

- 0 indicating Valid
- 1 indicating Not Found
- 2 indicating Invalid

If this command is configured, upon receiving a route with the extended community attribute attached from an IBGP peer, the router assigns the route the corresponding validation state.

This attribute will not be sent to External Border Gateway Protocol (EBGP) neighbors, even if they are configured to allow sending of the attribute.

The following behaviors also apply to this command:

- The **neighbor announce rpki state** command is possible only if the router is configured to send extended communities to that neighbor on that address family.
- The **neighbor announce rpki state** command is completely independent of whether RPKI is configured for the address family.
- Once the **neighbor announce rpki state** command or the **bgp rpki server** command is configured for an address family, the router starts doing RPKI validation for every path in that address family.
- The enabling and disabling of the **neighbor announce rpki state** command causes neighbors to be split into their own update groups based on whether this portion of their configuration is identical.
- If the **neighbor announce rpki state** command is not configured, the router will save the RPKI state received from other routers, but will only use it if at least one other neighbor in the address family is configured with the **neighbor announce rpki state** command or if the topology is otherwise enabled for the use of RPKI.
- If the **neighbor send-community extended** or **neighbor send-community both** command is removed from the configuration, the **neighbor announce rpki state** configuration is also removed.
- On route reflectors (RRs), networks that include an RPKI state extended community, but that come from neighbors for which the **neighbor announce rpki state** command is not configured, will be advertised to other RR clients, as long as those clients are capable of receiving an extended community.
- If a network has an RPKI state extended community and is received by an RR from a neighbor for which the **neighbor announce rpki state** command is configured, then it will be reflected to all RR clients that are configured to accept extended communities, regardless of whether the **neighbor announce rpki state** command is configured for those other RR clients.
- A **neighbor announce rpki state** command can be used in a peer policy template, and it is inherited.
- If a **neighbor announce rpki state** command is used in a peer policy template, it must be in the same template as the **send-community extended** command. The **neighbor announce rpki state** command and the **send-community extended** command must come from the same template or be configured for the same neighbor.

Examples

The following example causes the router to send prefixes and the RPKI state to the specified neighbor and also to receive prefixes and the RPKI state from the neighbor:

```
router bgp 65000
```



```
neighbor 192.168.2.2 remote-as 65000
address-family ipv4 unicast
neighbor 192.168.2.2 send-community extended
neighbor 192.168.2.2 announce rpki state
```

Related Commands

Command	Description
bgp rpki server	Connects to an RPKI server and enables the validation of BGP prefixes based on the AS from which the prefix originates.
clear ip bgp rpki server	Closes the TCP connection to the specified RPKI server, purges SOVC records downloaded from that server, renegotiates the connection, and redownloads SOVC records.
show ip bgp rpki servers	Displays the current state of communication with RPKI servers.
show ip bgp rpki table	Displays the currently cached list of networks and associated AS numbers received from the RPKI server.

neighbor bmp-activate

To activate the BGP Monitoring Protocol (BMP) monitoring for a BGP neighbor, use the **neighbor bmp-activate** command in router configuration mode. To deactivate the BMP monitoring for a BGP neighbor, use the **no** form of this command.

neighbor {*ipv4-addr* | *neighbor-tag* | *ipv6-addr*} **bmp-activate** {**all** | **server** *server-number-1* [**server** *server-number-2* ... [**server** *server-number-n*]]}

no neighbor {*ipv4-addr* | *neighbor-tag* | *ipv6-addr*} **bmp-activate**

Syntax Description

<i>ipv4-addr</i>	Specifies the IPv4 address for each BGP neighbor.
<i>neighbor-tag</i>	Specifies a name or tag for each BGP neighbor.
<i>ipv6-addr</i>	Specifies the IPv6 address for each BGP neighbor.
all	Activates BMP monitoring on all BGP BMP servers.
server <i>server-number-n</i>	Activates BMP monitoring on a specific BGP BMP server. The value of <i>n</i> ranges from 1 to 4. You can randomly specify any server number to activate BMP monitoring on it. Optionally, you can activate BMP monitoring on the other servers after you configure the first one.

Command Default

BMP monitoring is not activated on the BMP servers for BGP BMP neighbors.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

The **neighbor bmp-activate** command is only used to activate BMP monitoring on the BGP BMP servers for the BGP BMP neighbors. Only after you activate BMP monitoring, you can configure a BMP server and its parameters using the **bmp** command, which also enables the BMP server configuration commands to configure specific servers. Use the **show ip bgp bmp** command to display the configuration of the BMP servers and neighbors and the connectivity between them.

Examples

The following example shows how to activate BMP on a neighbor with IP address 10.1.1.1, which is monitored by BMP servers (in this case, server 1 and 2):

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# neighbor 10.1.1.1 bmp-activate server 1 server 2
Device(config-router)# end
```

The following example shows how to configure initial refresh delay of 30 seconds for BGP neighbors on which BMP is activated using the **neighbor bmp-activate** command:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp initial-refresh delay 30
Device(config-router)# end
```

The following is sample output from the **show ip bgp bmp neighbors** command, which shows the status of 10 peers configured for a BGP BMP neighbor monitored by BMP server 1 and 2:

```
Device# show ip bgp bmp server neighbors
```

```
Number of BMP neighbors configured: 10
BMP Refresh not in progress, refresh not scheduled
Initial Refresh Delay configured, refresh value 30s
BMP buffer size configured, buffer size 2048 MB, buffer size bytes used 0 MB
```

Neighbor	PriQ	MsgQ	CfgSvr#	ActSvr#	RM Sent
30.1.1.1	0	0	1 2	1 2	16
2001:DB8::2001	0	0	1 2	1 2	15
40.1.1.1	0	0	1 2	1 2	26
2001:DB8::2002	0	0	1 2	1 2	15
50.1.1.1	0	0	1 2	1 2	16
60.1.1.1	0	0	1 2	1 2	26
2001:DB8::2002	0	0	1	1	9
70.1.1.1	0	0	2	2	12
Neighbor	PriQ	MsgQ	CfgSvr#	ActSvr#	RM Sent
80.1.1.1	0	0	1	1	10
2001:DB8::2002	0	0	1 2	1 2	16

Related Commands

Command	Description
bmp	Configures BMP parameters on BGP BMP servers.
show ip bgp bmp	Displays information about BMP servers and neighbors.

neighbor capability orf prefix-list

To advertise outbound route filter (ORF) capabilities to a peer router, use the **neighbor capability orf prefix-list** command in address family or router configuration mode. To disable ORF capabilities, use the **no** form of this command.

neighbor *ip-address* **capability orf prefix-list** [*receive*| *send*| *both*]

no neighbor *ip-address* **capability orf prefix-list** [*receive*| *send*| *both*]

Syntax Description

<i>ip-address</i>	The IP address of the neighbor router.
receive	(Optional) Enables the ORF prefix list capability in receive mode.
send	(Optional) Enables the ORF prefix list capability in send mode.
both	(Optional) Enables the ORF prefix list capability in both receive and send modes.

Command Default

No ORF capabilities are advertised to a peer router.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
12.0(11)ST	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
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

The **neighbor capability orf prefix-list** command is used to reduce the number of BGP prefixes that a BGP speaker sends or receives from a peer router based on prefix filtering.

In most configurations, this command will be used to advertise both send and receive ORF capabilities with the **both** keyword. However, this feature can be configured in one direction between two routers with one router configured to send ORF capabilities and another router configured to receive ORF capabilities from the first router.

Examples

The following examples configure routers to advertise ORF send or receive capabilities to BGP neighbors.

Examples

The following example creates an outbound route filter and configures Router-A (10.1.1.1) to advertise the filter to Router-B (172.16.1.2). An IP prefix list named FILTER is created to specify the 192.168.1.0/24 subnet for outbound route filtering. The ORF send capability is configured on Router-A so that Router-A can advertise the outbound route filter to Router-B.

```
ip prefix-list FILTER seq 10 permit 192.168.1.0/24
!
router bgp 100
 address-family ipv4 unicast
  neighbor 172.16.1.2 remote-as 200
  neighbor 172.16.1.2 ebgp-multihop
  neighbor 172.16.1.2 capability orf prefix-list send
  neighbor 172.16.1.2 prefix-list FILTER in
exit
```

Examples

The following example configures Router-B to advertise the ORF receive capability to Router-A. Router-B will install the outbound route filter, defined in the FILTER prefix list, after ORF capabilities have been exchanged. An inbound soft reset is initiated on Router-B at the end of this configuration to activate the outbound route filter.

```
router bgp 200
 address-family ipv4 unicast
  neighbor 10.1.1.1 remote-as 100
  neighbor 10.1.1.1 ebgp-multihop 255
  neighbor 10.1.1.1 capability orf prefix-list receive
end
clear ip bgp 10.1.1.1 in prefix-filter
```

**Note**

The inbound soft refresh must be initiated with the **clear ip bgp** command in order for the BGP ORF feature to function.

Related Commands

Command	Description
neighbor prefix-list	Distributes BGP neighbor information as specified in a prefix list.

neighbor cluster-id

To set the cluster ID of a client, use the **neighbor cluster-id** command in router configuration mode. To remove the cluster ID, use the **no** form of this command.

neighbor {*ip-address*|*ipv6-address*} **cluster-id** *cluster-id*

no neighbor {*ip-address*|*ipv6-address*} **cluster-id** *cluster-id*

Syntax Description

<i>ip-address</i>	IPv4 address of the BGP-speaking neighbor.
<i>ipv6-address</i>	IPv6 address of the BGP-speaking neighbor.
<i>cluster-id</i>	Cluster ID of this neighbor; maximum of 4 bytes. • The cluster ID can be in dotted decimal (such as 192.168.7.4) or decimal format (such as 23). • A cluster ID that is configured in decimal format (such as 23) will appear in a configuration file in dotted decimal format (such as 0.0.0.23). The decimal format does not appear in the configuration file.

Command Default

The local router ID of the route reflector is used as the cluster ID if no cluster ID is specified.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

This command is used on an IBGP neighbor (usually a route reflector) to configure cluster IDs on a per-neighbor basis. Configuring a cluster ID per neighbor allows the following functions:

- The loop-prevention mechanism is modified such that when receiving a route, the RR discards the route if the RR's global cluster ID or any of the cluster IDs assigned to any of the clients is contained in the CLUSTER_LIST of the route.
- The network administrator can disable client-to-client reflection on a per-neighbor basis if, for example, clients are fully meshed and hence there is no need to reflect the routes between them. (See the example below.)

If you change a cluster ID for a neighbor, BGP automatically does an inbound soft refresh and an outbound soft refresh for all iBGP peers.

**Note**

Even if cluster IDs are configured on a per-neighbor basis, the global cluster ID for the route reflector can still be configured as usual; use the **bgp cluster-id** command.

Examples

In the following example, the neighbor/client at 192.168.1.24 is configured with cluster ID 0.0.0.4:

```
router bgp 60000
 neighbor 192.168.1.24 cluster-id 0.0.0.4
```

In the following example, intracustomer client-to-client route reflection is disabled for the cluster that has cluster ID 0.0.0.5:

```
router bgp 60000
 neighbor 192.168.1.24 cluster-id 192.168.0.115
 no bgp client-to-client reflection intra-cluster cluster-id 0.0.0.5
```

Related Commands

Command	Description
bgp client-to-client reflection intra-cluster	Enables or restores intra-cluster client-to-client route reflection to clients for the specified clusters.
bgp cluster-id	Sets the global cluster ID on a route reflector for a route reflector cluster.
neighbor route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
show ip bgp cluster-ids	Displays cluster IDs, how many neighbors are in each cluster, and whether client-to-client route reflection is disabled for each cluster.
show ip bgp neighbor	Displays the cluster ID of the neighbor.
show ip bgp template peer-session	Displays the cluster ID assigned to the template.
show ip bgp update-group	Displays the cluster ID assigned to the update group.

neighbor default-originate

To allow a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route, use the **neighbor default-originate** command in address family or router configuration mode. To send no route as a default, use the **no** form of this command.

neighbor {*ip-address*|*peer-group-name*} **default-originate** [**route-map** *map-name*]

no neighbor {*ip-address*|*peer-group-name*} **default-originate** [**route-map** *map-name*]

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
route-map <i>map-name</i>	(Optional) Name of the route map. The route map allows route 0.0.0.0 to be injected conditionally.

Command Default

No default route is sent to the neighbor.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
11.0	This command was introduced.
12.0	Modifications were added to permit extended access lists.
12.0(7)T	Address family configuration mode 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.

Usage Guidelines

This command does not require the presence of 0.0.0.0 in the local router. When used with a route map, the default route 0.0.0.0 is injected if the route map contains a **match ip address** clause and there is a route that matches the IP access list exactly. The route map can contain other match clauses also.

You can use standard or extended access lists with the **neighbor default-originate** command.

Examples

In the following router configuration example, the local router injects route 0.0.0.0 to the neighbor 172.16.2.3 unconditionally:

```
router bgp 109
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 200
 neighbor 172.16.2.3 default-originate
```

In the following example, the local router injects route 0.0.0.0 to the neighbor 172.16.2.3 only if there is a route to 192.168.68.0 (that is, if a route with any mask exists, such as 255.255.255.0 or 255.255.0.0):

```
router bgp 109
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 200
 neighbor 172.16.2.3 default-originate route-map default-map
!
route-map default-map 10 permit
 match ip address 1
!
access-list 1 permit 192.168.68.0
```

In the following example, the last line of the configuration has been changed to show the use of an extended access list. The local router injects route 0.0.0.0 to the neighbor 172.16.2.3 only if there is a route to 192.168.68.0 with a mask of 255.255.0.0:

```
router bgp 109
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 200
 neighbor 172.16.2.3 default-originate route-map default-map
!
route-map default-map 10 permit
 match ip address 100
!
access-list 100 permit ip host 192.168.68.0 host 255.255.0.0
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
neighbor ebgp-multihop	Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.

neighbor description

To associate a description with a neighbor, use the **neighbor description** command in router configuration mode or address family configuration mode. To remove the description, use the **no** form of this command.

neighbor {*ip-address*|*peer-group-name*} **description** *text*

no neighbor {*ip-address*|*peer-group-name*} **description** [*text*]

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of an EIGRP peer group. This argument is not available in address-family configuration mode.
<i>text</i>	Text (up to 80 characters in length) that describes the neighbor.

Command Default

There is no description of the neighbor.

Command Modes

Router configuration (config-router) Address family configuration (config-router-af)

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.
15.0(1)M	This command was modified. Address-family configuration mode was added.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Examples

In the following examples, the description of the neighbor is “peer with example.com”:

```
Router(config)# router bgp 109
Router(config-router)# network 172.16.0.0
Router(config-router)# neighbor 172.16.2.3 description peer with example.com
```

In the following example, the description of the address family neighbor is “address-family-peer”:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 4453
Router(config-router-af)#
network 172.16.0.0
Router(config-router-af)#
neighbor 172.16.2.3 description address-family-peer
```

Related Commands

Command	Description
address-family (EIGRP)	Enters address family configuration mode to configure an EIGRP routing instance.
network (EIGRP)	Specifies the network for an EIGRP routing process.
router eigrp	Configures the EIGRP address family process.

neighbor disable-connected-check

To disable connection verification to establish an eBGP peering session with a single-hop peer that uses a loopback interface, use the **neighbor disable-connected-check** command in address family or router configuration mode. To enable connection verification for eBGP peering sessions, use the **no** form of this command.

neighbor {*ip-address*|*peer-group-name*} **disable-connected-check**

no neighbor {*ip-address*|*peer-group-name*} **disable-connected-check**

Syntax Description

<i>ip-address</i>	IP address of a neighbor.
peer-group-name	Name of a BGP peer group.

Command Default

A BGP routing process will verify the connection of single-hop eBGP peering session (TTL=254) to determine if the eBGP peer is directly connected to the same network segment by default. If the peer is not directly connected to same network segment, connection verification will prevent the peering session from being established.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

The **neighbor disable-connected-check** command is used to disable the connection verification process for eBGP peering sessions that are reachable by a single hop but are configured on a loopback interface or otherwise configured with a non-directly connected IP address.

This command is required only when the **neighbor ebgp-multihop** command is configured with a TTL value of 1. The address of the single-hop eBGP peer must be reachable. The **neighbor update-source** command must be configured to allow the BGP routing process to use the loopback interface for the peering session.

Examples

In the following example, a single-hop eBGP peering session is configured between two BGP peers that are reachable on the same network segment through a local loopback interfaces on each router:

Examples

```
Router(config)# interface loopback 1
Router(config-if)# ip address 10.0.0.100 255.255.255

Router(config-if)# exit

Router(config)# router bgp 64512

Router(config-router)# neighbor 192.168.0.200 remote-as 65534
Router(config-router)# neighbor 192.168.0.200 ebgp-multihop 1
Router(config-router)# neighbor 192.168.0.200 update-source loopback 2
Router(config-router)# neighbor 192.168.0.200 disable-connected-check
Router(config-router)# end
```

Examples

```
Router(config)# interface loopback 2

Router(config-if)# ip address 192.168.0.200 255.255.255

Router(config-if)# exit

Router(config)# router bgp 65534
Router(config-router)# neighbor 10.0.0.100 remote-as 64512

Router(config-router)# neighbor 10.0.0.100 ebgp-multihop 1
Router(config-router)# neighbor 10.0.0.100 update-source loopback 1

Router(config-router)# neighbor 10.0.0.100 disable-connected-check
Router(config-router)# end
```

Related Commands

Command	Description
neighbor ebgp-multihop	Accepts or initiates BGP connections to external peers residing on networks that are not directly connected.
neighbor update-source	Configures Cisco IOS software to allow BGP sessions to use any operational interface for TCP connections.

neighbor distribute-list

To distribute BGP neighbor information as specified in an access list, use the **neighbor distribute-list** command in address family or router configuration mode. To remove an entry, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **distribute-list** {*access-list-number* | *expanded-list-number* | *access-list-name* | *prefix-list-name*} {**in** | **out**}

no neighbor {*ip-address* | *peer-group-name*} **distribute-list** {*access-list-number* | *expanded-list-number* | *access-list-name* | *prefix-list-name*} {**in** | **out**}

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>access-list-number</i>	Number of a standard or extended access list. The range of a standard access list number is from 1 to 99. The range of an extended access list number is from 100 to 199.
<i>expanded-list-number</i>	Number of an expanded access list number. The range of an expanded access list is from 1300 to 2699.
<i>access-list-name</i>	Name of a standard or extended access list.
<i>prefix-list-name</i>	Name of a BGP prefix list.
in	Access list is applied to incoming advertisements to that neighbor.
out	Access list is applied to outgoing advertisements to that neighbor.

Command Default

No BGP neighbor is specified.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
11.0	The <i>peer-group-name</i> argument was added.

Release	Modification
11.2	The <i>access-list-name</i> argument was added.
12.0	The <i>prefix-list-name</i> argument was added.
12.0(7)T	Address family configuration mode 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.

Usage Guidelines

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

Using a distribute list is one of several ways to filter advertisements. Advertisements can also be filtered by using the following methods:

- Autonomous system path filters can be configured with the **ip as-path access-list** and **neighbor filter-list** commands.
- The **access-list (IP standard)** and **access-list (IP extended)** commands can be used to configure standard and extended access lists for the filtering of advertisement.
- The **route-map (IP)** command can be used to filter advertisements. Route maps may be configured with autonomous system filters, prefix filters, access lists and distribute lists.

Standard access lists may be used to filter routing updates. However, in the case of route filtering when using classless interdomain routing (CIDR), standard access lists do not provide the level of granularity that is necessary to configure advanced filtering of network addresses and masks. Extended access lists, configured with the **access-list (IP extended)** command, should be used to configure route filtering when using CIDR because extended access lists allow the network operator to use wild card bits to filter the relevant prefixes and masks. Wild card bits are similar to the bit masks that are used with normal access lists; prefix and mask bits that correspond to wild card bits that are set to 0 are used in the comparison of addresses or prefixes and wild card bits that are set to 1 are ignored during any comparisons. This function of extended access list configuration can also be used to filter addresses or prefixes based on the prefix length.



Note

Do not apply both a **neighbor distribute-list** and a **neighbor prefix-list** command to a neighbor in any given direction (inbound or outbound). These two commands are mutually exclusive, and only one command (**neighbor prefix-list** or **neighbor distribute-list**) can be applied to each inbound or outbound direction.

Examples

The following router configuration mode example applies list 39 to incoming advertisements from neighbor 172.16.4.1. List 39 permits the advertisement of network 10.109.0.0.

```
router bgp 109
 network 10.108.0.0
 neighbor 172.16.4.1 distribute-list 39 in
```

The following three examples show different scenarios for using an extended access list with a distribute list. The three examples are labeled “Example A”, “Example B”, and “Example C.” Each of the example extended access list configurations are used with the **neighbor distribute-list** command configuration example below.

```
router bgp 109
 network 10.108.0.0
 neighbor 172.16.4.1 distribute-list 101 in
```

Examples

The following extended access list example will permit route 192.168.0.0 255.255.0.0 but deny any more specific routes of 192.168.0.0 (including 192.168.0.0 255.255.255.0):

```
access-list 101 permit ip 192.168.0.0 0.0.0.0 255.255.0.0 0.0.0.0
access-list 101 deny ip 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255
```

Examples

The following extended access list example will permit route 10.108.0/24 but deny 10.108/16 and all other subnets of 10.108.0.0:

```
access-list 101 permit ip 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0
access-list 101 deny ip 10.108.0.0 0.0.255.255 255.255.0.0 0.0.255.255
```

Examples

The following extended access list example will deny all prefixes that are longer than 24 bits and permit all of the shorter prefixes:

```
access-list 101 deny ip 0.0.0.0 255.255.255.255 255.255.255.0 0.0.0.255
access-list 101 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.

Command	Description
ip as-path access-list	Defines a BGP-related access list.
neighbor filter-list	Sets up a BGP filter.
neighbor peer-group (creating)	Creates a BGP peer group.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.

neighbor dmzlink-bw

To configure Border Gateway Protocol (BGP) to advertise the bandwidth of links that are used to exit an autonomous system, use the **neighbor dmzlink-bw** command in address family configuration mode. To disable the linkbandwidthadvertisement, use the **no** form of this command.

neighbor *ip-address* **dmzlink-bw**

no neighbor *ip-address* **dmzlink-bw**

Syntax Description

<i>ip-address</i>	IP address of the neighbor router for which the bandwidth of the outbound link is advertised.

Command Default

This command is disabled by default.

Command Modes

Address family configuration (config-router-af)

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.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)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

The **neighbor dmzlink-bw** command is used to configure BGP to advertise the bandwidth of the specified external interface as an extended community. This command is configured for links between directly connected external BGP (eBGP) neighbors. The link bandwidth extended community attribute is propagated to iBGP peers when extended community exchange is enabled with the **neighbor send-community** command. This feature is used with BGP multipath features to configure load balancing over links with unequal bandwidth. This feature is not enabled until the **bgp dmzlink-bw** command is entered under the address family session for each router that has a directly connected external link.

Examples

In the following example, the BGP Link Bandwidth feature is configured to allow multipath load balancing to distribute link traffic proportionally to the bandwidth of each external link, and to advertise the bandwidth of these links to iBGP peers as an extended community:

```
Router(config)# router bgp 100
Router(config-router)# neighbor 10.10.10.1 remote-as 100
Router(config-router)# neighbor 10.10.10.1 update-source Loopback 0
Router(config-router)# neighbor 10.10.10.3 remote-as 100
Router(config-router)# neighbor 10.10.10.3 update-source Loopback 0
Router(config-router)# neighbor 172.16.1.1 remote-as 200
Router(config-router)# neighbor 172.16.1.1 ebgp-multihop 1
Router(config-router)# neighbor 172.16.2.2 remote-as 200
Router(config-router)# neighbor 172.16.2.2 ebgp-multihop 1
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp dmzlink-bw
Router(config-router-af)# neighbor 10.10.10.1 activate
Router(config-router-af)# neighbor 10.10.10.1 next-hop-self
Router(config-router-af)# neighbor 10.10.10.1 send-community both
Router(config-router-af)# neighbor 10.10.10.3 activate
Router(config-router-af)# neighbor 10.10.10.3 next-hop-self
Router(config-router-af)# neighbor 10.10.10.3 send-community both
Router(config-router-af)# neighbor 172.16.1.1
  activate
Router(config-router-af)# neighbor 172.16.1.1 dmzlink-bw
Router(config-router-af)# neighbor 172.16.2.2 activate
Router(config-router-af)# neighbor 172.16.2.2 dmzlink-bw
Router(config-router-af)# maximum-paths ibgp 6
Router(config-router-af)# maximum-paths 6
```

Related Commands

Command	Description
bgp dmzlink-bw	Configures BGP to distribute traffic proportionally over external links with unequal bandwidth when multipath load balancing is enabled.
neighbor send-community	Specifies that a communities attribute should be sent to a BGP neighbor.

neighbor ebgp-multihop

To accept and attempt BGP connections to external peers residing on networks that are not directly connected, use the **neighbor ebgp-multihop** command in router configuration mode. To return to the default, use the **no** form of this command.

neighbor {*ip-address*|*ipv6-address*|*peer-group-name*} **ebgp-multihop** [*tth*]

no neighbor {*ip-address*|*ipv6-address*|*peer-group-name*} **ebgp-multihop**

Syntax Description

<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>ipv6-address</i>	IPv6 address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>tth</i>	(Optional) Time-to-live in the range from 1 to 255 hops.

Command Default

Only directly connected neighbors are allowed.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
11.0	The <i>peer-group-name</i> argument was added.
12.2(33)SRA	The <i>ipv6-address</i> argument and support for the IPv6 address family were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

This feature should be used only under the guidance of Cisco technical support staff.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

To prevent the creation of loops through oscillating routes, the multihop will not be established if the only route to the multihop peer is the default route (0.0.0.0).

Examples

The following example allows connections to or from neighbor 10.108.1.1, which resides on a network that is not directly connected:

```
router bgp 109
 neighbor 10.108.1.1 ebgp-multihop
```

Related Commands

Command	Description
neighbor advertise-map non-exist-map	Allows a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route.
neighbor peer-group (creating)	Creates a BGP peer group.
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.

neighbor fall-over

To enable Border Gateway Protocol (BGP) to monitor the peering session of a specified neighbor for adjacency changes and to deactivate the peering session, use the **neighbor fall-over** command in address family configuration mode or router configuration mode. To disable BGP monitoring of the neighbor peering session, use the **no** form of this command.

neighbor {*ip-address*|*ipv6-address*} **fall-over** [**bfd** [**check-control-plane-failure**]] **route-map** *map-name*
no neighbor {*ip-address*|*ipv6-address*} **fall-over** [**bfd** [**check-control-plane-failure**]] **route-map** *map-name*

Syntax Description

<i>ip-address</i>	IPv4 address of a BGP neighbor.
<i>ipv6-address</i>	IPv6 address of a BGP neighbor.
bfd	(Optional) Enables Bidirectional Forwarding Detection (BFD) protocol support for fallover.
check-control-plane-failure	(Optional) Retrieves control plane dependent failure (c-bit) information from BFD for BGP graceful restart (GR)/Nonstop Forwarding (NSF) operation.
route-map <i>map-name</i>	(Optional) Specifies the use of a route map by name. Note The route map applies only to a neighbor with an IPv4 address.

Command Default

BGP does not monitor neighbor peering sessions.

Command Modes

Address family configuration (config-router-af)
 Router configuration (config-router)

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.4(4)T	This command was modified. The route-map keyword and <i>map-name</i> argument were added to support the BGP Selective Address Tracking feature.
12.2(33)SRA	This command was modified. The bfd keyword was added to support the BFD feature, and this command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SRB	This command was modified. The route-map keyword and <i>map-name</i> argument were added to support the BGP Selective Address Tracking 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.
12.2(33)SB	This command was modified. The bfd keyword was added to support the BFD feature.
15.1(2)S	This command was modified. The <i>ipv6-address</i> argument was added.
Cisco IOS XE 3.3S	This command was modified. The <i>ipv6-address</i> argument was added.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
Cisco IOS XE Release 3.6S	This command was modified. The check-control-plane-failure keyword was added.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
Cisco IOS XE Release 3.7S	This command was implemented on the Cisco ASR 903 router.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

The **neighbor fall-over** command is a BGP neighbor session command that is used to enable BGP fast peering session deactivation. BGP fast peering session deactivation improves BGP convergence and response time to adjacency changes with BGP neighbors. BGP fast peering session deactivation is event-driven and is configured on a per-neighbor basis. When BGP fast peering session deactivation is enabled, BGP will monitor the peering session with the specified neighbor. Adjacency changes are detected, and terminated peering sessions are deactivated in between the default or configured BGP scanning interval.

In Cisco IOS Release 12.4(4)T, 12.2(33)SRB, and later releases, the optional **route-map** keyword and *map-name* argument are used with this command to determine if a peering session with a BGP neighbor should be deactivated (reset) when a route to the BGP peer changes. The route map is evaluated against the new route, and if a deny statement is returned, the peer session is reset. The route map is not used for session establishment.



Note

Only the **match ip address** and **match source-protocol** commands are supported in the route map. No **set** commands or other **match** commands are supported.

In Cisco IOS Release 12.2(33)SRA, 12.2(33)SB, and later releases, the optional **bfd** keyword is used to enable BFD protocol support for fallover. BFD provides fast forwarding path failure detection and a consistent failure detection method for network administrators. Because the network administrator can use BFD to detect

forwarding path failures at a uniform rate, rather than the variable rates for different routing protocol hello mechanisms, network profiling and planning is easier, and reconvergence time is consistent and predictable. The main benefit of implementing BFD for BGP is a marked decrease in reconvergence time.

In Cisco IOS Release 15.1(2)S, Cisco IOS XE Release 3.3S, and later releases, an IPv6 address can be specified with the **bfd** keyword. Once it has been verified that BFD neighbors are up, the output from the **show bgp ipv6 unicast neighbors** command with a specified IPv6 address will display that BFD is being used to detect fast fallover.

Examples

In the following example, the BGP routing process is configured to monitor and use fast peering session deactivation for the neighbor session with the neighbor at 192.168.1.2:

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 fall-over
end
```

In the following example, the BGP peering session is reset if a route with a prefix of /28 or a more specific route to a peer destination is no longer available:

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.1.2 fall-over route-map CHECK-NBR
exit
ip prefix-list FILTER28 seq 5 permit 0.0.0.0/0 ge 28
route-map CHECK-NBR permit 10
 match ip address prefix-list FILTER28
end
```

In the following example, BFD is enabled for Fast Ethernet interface 0/1/1 with a specified BFD interval. The BGP peering session is also BFD enabled, which will result in a decreased reconvergence time for BGP if any of the forwarding paths to specified neighbors fail.

```
interface FastEthernet 0/1/1
 ip address 172.16.10.1 255.255.255.0
 bfd interval 50 min_rx 50 multiplier 3
exit
router bgp 40000
 bgp log-neighbor-changes
 neighbor 172.16.10.2 remote-as 45000
 neighbor 172.16.10.2 fall-over bfd
exit
```

In the following IPv6 example, BFD is enabled for Fast Ethernet interface 0/1/1 with a specified BFD interval. The BGP peering session is also BFD enabled and this will result in a decreased reconvergence time for BGP if any of the forwarding paths to the specified neighbor at 2001:DB8:2:1::4 fail.

```
ipv6 unicast-routing
ipv6 cef
interface fastethernet 0/1/1
 ipv6 address 2001:DB8:1:1::1/64
 bfd interval 500 min_rx 500 multiplier 3
 no shutdown
exit
router bgp 65000
 no bgp default ipv4-unicast
 address-family ipv6 unicast
 bgp log-neighbor-changes
 neighbor 2001:DB8:2:1::4 remote-as 45000
 neighbor 2001:DB8:2:1::4 fall-over bfd
end
```


Related Commands

Command	Description
bfd	Sets the baseline BFD session parameters on an interface.
match ip address	Matches IP addresses defined by a prefix list.
match source-protocol	Matches the route type based on the source protocol.
show bgp ipv6 unicast neighbors	Displays information about BGP IPv6 neighbors.

neighbor filter-list

To set up a BGP filter, use the **neighbor filter-list** command in address family or router configuration mode. To disable this function, use the **no** form of this command.

neighbor {*ip-address*|*peer-group-name*} **filter-list** *access-list-number* {**in**|**out**}

no neighbor {*ip-address*|*peer-group-name*} **filter-list** *access-list-number* {**in**|**out**}

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>access-list-number</i>	Number of an autonomous system path access list. You define this access list with the ip as-path access-list command.
in	Access list is applied to incoming routes.
out	Access list is applied to outgoing routes.

Command Default

No BGP filter is used.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.1	The weight keyword was removed.
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 establishes filters on both inbound and outbound BGP routes.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group.

**Note**

Do not apply both a **neighbor distribute-list** and a **neighbor prefix-list** command to a neighbor in any given direction (inbound or outbound). These two commands are mutually exclusive, and only one command (**neighbor distribute-list** or **neighbor prefix-list**) can be applied to each inbound or outbound direction.

Examples

In the following router configuration mode example, the BGP neighbor with IP address 172.16.1.1 is not sent advertisements about any path through or from the adjacent autonomous system 123:

```
ip as-path access-list 1 deny _123
ip as-path access-list 1 deny ^123$
router bgp 109
 network 10.108.0.0
 neighbor 192.168.6.6 remote-as 123
 neighbor 172.16.1.1 remote-as 47
 neighbor 172.16.1.1 filter-list 1 out
```

In the following address family configuration mode example, the BGP neighbor with IP address 172.16.1.1 is not sent advertisements about any path through or from the adjacent autonomous system 123:

```
ip as-path access-list 1 deny _123
ip as-path access-list 1 deny ^123$
router bgp 109
 address-family ipv4 unicast
  network 10.108.0.0
  neighbor 192.168.6.6 remote-as 123
  neighbor 172.16.1.1 remote-as 47
  neighbor 172.16.1.1 filter-list 1 out
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
ip as-path access-list	Defines a BGP-related access list.
match as-path	Matches BGP autonomous system path access lists.
neighbor distribute-list	Distributes BGP neighbor information as specified in an access list.
neighbor peer-group (creating)	Creates a BGP peer group.

Command	Description
neighbor prefix-list	Prevents distribution of BGP neighbor information as specified in a prefix list, a CLNS filter expression, or a CLNS filter set.
neighbor weight	Assigns a weight to a neighbor connection.
set weight	Specifies the BGP weight for the routing table.

neighbor ha-mode graceful-restart

To enable or disable the Border Gateway Protocol (BGP) graceful restart capability for a BGP neighbor or peer group, use the **neighbor ha-mode graceful-restart** command in router configuration mode. To remove from the configuration the BGP graceful restart capability for a neighbor, use the **no** form of this command.

neighbor {*ip-address*|*peer-group-name*} **ha-mode graceful-restart** [**disable**]

no neighbor {*ip-address*|*peer-group-name*} **ha-mode graceful-restart** [**disable**]

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
disable	(Optional) Disables BGP graceful restart capability for a neighbor.

Command Default

BGP graceful restart capability is disabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

The **neighbor ha-mode graceful-restart** command is used to enable or disable the graceful restart capability for an individual BGP neighbor or peer group in a BGP network. Use the **disable** keyword to disable the graceful restart capability when graceful restart has been previously enabled for the BGP peer.

The graceful restart capability is negotiated between nonstop forwarding (NSF)-capable and NSF-aware peers in OPEN messages during session establishment. If the graceful restart capability is enabled after a BGP session has been established, the session will need to be restarted with a soft or hard reset.

The graceful restart capability is supported by NSF-capable and NSF-aware routers. A router that is NSF-capable can perform a stateful switchover (SSO) operation (graceful restart) and can assist restarting peers by holding routing table information during the SSO operation. A router that is NSF-aware functions like a router that is NSF-capable but cannot perform an SSO operation.

To enable the BGP graceful restart capability globally for all BGP neighbors, use the **bgp graceful-restart** command. When the BGP graceful restart capability is configured for an individual neighbor, each method of configuring graceful restart has the same priority, and the last configuration instance is applied to the neighbor.

Use the **show ip bgp neighbors** command to verify the BGP graceful restart configuration for BGP neighbors.

Examples

The following example enables the BGP graceful restart capability for the BGP neighbor, 172.21.1.2:

```
router bgp 45000
  bgp log-neighbor-changes
  address-family ipv4 unicast
  neighbor 172.21.1.2 remote-as 45000
  neighbor 172.21.1.2 activate
  neighbor 172.21.1.2 ha-mode graceful-restart
end
```

The following example enables the BGP graceful restart capability globally for all BGP neighbors and then disables the BGP graceful restart capability for the BGP peer group PG1. The BGP neighbor 172.16.1.2 is configured as a member of the peer group PG1 and inherits the disabling of the BGP graceful restart capability.

```
router bgp 45000
  bgp log-neighbor-changes
  bgp graceful-restart
  address-family ipv4 unicast
  neighbor PG1 peer-group
  neighbor PG1 remote-as 45000
  neighbor PG1 ha-mode graceful-restart disable
  neighbor 172.16.1.2 peer-group PG1
end
```

Related Commands

Command	Description
bgp graceful-restart	Enables the BGP graceful restart capability globally for all BGP neighbors.
ha-mode graceful-restart	Enables or disables the BGP graceful restart capability for a BGP peer session template.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

neighbor ha-mode sso

To configure a Border Gateway Protocol (BGP) neighbor to support BGP nonstop routing (NSR) with stateful switchover (SSO), use the **neighbor ha-mode sso** command in the appropriate command mode. To remove the configuration, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address*} **ha-mode sso**

no neighbor {*ip-address* | *ipv6-address*} **ha-mode sso**

Syntax Description

<i>ip-address</i>	IP address of the neighboring router.
<i>ipv6-address</i>	IPv6 address of the neighboring router.

Command Default

BGP NSR with SSO support is disabled.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Session-template configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
Cisco IOS XE 3.6S	This command was modified. It is supported in router configuration mode.
15.2(2)S	This command was modified. It is supported in router configuration mode.
Cisco IOS XE 3.7S	This command was implemented on the Cisco ASR 903 router.

Usage Guidelines

The **neighbor ha-mode sso** command is used to configure a BGP neighbor to support BGP NSR with SSO. BGP NSR with SSO is disabled by default.

BGP NSR with SSO is supported in BGP peer, BGP peer group, and BGP session template configurations. To configure BGP NSR with SSO in BGP peer and BGP peer group configurations, use the **neighbor ha-mode sso** command in address family configuration mode for address family BGP peer sessions. To include support

for Cisco BGP NSR with SSO in a peer session template, use the **ha-mode sso** command in session-template configuration mode.

Examples

The following example shows how to configure a BGP neighbor to support SSO:

```
Router(config-router-af) # neighbor 10.3.32.154 ha-mode sso
```

Related Commands

Command	Description
show ip bgp sso summary	Displays the state of NSR established sessions for the IPv4 address family or all address families.
show ip bgp vpnv4	Displays VPN address information from the BGP table.
show ip bgp vpnv4 all sso summary	Displays the number of BGP neighbors that support SSO.

neighbor inherit peer-policy

To send a peer policy template to a neighbor so that the neighbor can inherit the configuration, use the **neighbor inherit peer-policy** command in address family or router configuration mode. To stop sending the peer policy template, use the **no** form of this command.

neighbor *ip-address* **inherit peer-policy** *policy-template-name*

no neighbor *ip-address* **inherit peer-policy** *policy-template-name*

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>policy-template-name</i>	Name or tag for the peer policy template.

Command Default

No default behavior or values

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
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 used to send locally configured policy templates to the specified neighbor. If the policy template is configured to inherit configurations from other peer policy templates, the specified neighbor will also indirectly inherit these configurations from the other peer policy templates. A directly applied peer policy template can directly or indirectly inherit configurations from up to seven peer policy templates. So, a total of eight peer policy templates can be applied to a neighbor or neighbor group.

**Note**

A Border Gateway Protocol (BGP) neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured to belong only to a peer group or to inherit policies only from peer templates.

Examples

The following example configures the 10.0.0.1 neighbor in address family configuration mode to inherit the peer policy template name CUSTOMER-A. The 10.0.0.1 neighbor will also indirectly inherit the peer policy templates in CUSTOMER-A. The explicit remote-as statement is required for the neighbor inherit statement to work. If a peering is not configured, the specified neighbor will not accept the session template.

```
Router(config)# router bgp 101
Router(config-router)# neighbor 10.0.0.1 remote-as 202
Router(config-router)# address-family ipv4 unicast
Router(config-router-af)# neighbor 10.0.0.1 inherit peer-policy CUSTOMER-A
Router(config-router-af)# exit
```

Related Commands

Command	Description
exit peer-policy	Exits policy-template configuration mode and enters router configuration mode.
inherit peer-policy	Configures a peer policy template to inherit the configuration from another peer policy template.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.
show ip bgp template peer-policy	Displays locally configured peer policy templates.
template peer-policy	Creates a peer policy template and enters policy-template configuration mode.

neighbor inherit peer-session

To send a peer session template to a neighbor so that the neighbor can inherit the configuration, use the **neighbor inherit peer-session** command in address family or router configuration mode. To stop sending the peer session template, use the **no** form of this command.

neighbor *ip-address* **inherit peer-session** *session-template-name*

no neighbor *ip-address* **inherit peer-session** *session-template-name*

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>session-template-name</i>	Name or tag for the peer session template.

Command Default

No default behavior or values

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
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 used to send locally configured session templates to the specified neighbor. If the session template is configured to inherit configurations from other session templates, the specified neighbor will also indirectly inherit these configurations from the other session templates. A neighbor can directly inherit only one peer session template and indirectly inherit up to seven peer session templates.

**Note**

A Border Gateway Protocol (BGP) neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured to belong only to a peer group or to inherit policies only from peer templates.

Examples

The following example configures the 172.16.0.1 neighbor to inherit the CORE1 peer session template. The 172.16.0.1 neighbor will also indirectly inherit the configuration from the peer session template named INTERNAL-BGP. The explicit remote-as statement is required for the neighbor inherit statement to work. If a peering is not configured, the specified neighbor will not accept the session template.

```
Router(config)# router bgp 101
Router(config)# neighbor 172.16.0.1 remote-as 202
Router(config-router)# neighbor 172.16.0.1 inherit peer-session CORE1
```

Related Commands

Command	Description
exit peer-session	Exits session-template configuration mode and enters router configuration mode.
inherit peer-session	Configures a peer session template to inherit the configuration from another peer session template.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.
show ip bgp template peer-session	Displays locally configured peer session templates.
template peer-session	Creates a peer session template and enters session-template configuration mode.

neighbor internal-vpn-client

To enable provider edge (PE) or customer edge (CE) devices to exchange Border Gateway Protocol (BGP) routing by peering as internal BGP (iBGP), use the **neighbor internal-vpn-client** command in address family configuration mode. To disable this command, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name* | *ipv6-address*} **internal-vpn-client**

no neighbor {*ip-address* | *peer-group-name* | *ipv6-address*} **internal-vpn-client**

Syntax Description

<i>ip-address</i>	IP address of the neighboring device.
<i>peer-group-name</i>	Name of the BGP peer group.
<i>ipv6-address</i>	IPv6 address of the iBGP neighbor.

Command Default

No default behavior or values

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE Release 3.10S	This command was introduced.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

Usage Guidelines

The **neighbor *ip-address* internal-vpn-client** command enables PE devices to make the entire VPN cloud act like an internal VPN client to the CE devices connected internally. This command is used so that existing internal BGP VRF lite scenarios are not affected.

You need not configure autonomous system override for CE devices after enabling this command..

Examples

The following example shows how to enable **neighbor *ip-address* internal-vpn-client** command.

```
Device(config-router)# address-family ipv4 vrf blue
Device(config-router-af)# neighbor 10.0.0.1 internal-vpn-client
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a BGP neighbor.

 neighbor internal-vpn-client

neighbor local-as

To customize the AS_PATH attribute for routes received from an external Border Gateway Protocol (eBGP) neighbor, or to configure the BGP—Support for iBGP Local-AS feature, use the **neighbor local-as** command in address family or router configuration mode. To disable AS_PATH attribute customization or iBGP Local-AS support, use the **no** form of this command.

neighbor {*ip-address*|*ipv6-address*|*peer-group-name*} **local-as** [*autonomous-system-number* [**no-prepend** [**replace-as** [**dual-as**]]]]

no neighbor {*ip-address*|*ipv6-address*|*peer-group-name*} **local-as**

Syntax Description

<i>ip-address</i>	IPv4 address of the eBGP neighbor.
<i>ipv6-address</i>	IPv6 address of the eBGP neighbor.
<i>peer-group</i>	Name of a BGP peer group.
<i>autonomous-system-number</i>	(Optional) Number of an autonomous system to prepend to the AS_PATH attribute. The range of values for this argument is any valid autonomous system number from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the router bgp command. Note With this argument, you cannot specify the autonomous system number from the local BGP routing process or from the network of the remote peer.
no-prepend	(Optional) Does not prepend the local autonomous system number to any routes received from the eBGP neighbor.

replace-as	(Optional) Replaces the real autonomous system number with the local autonomous system number in the eBGP updates. The autonomous system number from the local BGP routing process is not prepended.
dual-as	(Optional) Configures the eBGP neighbor to establish a peering session by using the real autonomous system number (from the local BGP routing process) or by using the autonomous system number configured with the <i>autonomous-system-number</i> argument (local-as).

Command Default

The autonomous system number from the local BGP routing process is prepended to all external routes by default.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	CLI support for address family configuration mode was added.
12.2(8)T	The no-prepend keyword was added.
12.2(14)S	The no-prepend keyword was integrated into Cisco IOS Release 12.2(14)S.
12.0(18)S	The no-prepend keyword was integrated into Cisco IOS Release 12.0(18)S.
12.0(27)S	The replace-as and dual-as keywords were added.
12.2(25)S	The replace-as and dual-as keywords were integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	The replace-as and dual-as keywords were integrated into Cisco IOS Release 12.3(11)T.
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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.

Release	Modification
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(1)SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.3(2)S	This command was modified. It can be used to configure the iBGP Local-AS feature.
Cisco IOS XE Release 3.9S	This command was modified. It can be used to configure the iBGP Local-AS feature.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

The **neighbor local-as** command is used to customize the AS_PATH attribute by adding and removing autonomous system numbers for routes received from eBGP neighbors. The configuration of this command allows a router to appear to external peers as a member of another autonomous system for the purpose of autonomous system number migration. This feature simplifies the process of changing the autonomous system number in a BGP network by allowing the network operator to migrate customers to new configurations during normal service windows without disrupting existing peering arrangements.

**Caution**

BGP prepends the autonomous system number from each BGP network that a route traverses to maintain network reachability information and to prevent routing loops. This command should be configured only for autonomous system migration, and should be deconfigured after the transition has been completed. This procedure should be attempted only by an experienced network operator. Routing loops can be created through improper configuration.

This command can be used for only true eBGP peering sessions. This command does not work for two peers in different subautonomous systems of a confederation.

This command supports individual peering sessions and configurations applied through peer groups and peer templates. If this command is applied to a group of peers, the individual peers cannot be customized.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

To ensure a smooth transition, we recommend that all BGP speakers within an AS that is identified using a 4-byte AS number be upgraded to support 4-byte AS numbers.

BGP—Support for iBGP Local-AS

There can be scenarios where the network administrator wants iBGP attributes to be passed unmodified, typically to facilitate the merging of two autonomous systems. The BGP—Support for iBGP Local-AS feature causes BGP to treat an iBGP local-AS connection as an iBGP connection and pass the LOCAL_PREF, ORIGINATOR_ID, CLUSTER_ID, and CLUSTER_LIST attributes unmodified. If a BGP peer has a **neighbor remote-as** command and a **neighbor local-as** command that specify the same AS number, the session with that neighbor is treated as iBGP when advertising routes received in this session to iBGP peers that have no **neighbor local-as** command configured. That means that during re-advertisement, BGP will pass the LOCAL_PREF, ORIGINATOR_ID, CLUSTER_ID, and CLUSTER_LIST attributes unmodified instead of dropping them.

**Note**

The other keywords in the **neighbor local-as** command (**no-prepend**, **replace-as**, and **dual-as**) do not affect an iBGP local-AS client. Even if these keywords are configured for an iBGP client, no action is taken to modify the AS_PATH.

Examples

The following example establishes peering between Router 1 and Router 2 through autonomous system 300, using the local-as feature:

```
router bgp 100
 address-family ipv4 unicast
  neighbor 172.16.1.1 remote-as 200
```

```
neighbor 172.16.1.1 local-as 300
```

```
router bgp 200
address-family ipv4 unicast
neighbor 10.0.0.1 remote-as 300
```

The following example configures BGP to not prepend autonomous system 500 to routes received from the 192.168.1.1 neighbor:

```
router bgp 400
address-family ipv4 multicast
network 192.168.0.0
neighbor 192.168.1.1 local-as 500 no-prepend
```

The following example strips private autonomous system 64512 from outbound routing updates for the 172.20.1.1 neighbor and replaces it with autonomous system 600:

```
router bgp 64512
address-family ipv4 unicast
neighbor 172.20.1.1 local-as 600 no-prepend replace-as
neighbor 172.20.1.1 remove-private-as
```

The following examples show the configurations for two provider networks and one customer network. Router 1 belongs to AS 100, and Router 2 belongs to AS 200. AS 200 is being merged into AS 100. This transition must occur without interrupting service to Router 3 in AS 300 (customer network). The **neighbor local-as** command is configured on Router 1 to allow Router 3 to maintain peering with AS 200 during this transition. After the transition is complete, the configuration on Router 3 can be updated to peer with AS 100 during a normal maintenance window or during other scheduled downtime.

```
interface Serial3/0
ip address 10.3.3.11 255.255.255.0
!
router bgp 100
no synchronization
bgp router-id 100.0.0.11
neighbor 10.3.3.33 remote-as 300
neighbor 10.3.3.33 local-as 200 no-prepend replace-as dual-as
```

```
interface Serial3/0
ip address 10.3.3.11 255.255.255.0
!
router bgp 200
bgp router-id 100.0.0.11
neighbor 10.3.3.33 remote-as 300
```

```
interface Serial3/0
ip address 10.3.3.33 255.255.255.0
!
router bgp 300
bgp router-id 100.0.0.3
neighbor 10.3.3.11 remote-as 200
```

To complete the migration after the two autonomous systems have merged, the peering session is updated on Router 3:

```
neighbor 10.3.3.11 remote-as 100
```

The following example configures BGP to not prepend the 4-byte AS number of 65536 in asplain format to routes received from the 192.168.1.2 neighbor. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or a later release.

```
router bgp 65538
 address-family ipv4 multicast
  network 192.168.0.0
  neighbor 192.168.1.2 local-as 65536 no-prepend
```

The following example configures BGP to not prepend the 4-byte AS number of 1.0 in asdot format to routes received from the 192.168.1.2 neighbor. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, 12.4(24)T, or Cisco IOS XE Release 2.3.

```
router bgp 1.2
 address-family ipv4 multicast
  network 192.168.0.0
  neighbor 192.168.1.2 local-as 1.0 no-prepend
```

The following example configures a route reflector (RR) in AS 4000 to treat BGP sessions with the neighbor in AS 2500 as iBGP sessions. That is, iBGP attributes (LOCAL_PREF, ORIGINATOR_ID, CLUSTER_ID, and CLUSTER_LIST) will not be dropped from routes in advertisements to and from the neighbor; the attributes will be preserved. AS 2500 will be prepended to the AS_PATH attribute in all routes to and from the neighbor. Additionally, the RR is enabled so that it can be configured with iBGP policies (by using a route map, which is not shown here).

```
router bgp 4000
 neighbor 192.168.1.1 remote-as 2500
 neighbor 192.168.1.1 local-as 2500
 neighbor 192.168.1.1 route-reflector-client
 address-family vpnv4
  neighbor 192.168.1.1 allow-policy
!
 address-family vpnv6
  neighbor 192.168.1.1 allow-policy
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
neighbor allow-policy	Allows iBGP policies to be preserved and passed on to a peer in a different AS.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
neighbor remove-private-as	Removes private autonomous system numbers from outbound routing updates.
router bgp	Configures the BGP routing process.
show ip bgp	Displays entries in the BGP routing table.

Command	Description
show ip bgp neighbors	Displays information about BGP neighbors.

neighbor maximum-prefix (BGP)

To control how many prefixes can be received from a neighbor, use the **neighbor maximum-prefix** command in router configuration mode. To disable this function, use the **no** form of this command.

neighbor {*ip-address*|*peer-group-name*} **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**]

no neighbor {*ip-address*|*peer-group-name*} **maximum-prefix** *maximum*

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a Border Gateway Protocol (BGP) peer group.
<i>maximum</i>	Maximum number of prefixes allowed from the specified neighbor. The number of prefixes that can be configured is limited only by the available system resources on a router.
<i>threshold</i>	(Optional) Integer specifying at what percentage of the <i>maximum-prefix</i> limit the router starts to generate a warning message. The range is from 1 to 100; the default is 75.
restart	(Optional) Configures the router that is running BGP to automatically reestablish a peering session that has been disabled because the maximum-prefix limit has been exceeded. The restart timer is configured with the <i>restart-interval</i> argument.
<i>restart-interval</i>	(Optional) Time interval (in minutes) that a peering session is reestablished. The range is from 1 to 65535 minutes.
warning-only	(optional) Allows the router to generate a sys-log message when the <i>maximum-prefix</i> limit is exceeded, instead of terminating the peering session.

Command Default

This command is disabled by default. Peering sessions are disabled when the maximum number of prefixes is exceeded. If the *restart-interval* argument is not configured, a disabled session will stay down after the maximum-prefix limit is exceeded.

threshold : 75 percent

Command Modes

Router configuration (config-router)

Command History

Release	Modification
11.3	This command was introduced.
12.0(22)S	The restart keyword was introduced.
12.2(15)T	The restart keyword was integrated into Cisco IOS Release 12.2(15)T.
12.2(18)S	The restart keyword was integrated into Cisco IOS Release 12.2(18)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
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.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

The **neighbor maximum-prefix** command allows you to configure a maximum number of prefixes that a Border Gateway Protocol (BGP) routing process will accept from the specified peer. This feature provides a mechanism (in addition to distribute lists, filter lists, and route maps) to control prefixes received from a peer.

When the number of received prefixes exceeds the maximum number configured, BGP disables the peering session (by default). If the **restart** keyword is configured, BGP will automatically reestablish the peering session at the configured time interval. If the **restart** keyword is not configured and a peering session is terminated because the maximum prefix limit has been exceeded, the peering session will not be reestablished until the **clear ip bgp** command is entered. If the **warning-only** keyword is configured, BGP sends only a log message and continues to peer with the sender.

There is no default limit on the number of prefixes that can be configured with this command. Limitations on the number of prefixes that can be configured are determined by the amount of available system resources.

Examples

In the following example, the maximum prefixes that will be accepted from the 192.168.1.1 neighbor is set to 1000:

```
Router(config)# router bgp 40000
Router(config-router)# network 192.168.0.0
Router(config-router)# neighbor 192.168.1.1 maximum-prefix 1000
```

In the following example, the maximum number of prefixes that will be accepted from the 192.168.2.2 neighbor is set to 5000. The router is also configured to display warning messages when 50 percent of the maximum-prefix limit (2500 prefixes) has been reached.

```
Router(config)# router bgp 40000
Router(config-router)# network 192.168.0.0
```

```
Router(config-router)# neighbor 192.168.2.2 maximum-prefix 5000 50
```

In the following example, the maximum number of prefixes that will be accepted from the 192.168.3.3 neighbor is set to 2000. The router is also configured to reestablish a disabled peering session after 30 minutes.

```
Router(config)# router bgp 40000
```

```
Router(config-router)# network 192.168.0.0
```

```
Router(config-router)# neighbor 192.168.3.3 maximum-prefix 2000 restart 30
```

In the following example, warning messages will be displayed when the threshold of the maximum-prefix limit ($500 \times 0.75 = 375$) for the 192.168.4.4 neighbor is exceeded:

```
Router(config)# router bgp 40000
```

```
Router(config-router)# network 192.168.0.0
```

```
Router(config-router)# neighbor 192.168.4.4 maximum-prefix 500 warning-only
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection using BGP soft reconfiguration.

neighbor next-hop-self

To configure a router as the next hop for a BGP-speaking neighbor or peer group, use the **neighbor next-hop-self** command in router configuration mode. To disable this feature, use the **no** form of this command.

neighbor {*ip-address*|*peer-group-name*} **next-hop-self** [**all**]

no neighbor {*ip-address*|*peer-group-name*} **next-hop-self** [**all**]

Syntax Description

<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
all	(Optional) Specifies that the next hop of both eBGP- and iBGP-learned routes is updated by the route reflector (RR).

Command Default

This command is disabled by default.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
11.0	The <i>peer-group-name</i> 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.
15.1(1)SY	This command was modified. The optional all keyword was added.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command is useful in unmeshed networks (such as Frame Relay or X.25) where BGP neighbors may not have direct access to all other neighbors on the same IP subnet.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group.

For a finer granularity of control, see the **set ip next-hop** command.

If you do not use the optional **all** keyword, the next hop of only eBGP-learned routes will be updated by the RR. With the **all** keyword configured, the next hop of both eBGP- and iBGP-learned routes will be updated by the RR.

Both the **no neighbor {ip-address | peer-group-name} next-hop-self** and the **no neighbor {ip-address | peer-group-name} next-hop-self all** commands can be used to disable next-hop-self for both eBGP and iBGP paths (if any or both of them are configured).

Examples

The following example forces all updates destined for 10.108.1.1 to advertise this router as the next hop:

```
router bgp 109
 neighbor 10.108.1.1 next-hop-self
```

Related Commands

Command	Description
neighbor peer-group (creating)	Creates a BGP peer group.
set ip next-hop (BGP)	Indicates where to output packets that pass a match clause of a route map for policy routing.

neighbor next-hop-unchanged

To enable an external BGP (eBGP) peer that is configured as multihop to propagate the next hop unchanged, use the **neighbor next-hop-unchanged** command in address family or router configuration mode. To disable that propagation of the next hop being unchanged, use the **no** form of this command.

neighbor {*ip-address*|*ipv6-address*|*peer-group-name*} **next-hop-unchanged** [**allpaths**]

no neighbor {*ip-address*|*ipv6-address*|*peer-group-name*} **next-hop-unchanged** [**allpaths**]

Syntax Description

<i>ip-address</i>	Propagate the iBGP path's next hop unchanged for this IPv4 neighbor.
<i>ipv6-address</i>	Propagate the iBGP path's next hop unchanged for this IPv6 neighbor.
<i>peer-group-name</i>	Propagate the iBGP path's next hop unchanged for this BGP peer group.
allpaths	(Optional) Propagate the next hop unchanged, for all paths (iBGP and eBGP) to this neighbor.

Command Default

This command is disabled by default.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
12.0(16)ST	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2.
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(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. The allpaths keyword was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Release	Modification
Cisco IOS XE 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

By default, for eBGP, the next hop to reach a connected network is the IP address of the neighbor that sent the update. Therefore, as an update goes from router to router, the next hop typically changes to be the address of the neighbor that sent the update (the router's own address).

However, there might be a scenario where you want the next hop to remain unchanged. The **neighbor next-hop-unchanged** command is used to propagate the next hop unchanged for multihop eBGP peering sessions. This command is configured on an eBGP neighbor, but the neighbor propagates routes learned from iBGP; that is, the neighbor propagates the next hop of iBGP routes toward eBGP.



Caution

Using the **neighbor next-hop-unchanged** command or incorrectly altering the BGP next hop can cause inconsistent routing, routing loops, or a loss of connectivity. It should only be attempted by someone who has a good understanding of the design implications.

This command can be used to configure MPLS VPNs between service providers by not modifying the next hop attribute when advertising routes to an eBGP peer.

Examples

The following example configures a multihop eBGP peer at 10.0.0.100 in a remote autonomous system (AS). When the local router sends updates to that peer, it will send them without modifying the next hop attribute.

```
router bgp 65535
 address-family ipv4
  neighbor 10.0.0.100 remote-as 65600
  neighbor 10.0.0.100 activate
  neighbor 10.0.0.100 ebgp-multihop 255
  neighbor 10.0.0.100 next-hop-unchanged
end
```

Related Commands

Command	Description
address-family ipv4	Enters address family configuration mode for configuring routing sessions, such as BGP, RIP, or static routing sessions, that use standard IPv4 address prefixes.
address-family vpnv4	Enters address family configuration mode for configuring routing sessions, such as BGP, RIP, or static routing sessions, that use standard VPNv4 address prefixes.
neighbor ebgp-multihop	Accepts and attempts BGP connections to external peers residing on networks that are not directly connected.

Command	Description
neighbor next-hop-self	Configures the router as the next hop for a BGP-speaking neighbor or peer group.

neighbor password

To enable message digest5 (MD5) authentication on a TCP connection between two BGP peers, use the **neighbor password** command in router configuration mode. To disable this function, use the **no** form of this command.

neighbor {*ip-address*|*peer-group-name*} **password** *string*

no neighbor {*ip-address*|*peer-group-name*} **password**

Syntax Description

<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>string</i>	Case-sensitive password of up to 25 characters in length. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces. You cannot specify a password in the format <i>number-space-anything</i> . The space after the number can cause authentication to fail.

Command Default

MD5 is not authenticated on a TCP connection between two BGP peers.

Command Modes

Router configuration (config-router)

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.
12.4(24)T	This command was integrated into Cisco IOS Release 12.2(24)T. The password was restricted to 25 characters regardless of whether the service password-encryption command was enabled.

Usage Guidelines

You can configure MD5 authentication between two BGP peers, meaning that each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both BGP peers; otherwise, the connection between them will not be made. Configuring MD5 authentication

causes the Cisco IOS software to generate and check the MD5 digest of every segment sent on the TCP connection.

When configuring you can provide a case-sensitive password of up to 25 characters regardless of whether the **service password-encryption** command is enabled. If the length of password is more than 25 characters, an error message is displayed and the password is not accepted. The string can contain any alphanumeric characters, including spaces. A password cannot be configured in the number-space-anything format. The space after the number can cause authentication to fail. You can also use any combination of the following symbolic characters along with alphanumeric characters:

` ~ ! @ # \$ % ^ & * () - _ = + | \ }] { [" ' ; / > < . , ?



Caution

If the authentication string is configured incorrectly, the BGP peering session will not be established. We recommend that you enter the authentication string carefully and verify that the peering session is established after authentication is configured.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

If a router has a password configured for a neighbor, but the neighbor router does not, a message such as the following will appear on the console while the routers attempt to establish a BGP session between them:

```
%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's IP address]:179
```

Similarly, if the two routers have different passwords configured, a message such as the following will appear on the screen:

```
%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's IP address]:179
```

Configuring an MD5 Password in an Established BGP Session

If you configure or change the password or key used for MD5 authentication between two BGP peers, the local router will not tear down the existing session after you configure the password. The local router will attempt to maintain the peering session using the new password until the BGP hold-down timer expires. The default time period is 180 seconds. If the password is not entered or changed on the remote router before the hold-down timer expires, the session will time out.



Note

Configuring a new timer value for the hold-down timer will only take effect after the session has been reset. So, it is not possible to change the configuration of the hold-down timer to avoid resetting the BGP session.

Examples

The following example configures MD5 authentication for the peering session with the 10.108.1.1 neighbor. The same password must be configured on the remote peer before the hold-down timer expires.

```
router bgp 109
 neighbor 10.108.1.1 password bla4u00=2nkq
```

The following example configures a password for more than 25 characters when the **service password-encryption** command is disabled.

```
Router(config)# router bgp 200
Router(config-router)# bgp router-id 2.2.2.2
```

```
Router(config-router)# neighbor remote-as 3
Router(config-router)# neighbor 209.165.200.225 password 1234567891234567891234567890
% BGP: Password length must be less than or equal to 25.
Router(config-router)# do show run | i password
no service password-encryption
neighbor 209.165.200.225 password 1234567891234567891234567
```

In the following example an error message occurs when you configure a password for more than 25 characters when the **service password-encryption** command is enabled.

```
Router(config)# service password-encryption
Router(config)# router bgp 200
Router(config-router)# bgp router-id 2.2.2.2
Router(config-router)# neighbor 209.165.200.225 remote-as 3
Router(config-router)# neighbor 209.165.200.225 password 1234567891234567891234567890
% BGP: Password length must be less than or equal to 25.
Router(config-router)# do show run | i password
service password-encryption
neighbor 209.165.200.225 password 1234567891234567891234567
```

Related Commands

Command	Description
neighbor peer-group (creating)	Creates a BGP peer group.
service password-encryption	Encrypts passwords.

neighbor path-attribute discard

To configure the device to discard specific path attributes from Update messages from the specified neighbor, use the **neighbor path-attribute discard** command in router configuration mode. To disable this function, use the **no** form of this command.

neighbor {*ip-address*|*ipv6-address*} **path-attribute discard** {*attribute-value*|**range** *start-value end-value*} **in**

no neighbor {*ip-address*|*ipv6-address*} **path-attribute discard** {*attribute-value*|**range** *start-value end-value*} **in**

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>ipv6-address</i>	IPv6 address of the neighbor.
<i>attribute-value</i>	Value of a path attribute to discard, in the range from 1 to 255.
range <i>start</i>	Starting value of a range of path attributes to discard, in the range from 1 to 255.
<i>end</i>	Ending value of a range of path attributes to discard, in the range from 1 to 255.
in	Discard is applied to incoming Update messages.

Command Default

No path attributes are removed from Update messages.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS Release XE 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines

This command provides a security mechanism whereby one or more unwanted path attributes are dropped (discarded) from Update messages. The rest of the Update message is processed normally. Specify either a single attribute value or a range of attribute values to be discarded.

Attribute types 1, 2, 3, 4, 8, 14, 15, and 16 cannot be specified to be discarded. Attribute type 5 (localpref), type 9 (Originator), and type 10 (Cluster-ID) can be specified for discard for eBGP neighbors only.

Configuring this command will trigger an inbound Route Refresh to ensure that the BGP routing table is up to date.

Examples

In the following example, path attributes 100 and 128 are dropped from Update messages from the specified neighbor:

```
router bgp 65000
 neighbor 2001:DB8:1::1 path-attribute discard 100 in
 neighbor 2001:DB8:1::1 path-attribute discard 128 in
```

In the following example, all path attributes in the range from 17 to 255 are dropped from Update messages from the specified neighbor:

```
router bgp 65000
 neighbor 2001:DB8:1::1 path-attribute discard range 17 255 in
```

Related Commands

Command	Description
neighbor path-attribute treat-as-withdraw	Configures the device to treat as withdrawn any unwanted path attributes from the specified neighbor, so those prefixes are removed from the BGP routing table.
show ip bgp neighbor	Displays the configured discard and treat-as-withdraw attribute values and counters of incoming Update messages containing those attributes.
show ip bgp path-attribute discard	Displays all prefixes for which an attribute has been discarded.
show ip bgp path-attribute unknown	Displays all prefixes that have an unknown attribute.
show ip bgp vpnv4 all	Displays the unknown attributes and discarded attributes associated with a prefix.

neighbor path-attribute treat-as-withdraw

To treat-as-withdraw updates from specified neighbors containing specified path attributes, use the **neighbor path-attribute discard** command in router configuration mode. To disable this function, use the **no** form of this command.

neighbor {*ip-address*|*ipv6-address*} **path-attribute treat-as-withdraw** {*attribute-value*|**range** *start-value end-value*} **in**

no neighbor {*ip-address*|*ipv6-address*} **path-attribute treat-as-withdraw** {*attribute-value*|**range** *start-value end-value*} **in**

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>ipv6-address</i>	IPv6 address of the neighbor.
<i>attribute-value</i>	Value of a path attribute, in the range from 1 to 255.
range <i>start</i>	Starting value of a range of path attributes, in the range from 1 to 255.
<i>end</i>	Ending value of a range of path attributes, in the range from 1 to 255.
in	Command is applied to incoming Update messages.

Command Default

No prefixes are withdrawn from the BGP routing table based on path attribute.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS Release XE 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines

This command provides a security mechanism whereby updates from the specified neighbor containing the specified path attributes are “treat-as-withdraw”. Treat-as-withdraw means that the prefixes in that Update are removed from the BGP routing table.

Attribute types 1, 2, 3, 4, 8, 14, 15, and 16 cannot be specified to cause the withdrawal of a prefix. Attribute type 5 (localpref), type 9 (Originator), and type 10 (Cluster-ID) can be specified for withdrawal for eBGP neighbors only.

Configuring this command will trigger an inbound Route Refresh to ensure that the routing table is up to date.

Examples

In the following example, updates from the specified neighbor that contain path attribute 100 or 128 are treat-as-withdraw and the prefixes are withdrawn from the BGP routing table:

```
router bgp 65000
 neighbor 2001:DB8:1::1 path-attribute treat-as-withdraw 100 in
 neighbor 2001:DB8:1::1 path-attribute treat-as-withdraw 128 in
```

In the following example, updates from the specified neighbor that contain path attributes in the range from 17 to 255 are treat-as-withdraw and the prefixes are withdrawn from the BGP routing table:

```
router bgp 65000
 neighbor 2001:DB8:1::1 path-attribute treat-as-withdraw range 17 255 in
```

Related Commands

Command	Description
neighbor path-attribute discard	Configures the device to discard specific path attributes from Update messages from the specified neighbor.
show ip bgp neighbor	Displays the configured discard and treat-as-withdraw attribute values and counters of incoming Update messages containing those attributes.
show ip bgp path-attribute discard	Displays all prefixes for which an attribute has been discarded.
show ip bgp path-attribute unknown	Displays all prefixes that have an unknown attribute.
show ip bgp vpnv4 all	Displays the unknown attributes and discarded attributes associated with a prefix.

neighbor peer-group (assigning members)

To configure a BGP neighbor to be a member of a peer group, use the **neighbor peer-group** command in address family or router configuration mode. To remove the neighbor from the peer group, use the **no** form of this command.

neighbor {*ip-address*|*ipv6-address*} **peer-group** *peer-group-name*

no neighbor {*ip-address*|*ipv6-address*} **peer-group** *peer-group-name*

Syntax Description

<i>ip-address</i>	IP address of the BGP neighbor that belongs to the peer group specified by the <i>peer-group-name</i> argument.
<i>ipv6-address</i>	IPv6 address of the BGP neighbor that belongs to the peer group specified by the <i>peer-group-name</i> argument.
<i>peer-group-name</i>	Name of the BGP peer group to which this neighbor belongs.

Command Default

There are no BGP neighbors in a peer group.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
11.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(2)T	Support for IPv6 was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The neighbor at the IP address indicated inherits all the configured options of the peer group.

**Note**

Using the **no** form of the **neighbor peer-group** command removes all of the BGP configuration for that neighbor, not just the peer group association.

Examples

The following router configuration mode example assigns three neighbors to the peer group named internal:

```
router bgp 100
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 172.16.232.53 peer-group internal
 neighbor 172.16.232.54 peer-group internal
 neighbor 172.16.232.55 peer-group internal
 neighbor 172.16.232.55 filter-list 3 in
```

The following address family configuration mode example assigns three neighbors to the peer group named internal:

```
router bgp 100
 address-family ipv4 unicast
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 172.16.232.53 peer-group internal
 neighbor 172.16.232.54 peer-group internal
 neighbor 172.16.232.55 peer-group internal
 neighbor 172.16.232.55 filter-list 3 in
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
neighbor peer-group (creating)	Creates a BGP peer group.
neighbor shutdown	Disables a neighbor or peer group.

neighbor peer-group (creating)

To create a BGP or multiprotocol BGP peer group, use the **neighbor peer-group** command in address family or router configuration mode. To remove the peer group and all of its members, use the **no** form of this command.

neighbor *peer-group-name* **peer-group**

no neighbor *peer-group-name* **peer-group**

Syntax Description

<i>peer-group-name</i>	Name of the BGP peer group.

Command Default

There is no BGP peer group.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
11.0	This command was introduced.
11.1(20)CC	The nlri unicast , nlri multicast , and nlri unicast multicast keywords were added.
12.0(2)S	The nlri unicast , nlri multicast , and nlri unicast multicast keywords were added.
12.0(7)T	The nlri unicast , nlri multicast , and nlri unicast multicast keywords were removed. Address family configuration mode was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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

Often in a BGP or multiprotocol BGP speaker, many neighbors are configured with the same update policies (that is, same outbound route maps, distribute lists, filter lists, update source, and so on). Neighbors with the

same update policies can be grouped into peer groups to simplify configuration and make update calculation more efficient.

**Note**

Peer group members can span multiple logical IP subnets, and can transmit, or pass along, routes from one peer group member to another.

Once a peer group is created with the **neighbor peer-group** command, it can be configured with the **neighbor** commands. By default, members of the peer group inherit all the configuration options of the peer group. Members also can be configured to override the options that do not affect outbound updates.

All the peer group members will inherit the current configuration as well as changes made to the peer group. Peer group members will always inherit the following configuration options by default:

- remote-as (if configured)
- version
- update-source
- outbound route-maps
- outbound filter-lists
- outbound distribute-lists
- minimum-advertisement-interval
- next-hop-self

If a peer group is not configured with a remote-as option, the members can be configured with the **neighbor {ip-address | peer-group-name} remote-as** command. This command allows you to create peer groups containing external BGP (eBGP) neighbors.

Examples

The following example configurations show how to create these types of neighbor peer group:

- internal Border Gateway Protocol (iBGP) peer group
- eBGP peer group
- Multiprotocol BGP peer group

In the following example, the peer group named internal configures the members of the peer group to be iBGP neighbors. By definition, this is an iBGP peer group because the **router bgp** command and the **neighbor remote-as** command indicate the same autonomous system (in this case, autonomous system 100). All the peer group members use loopback 0 as the update source and use set-med as the outbound route map. The **neighbor internal filter-list 2 in** command shows that, except for 172.16.232.55, all the neighbors have filter list 2 as the inbound filter list.

```
router bgp 100
 neighbor internal peer-group
 neighbor internal remote-as 100
 neighbor internal update-source loopback 0
 neighbor internal route-map set-med out
 neighbor internal filter-list 1 out
 neighbor internal filter-list 2 in
 neighbor 172.16.232.53 peer-group internal
 neighbor 172.16.232.54 peer-group internal
```



```
neighbor 172.16.232.55 peer-group internal
neighbor 172.16.232.55 filter-list 3 in
```

The following example defines the peer group named external-peers without the **neighbor remote-as** command. By definition, this is an eBGP peer group because each individual member of the peer group is configured with its respective autonomous system number separately. Thus the peer group consists of members from autonomous systems 200, 300, and 400. All the peer group members have the set-metric route map as an outbound route map and filter list 99 as an outbound filter list. Except for neighbor 172.16.232.110, all of them have 101 as the inbound filter list.

```
router bgp 100
 neighbor external-peers peer-group
 neighbor external-peers route-map set-metric out
 neighbor external-peers filter-list 99 out
 neighbor external-peers filter-list 101 in
 neighbor 172.16.232.90 remote-as 200
 neighbor 172.16.232.90 peer-group external-peers
 neighbor 172.16.232.100 remote-as 300
 neighbor 172.16.232.100 peer-group external-peers
 neighbor 172.16.232.110 remote-as 400
 neighbor 172.16.232.110 peer-group external-peers
 neighbor 172.16.232.110 filter-list 400 in
```

In the following example, all members of the peer group are multicast-capable:

```
router bgp 100
 neighbor 10.1.1.1 remote-as 1
 neighbor 172.16.2.2 remote-as 2
 address-family ipv4 multicast
  neighbor mygroup peer-group
  neighbor 10.1.1.1 peer-group mygroup
  neighbor 172.16.2.2 peer-group mygroup
  neighbor 10.1.1.1 activate
  neighbor 172.16.2.2 activate
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
clear ip bgp peer-group	Removes all the members of a BGP peer group.
show ip bgp peer-group	Displays information about BGP peer groups.

neighbor prefix-list

To prevent distribution of Border Gateway Protocol (BGP) neighbor information as specified in a prefix list, a Connectionless Network Service (CLNS) filter expression, or a CLNS filter set, use the **neighbor prefix-list** command in address family or router configuration mode. To remove a filter list, use the **no** form of this command.

neighbor *{ip-address| peer-group-name}* **prefix-list** *{prefix-list-name| clns-filter-expr-name| clns-filter-set-name}* **{in| out}**

no neighbor *{ip-address| peer-group-name}* **prefix-list** *{prefix-list-name| clns-filter-expr-name| clns-filter-set-name}* **{in| out}**

Syntax Description

<i>ip-address</i>	IP address of neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>prefix-list-name</i>	Name of a prefix list. This argument is used only under router configuration mode.
<i>clns-filter-expr-name</i>	Name of a CLNS filter expression. This argument is used only under network service access point (NSAP) address family configuration mode.
<i>clns-filter-set-name</i>	Name of a CLNS filter set. This argument is used only under NSAP address family configuration mode.
in	Filter list is applied to incoming advertisements from that neighbor.
out	Filter list is applied to outgoing advertisements to that neighbor.

Command Default

All external and advertised address prefixes are distributed to BGP neighbors.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.

Release	Modification
12.2(8)T	Under address family configuration mode, the <i>prefix-list-name</i> argument was amended to specify the name of a CLNS filter expression or a CLNS filter set.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
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 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Using prefix lists is one of three ways to filter BGP advertisements. You can also use AS-path filters, defined with the **ip as-path access-list** global configuration command and used in the **neighbor filter-list** command to filter BGP advertisements. The third way to filter BGP advertisements uses access or prefix lists with the **neighbor distribute-list** command.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command with an IP address will override the value inherited from the peer group.

Use the **neighbor prefix-list** command in address family configuration mode to filter NSAP BGP advertisements.



Note

Do not apply both a **neighbor distribute-list** and a **neighbor prefix-list** command to a neighbor in any given direction (inbound or outbound). These two commands are mutually exclusive, and only one command (**neighbor distribute-list** **neighbor prefix-list**) can be applied to each inbound or outbound direction.

Examples

The following router configuration mode example applies the prefix list named *abc* to incoming advertisements from neighbor 10.23.4.1:

```
router bgp 65200
 network 192.168.1.2
 neighbor 10.23.4.1 prefix-list abc in
```

The following address family configuration mode example applies the prefix list named *abc* to incoming advertisements from neighbor 10.23.4.2:

```
router bgp 65001
 address-family ipv4 unicast
 network 192.168.2.4
 neighbor 10.23.4.2 prefix-list abc in
```

The following router configuration mode example applies the prefix list named CustomerA to outgoing advertisements to neighbor 10.23.4.3:

```
router bgp 64800
 network 192.168.3.6
 neighbor 10.23.4.3 prefix-list CustomerA out
```

The following address family configuration mode example applies the CLNS filter list set named *default-prefix-only* to outbound advertisements to neighbor 10.1.2.1:

```
clns filter-set default-prefix-only deny 49...
clns filter-set default-prefix-only permit default
!
router bgp 65202
 address-family nsap
  neighbor 10.1.2.1 activate
  neighbor 10.1.2.1 default-originate
  neighbor 10.1.2.1 prefix-list default-prefix-only out
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Enters the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Enters the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
clear ip prefix-list	Resets the hit count of the prefix list entries.
clns filter-expr	Creates an entry in a CLNS filter expression.
clns filter-set	Creates an entry in a CLNS filter set.
ip as-path access-list	Defines a BGP-related access list.
ip prefix-list	Creates an entry in a prefix list.
ip prefix-list description	Adds a text description of a prefix list.
ip prefix-list sequence-number	Enables the generation of sequence numbers for entries in a prefix list.
neighbor filter-list	Sets up a BGP filter.
show bgp nsap filter-list	Displays information about a filter list or filter list entries.
show ip bgp peer-group	Displays information about BGP peer groups.

Command	Description
show ip prefix-list	Displays information about a prefix list or prefix list entries.

neighbor remote-as

To add an entry to the BGP or multiprotocol BGP neighbor table, use the **neighbor remote-as** command in router configuration mode. To remove an entry from the table, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address* % | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number* ...]

no neighbor {*ip-address* | *ipv6-address* % | *peer-group-name*} **remote-as** *autonomous-system-number* [**alternate-as** *autonomous-system-number* ...]

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>ipv6-address</i>	IPv6 address of the neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>autonomous-system-number</i>	Number of an autonomous system to which the neighbor belongs in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the router bgp command. When used with the alternate-as keyword, up to five autonomous system numbers may be entered.
alternate-as	(Optional) Specifies an alternate autonomous system in which a potential dynamic neighbor can be identified. Up to five autonomous system numbers may be entered when this keyword is specified.

Command Default There are no BGP or multiprotocol BGP neighbor peers.

Command Modes Router configuration (config-router)

Command History	Release	Modification
	10.0	This command was introduced.
	11.0	The <i>peer-group-name</i> argument was added.
	11.1(20)CC	The nlri unicast , nlri multicast , and nlri unicast multicast keywords were added.
	12.0(7)T	The nlri unicast , nlri multicast , and nlri unicast multicast keywords were removed.
	12.2(4)T	Support for the IPv6 address family was added.
	12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
	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 % keyword was added.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH. The alternate-as keyword was added to support BGP dynamic neighbors.
	12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
	Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
	12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
	12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
	12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
	Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
	12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
15.1(1)SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

Specifying a neighbor with an autonomous system number that matches the autonomous system number specified in the **router bgp** global configuration command identifies the neighbor as internal to the local autonomous system. Otherwise, the neighbor is considered external.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

By default, neighbors that are defined using the **neighbor remote-as** command in router configuration mode exchange only unicast address prefixes. To exchange other address prefix types, such as multicast and Virtual Private Network (VPN) Version 4, neighbors must also be activated in the appropriate address family configuration mode.

Use the **alternate-as** keyword introduced in Cisco IOS Release 12.2(33)SXH to specify up to five alternate autonomous systems in which a dynamic BGP neighbor may be identified. BGP dynamic neighbor support allows BGP peering to a group of remote neighbors that are defined by a range of IP addresses. BGP dynamic neighbors are configured using a range of IP addresses and BGP peer groups. After a subnet range is configured and associated with a BGP peer group using the **bgp listen** command and a TCP session is initiated for an IP address in the subnet range, a new BGP neighbor is dynamically created as a member of that group. The new BGP neighbor will inherit any configuration or templates for the group.

The **%** keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses

asplain--65538 for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot--1.2 for example--as the only configuration format, regular expression match, and output display, with no asplain support.

**Note**

In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

To ensure a smooth transition, we recommend that all BGP speakers within an autonomous system that is identified using a 4-byte autonomous system number, be upgraded to support 4-byte autonomous system numbers.

Examples

The following example specifies that a router at the address 10.108.1.2 is an internal BGP (iBGP) neighbor in autonomous system number 65200:

```
router bgp 65200
 network 10.108.0.0
 neighbor 10.108.1.2 remote-as 65200
```

The following example specifies that a router at the IPv6 address 2001:0DB8:1:1000::72a is an external BGP (eBGP) neighbor in autonomous system number 65001:

```
router bgp 65300
 address-family ipv6 vrf sitel
 neighbor 2001:0DB8:1:1000::72a remote-as 65001
```

The following example assigns a BGP router to autonomous system 65400, and two networks are listed as originating in the autonomous system. Then the addresses of three remote routers (and their autonomous systems) are listed. The router being configured will share information about networks 10.108.0.0 and 192.168.7.0 with the neighbor routers. The first router is a remote router in a different autonomous system from the router on which this configuration is entered (an eBGP neighbor); the second **neighbor remote-as** command shows an internal BGP neighbor (with the same autonomous system number) at address 10.108.234.2; and the last **neighbor remote-as** command specifies a neighbor on a different network from the router on which this configuration is entered (also an eBGP neighbor).

```
router bgp 65400
 network 10.108.0.0
 network 192.168.7.0
 neighbor 10.108.200.1 remote-as 65200
 neighbor 10.108.234.2 remote-as 65400
 neighbor 172.29.64.19 remote-as 65300
```

The following example configures neighbor 10.108.1.1 in autonomous system 65001 to exchange only multicast routes:

```
router bgp 65001
 neighbor 10.108.1.1 remote-as 65001
 neighbor 172.31.1.2 remote-as 65001
 neighbor 172.16.2.2 remote-as 65002
 address-family ipv4 multicast
 neighbor 10.108.1.1 activate
 neighbor 172.31.1.2 activate
```

```
neighbor 172.16.2.2 activate
exit-address-family
```

The following example configures neighbor 10.108.1.1 in autonomous system 65001 to exchange only unicast routes:

```
router bgp 65001
neighbor 10.108.1.1 remote-as 65001
neighbor 172.31.1.2 remote-as 65001
neighbor 172.16.2.2 remote-as 65002
```

The following example, configurable only in Cisco IOS Release 12.2(33)SXH and later releases, configures a subnet range of 192.168.0.0/16 and associates this listen range with a BGP peer group. Note that the listen range peer group that is configured for the BGP dynamic neighbor feature can be activated in the IPv4 address family using the **neighbor activate** command. After the initial configuration on Router 1, when Router 2 starts a BGP router session and adds Router 1 to its BGP neighbor table, a TCP session is initiated, and Router 1 creates a new BGP neighbor dynamically because the IP address of the new neighbor is within the listen range subnet.

Examples

```
enable
configure terminal
router bgp 45000
  bgp log-neighbor-changes
  neighbor group192 peer-group
  bgp listen range 192.168.0.0/16 peer-group group192
  neighbor group192 remote-as 40000 alternate-as 50000
  address-family ipv4 unicast
  neighbor group192 activate
end
```

Examples

```
enable
configure terminal
router bgp 50000
  neighbor 192.168.3.1 remote-as 45000
exit
```

If the **show ip bgp summary** command is now entered on Router 1, the output shows the dynamically created BGP neighbor, 192.168.3.2.

```
Router1# show ip bgp summary
BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1
Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
*192.168.3.2  4 50000      2        2        0    0    0 00:00:37      0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1
BGP peer group group192 listen range group members:
  192.168.0.0/16
```

The following example configures a BGP process for autonomous system 65538 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asplain format. This example is supported only on Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or later releases.

```
router bgp 65538
neighbor 192.168.1.2 remote-as 65536
neighbor 192.168.3.2 remote-as 65550
neighbor 192.168.3.2 description finance
!
address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
no auto-summary
```

```
no synchronization
network 172.17.1.0 mask 255.255.255.0
exit-address-family
```

The following example configures a BGP process for autonomous system 1.2 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asdot format. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, 12.4(24)T, Cisco IOS XE Release 2.3, or a later release.

```
router bgp 1.2
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.3.2 remote-as 1.14
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
 no auto-summary
 no synchronization
 network 172.17.1.0 mask 255.255.255.0
 exit-address-family
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
bgp listen	Associates a subnet range with a BGP peer group and activates the BGP dynamic neighbors feature.
neighbor peer-group	Creates a BGP peer group.
router bgp	Configures the BGP routing process.

neighbor remove-private-as

To remove private autonomous system numbers from the autonomous system path (a list of autonomous systems that a route passes through to reach a BGP peer) in eBGP outbound routing updates, use the **neighbor remove-private-as** command in router configuration, address family configuration, or peer-group template mode. To disable this function, use the **no** form of this command.

neighbor {*ip-address*|*peer-group-name*} **remove-private-as** [**all** [**replace-as**]]

no neighbor {*ip-address*|*peer-group-name*} **remove-private-as**

Syntax Description

<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
all	(Optional) Removes all private AS numbers from the AS path in outgoing updates.
replace-as	(Optional) As long as the all keyword is specified, the replace-as keyword causes all private AS numbers in the AS path to be replaced with the router's local AS number.

Command Default

No private AS numbers are removed from the AS path.

Command Modes

Router configuration (config-router)

Address family configuration (config-router-af) [Release 15.1(2)T and later]

Peer-group template [Release 15.1(2)T and later]

Command History

Release	Modification
10.3	This command was introduced.
11.0	The <i>peer-group-name</i> 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.
15.1(2)T	This command was modified. The all keyword and the replace-as keyword were added.

Release	Modification
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

This command is available for external BGP (eBGP) neighbors only. The private AS values are 64512 to 65535.

When an update is passed to the external neighbor, if the AS path includes private AS numbers, the software will drop the private AS numbers.

Behavior Before Release 15.1(2)T

- If the AS path includes both private and public AS numbers, the software considers this to be a configuration error and does not remove the private AS numbers.
- If the AS path contains the AS number of the eBGP neighbor, the private AS numbers are not removed.
- If this command is used with confederation, it will work as long as the private AS numbers follow the confederation portion of the AS path.

Behavior in Release 15.1(2)T and Later

- The **neighbor remove-private-as** command removes private AS numbers from the AS path even if the path contains both public and private ASNs.
- The **neighbor remove-private-as** command removes private AS numbers even if the AS path contains only private AS numbers. There is no likelihood of a 0-length AS path because this command can be applied to eBGP peers only, in which case the AS number of the local router is appended to the AS path.
- The **neighbor remove-private-as** command removes private AS numbers even if the private ASNs appear before the Confederation segments in the AS path.
- Upon removing private AS numbers from the AS path, the path length of prefixes being sent out will decrease. Because the AS path length is a key element of BGP best path selection, it might be necessary to retain the path length. The **replace-as** keyword ensures that the path length is retained by replacing all removed AS numbers with the local router's AS number.
- The feature can be applied to neighbors per address family. Therefore, you can apply the feature to a neighbor in one address family and not in another, affecting update messages on the outbound side for only the address family for which the feature is configured.

Examples

The following example shows a configuration that removes the private AS number from the updates sent to 172.16.2.33. The result is that the AS path for the paths advertised by 10.108.1.1 through AS 100 will contain only "100" (as seen by autonomous system 2051).

```
router bgp 100
 neighbor 10.108.1.1 description peer with private-as
 neighbor 10.108.1.1 remote-as 65001
 neighbor 172.16.2.33 description eBGP peer
 neighbor 172.16.2.33 remote-as 2051
```

neighbor remove-private-as

```

neighbor 172.16.2.33 remove-private-as
Router-in-AS100# show ip bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/8, version 15
Paths: (1 available, best #1)
  Advertised to non peer-group peers:
    172.16.2.33
  65001
    10.108.1.1 from 10.108.1.1
      Origin IGP, metric 0, localpref 100, valid, external, best
Router-in-AS2501# show ip bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/8, version 3
Paths: (1 available, best #1)
  Not advertised to any peer
    2
    172.16.2.32 from 172.16.2.32
      Origin IGP, metric 0, localpref 100, valid, external, best

```

The following is an example of removing and replacing private ASNs using Cisco IOS Release 15.1(2)T or later. In this example, when Router A sends prefixes to the peer 172.30.0.7, all private ASNs in the AS path are replaced with the router's own ASN, which is 100.

Examples

```

router bgp 100
  bgp log-neighbor-changes
  neighbor 172.16.101.1 remote-as 1001
  neighbor 172.16.101.1 update-source Loopback0
  neighbor 172.30.0.7 remote-as 200
  neighbor 172.30.0.7 remove-private-as all replace-as
  no auto-summary

```

Router A receives 1.1.1.1 from peer 172.16.101.1, which has some private ASNs (65200, 65201, and 65201) in the AS path list, as shown in the following output:

```

RouterA# show ip bgp 1.1.1.1

BGP routing table entry for 1.1.1.1/32, version 2
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
    1          2
    1001 65200 65201 65201 1002 1003 1003
    172.16.101.1 from 172.16.101.1 (172.16.101.1)
      Origin IGP, localpref 100, valid, external, best RouterA#

```

Because Router A is configured with **neighbor 172.30.0.7 remove-private-as all replace-as**, Router A sends prefix 1.1.1.1 with all private ASNs replaced with 100:

Examples

```

RouterB# show ip bgp 1.1.1.1

BGP routing table entry for 1.1.1.1/32, version 3
Paths: (1 available, best #1, table default)
  Not advertised to any peer
    100 1001 100 100 100 1002 1003 1003
    172.30.0.6 from 172.30.0.6 (192.168.1.2)
      Origin IGP, localpref 100, valid, external, best RouterB#

```

Examples

```

router bgp 200
  bgp log-neighbor-changes
  neighbor 172.30.0.6 remote-as 100
  no auto-summary

```

Related Commands

Command	Description
neighbor remote-as	Allows entries to the BGP neighbor table.
show ip bgp neighbor	Displays entries in the BGP routing table.
show ip bgp update-group	Displays entries in the BGP routing table.

neighbor route-map

To apply a route map to incoming or outgoing routes, use the **neighbor route-map** command in address family or router configuration mode. To remove a route map, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name* | *ipv6-address* [%]} **route-map** *map-name* {**in** | **out**}

no neighbor {*ip-address* | *peer-group-name* | *ipv6-address* [%]} **route-map** *map-name* {**in** | **out**}

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP or multiprotocol BGP peer group.
<i>ipv6-address</i>	IPv6 address of the neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
<i>map-name</i>	Name of a route map.
in	Applies route map to incoming routes.
out	Applies route map to outgoing routes.

Command Default

No route maps are applied to a peer.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode was added.
12.2(4)T	Support for IPv6 was added.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The % keyword was added.

Release	Modification
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

When specified in address family configuration mode, this command applies a route map to that particular address family only. When specified in router configuration mode, this command applies a route map to IPv4 or IPv6 unicast routes only.

If an outbound route map is specified, it is proper behavior to only advertise routes that match at least one section of the route map.

If you specify a BGP or multiprotocol BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command. Specifying the command for a neighbor overrides the inbound policy that is inherited from the peer group.

The % keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces. This keyword does not need to be used for non-link-local IPv6 addresses.

Examples

The following router configuration mode example applies a route map named internal-map to a BGP incoming route from 172.16.70.24:

```
router bgp 5
 neighbor 172.16.70.24 route-map internal-map in
route-map internal-map
 match as-path 1
 set local-preference 100
```

The following address family configuration mode example applies a route map named internal-map to a multiprotocol BGP incoming route from 172.16.70.24:

```
router bgp 5
address-family ipv4 multicast
 neighbor 172.16.70.24 route-map internal-map in
route-map internal-map
 match as-path 1
 set local-preference 100
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.

Command	Description
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions that use standard VPNv6 address prefixes.
neighbor remote-as	Creates a BGP peer group.

neighbor route-reflector-client

To configure the router as a BGP route reflector and configure the specified neighbor as its client, use the **neighbor route-reflector-client** command in address family or router configuration mode. To indicate that the neighbor is not a client, use the **no** form of this command.

neighbor {*ip-address*|*ipv6-address*|*peer-group-name*} **route-reflector-client**

no neighbor {*ip-address*|*ipv6-address*|*peer-group-name*} **route-reflector-client**

Syntax Description

<i>ip-address</i>	IP address of the BGP neighbor being identified as a client.
<i>ipv6-address</i>	IPv6 address of the BGP neighbor being identified as a client.
<i>peer-group-name</i>	Name of a BGP peer group.

Command Default

There is no route reflector in the autonomous system.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
11.1	This command was introduced.
12.0(7)T	Address family configuration mode was added.
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 <i>ipv6-address</i> and <i>peer-group-name</i> arguments were added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

By default, all internal BGP (iBGP) speakers in an autonomous system must be fully meshed, and neighbors do not readvertise iBGP learned routes to neighbors, thus preventing a routing information loop. When all the clients are disabled, the local router is no longer a route reflector.

If you use route reflectors, all iBGP speakers need not be fully meshed. In the route reflector model, an Internal BGP peer is configured to be a *route reflector* responsible for passing iBGP learned routes to iBGP neighbors. This scheme eliminates the need for each router to talk to every other router.

Use the **neighbor route-reflector-client** command to configure the local router as the route reflector and the specified neighbor as one of its clients. All the neighbors configured with this command will be members of the client group and the remaining iBGP peers will be members of the nonclient group for the local route reflector.

The **bgp client-to-client reflection** command controls client-to-client reflection.

Examples

In the following router configuration mode example, the local router is a route reflector. It passes learned iBGP routes to the neighbor at 172.16.70.24.

```
router bgp 5
 neighbor 172.16.70.24 route-reflector-client
```

In the following address family configuration mode examples, the local router is a route reflector. It passes learned iBGP routes to the neighbor at 172.16.70.24.

```
router bgp 5
 address-family ipv4 unicast
 neighbor 172.16.70.24 route-reflector-client
```

```
router bgp 5
 address-family l2vpn evpn
 neighbor 172.16.70.24 route-reflector-client
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family l2vpn	Enters address family configuration mode for configuring routing sessions using Layer 2 Virtual Private Network (L2VPN) endpoint provisioning address information.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard VPNv6 address prefixes.

Command	Description
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard VPNv6 address prefixes.
bgp client-to-client reflection	Restores route reflection from a BGP route reflector to clients.
bgp cluster-id	Configures the cluster ID if the BGP cluster has more than one route reflector.
show bgp ipv6	Displays entries in the IPv6 BGP routing table.
show ip bgp	Displays entries in the BGP routing table.

neighbor route-server-client

To specify on a BGP route server that a neighbor is a route server client, use the **neighbor route-server-client** command in IPv4 or IPv6 address family configuration mode. To remove that neighbor as a route server client, use the **no** form of this command.

neighbor {*ipv4-address*|*ipv6-address*} **route-server-client** [**context** *context-name*]

no neighbor {*ipv4-address*|*ipv6-address*} **route-server-client** [**context** *context-name*]

Syntax Description

<i>ipv4-address</i>	IPv4 address of a BGP neighbor.
<i>ipv6-address</i>	IPv6 address of a BGP neighbor.
context <i>context-name</i>	(Optional) Assigns a route server context to the specified neighbor. Specify the name of a route server context, which you configure in the route-server-context command, when you want flexible policy handling.

Command Default

There are no BGP route servers or BGP route server clients.

Command Modes

IPv4 or IPv6 address family configuration (config-router-af)

Command History

Release	Modification
Cisco IOS XE 3.3S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

Use this command on a BGP route server to specify the neighbors that are route server clients.

If you want to configure flexible policy handling, you must create a route server context, which includes an import map. The import map points to a route map. The route map points to one or more **match** commands. The **match** command in the example below matches on autonomous system numbers by pointing to an access list. The access list is configured with at least one **permit** statement. The access list that is based on autonomous system numbers is configured by the **ip as-path access-list** command.

Examples

In the following example, the local router is a BGP route server. Its neighbors at 10.0.0.1 and 10.0.0.5 are its route server clients. This example enables basic route server functionality (nexthop, AS-path, and MED transparency).

```
router bgp 900
 neighbor 10.0.0.1 remote-as 100
 neighbor 10.0.0.5 remote-as 500
 address-family ipv4 unicast
 neighbor 10.0.0.1 route-server-client
 neighbor 10.0.0.5 route-server-client
 neighbor 10.0.0.1 activate
 neighbor 10.0.0.5 activate
```

In the following example, the local router is a BGP route server. Its neighbors at 10.10.10.12 and 10.10.10.13 are its route server clients. A route server context named ONLY_AS27_CONTEXT is created and applied to the neighbor at 10.10.10.13. The context uses an import map that references a route map named only_AS27_routemap. The route map matches routes permitted by access list 27. Access list 27 permits routes that have 27 in the autonomous system path.

```
router bgp 65000
  route-server-context ONLY_AS27_CONTEXT
    address-family ipv4 unicast
      import-map only_AS27_routemap
    exit-address-family
  exit-route-server-context
  !
  neighbor 10.10.10.12 remote-as 12
  neighbor 10.10.10.12 description Peer12
  neighbor 10.10.10.13 remote-as 13
  neighbor 10.10.10.13 description Peer13
  neighbor 10.10.10.21 remote-as 21
  neighbor 10.10.10.27 remote-as 27
  !
  address-family ipv4
    neighbor 10.10.10.12 activate
    neighbor 10.10.10.12 route-server-client
    neighbor 10.10.10.13 activate
    neighbor 10.10.10.13 route-server-client context ONLY_AS27_CONTEXT
    neighbor 10.10.10.21 activate
    neighbor 10.10.10.27 activate
  exit-address-family
  !
ip as-path access-list 27 permit 27
!
route-map only_AS27_routemap permit 10
  match as-path 27
!
```

Related Commands

Command	Description
route-server-context	Creates a route-server context in order to provide flexible policy handling for a BGP route server

neighbor send-community

To specify that a communities attribute should be sent to a BGP neighbor, use the **neighbor send-community** command in address family or router configuration mode. To remove the entry, use the **no** form of this command.

neighbor {*ip-address*|*ipv6-address*|*peer-group-name*} **send-community** [**both**|**standard**|**extended**]

no neighbor {*ip-address*|*ipv6-address*|*peer-group-name*} **send-community**

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>ipv6-address</i>	IPv6 address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
both	(Optional) Specifies that both standard and extended communities will be sent.
standard	(Optional) Specifies that only standard communities will be sent.
extended	(Optional) Specifies that only extended communities will be sent.

Command Default

No communities attribute is sent to any neighbor.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
10.3	This command was introduced.
11.0	The <i>peer-group-name</i> argument was added.
12.0(7)T	Address family configuration mode was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The <i>ipv6-address</i> argument was added.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Release	Modification
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

In the following router configuration mode example, the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 109
 neighbor 172.16.70.23 send-community
```

In the following address family configuration mode example, the router belongs to autonomous system 109 and is configured to send the communities attribute to its neighbor at IP address 172.16.70.23:

```
router bgp 109
 address-family ipv4 multicast
  neighbor 172.16.70.23 send-community
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes.
match community	Matches a BGP community.
neighbor remote-as	Creates a BGP peer group.
set community	Sets the BGP communities attribute.

 neighbor send-community

neighbor shutdown

To disable a neighbor or peer group or to gracefully shut down a link for maintenance, use the **neighbor shutdown** command in router configuration mode or address family configuration mode. To reenable the neighbor or peer group, use the **no** form of this command.

neighbor {*ip-address*|*peer-group-name*} **shutdown graceful** *seconds* [**community** *value*][**local-preference** *value*] [**community** *value*] [**local-preference** *value*]

no neighbor {*ip-address*|*peer-group-name*} **shutdown graceful** *seconds* [**community** *value*][**local-preference** *value*] [**community** *value*][**local-preference** *value*]

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
graceful	(Optional) Configures BGP graceful shutdown, and advertises the route with the GSHUT community and the other community, if specified.
<i>seconds</i>	(Optional) Number of seconds in which BGP graceful shutdown will occur. - Range is 30 to 65535 seconds. - Configure adequate time to allow iBGP peers to converge and to choose an alternate path as the best path.
community	Specifies whether another community value needs to added or not.
<i>value</i>	Specifies whether a value needs to added or not. The GSHUT community is set by default. You may specify a community other than the GSHUT community, which the receiving router can use to apply a routing policy. Number from 1-4294967295.
local-preference	Advertises the route with the GSHUT community and the specified local preference value.
<i>value</i>	Value of the local preference assigned to routes to the neighbor. The range is from 1 to 4294967295.

Command Default No change is made to the status of any BGP neighbor or peer group.

Command Modes Router configuration (config-router)
Address family configuration (config-router-af)

Command History	Release	Modification
	12.0	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.
	15.2(2)S	This command was modified. The graceful seconds keyword and argument, the community value keyword and argument, and the local-preference value keyword and argument were added.
	Cisco IOS XE 3.6S	This command was modified. The graceful seconds keyword and argument, the community value keyword and argument, and the local-preference value keyword and argument were added.
	Cisco IOS XE 3.7S	This command was implemented on the Cisco ASR 903 router.
	15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
	15.2(4)S	This command was implemented on the Cisco 7200 series router.

Usage Guidelines The **neighbor shutdown** command terminates any active session for the specified neighbor or peer group and removes all associated routing information. In the case of a peer group, a large number of peering sessions could be terminated suddenly.

To display a summary of BGP neighbors and peer group connections, use the **show ip bgp summary** command. Those neighbors with an Idle status and the Admin entry have been disabled by the **neighbor shutdown** command.

“State/PfxRcd” shows the current state of the BGP session or the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the **neighbor maximum-prefix** command) is reached, the string “PfxRcd” appears in the entry, the neighbor is shut down, and the connection is idle.

BGP Graceful Shutdown

Use the BGP Graceful Shutdown feature to shut down a link for planned, manual, maintenance operations and thereby reduce or eliminate packet loss. The feature can be configured globally (for all address families) or for the IPv4 VRF or IPv6 VRF address family.

Keep in mind that you should configure adequate time to allow iBGP peers to converge and to choose an alternate path as the best path. BGP will not prevent a network administrator from specifying too low a number of seconds, in which case there might not be enough time for graceful shutdown to occur.

If you use the **graceful** keyword, you must also configure at least one of the **community** or **local-preference** keywords. You may use both the **community** and **local-preference** keywords.

During graceful shutdown timer, there is no nvgen. There will be nvgen of the **neighbor shutdown** command only after the shutdown.

neighbor *ip-address* **shutdown graceful seconds local-pref value community value**

Once the graceful shutdown timer expires, the command will be nvgened as follows:

neighbor *ip-address* **shutdown**

If you reset the sessions using the **clear ip bgp** command, all timers will be reset. Therefore, there will be no graceful shutdown.

Examples

The following example disables any active session for the neighbor 172.16.70.23:

```
neighbor 172.16.70.23 shutdown
```

The following example disables all peering sessions for the peer group named internal:

```
neighbor internal shutdown
```

The following example configures the specified neighbor to be gracefully shut down in 1200 seconds and advertises the route with the well-known GSHUT community and a local preference of 400:

```
neighbor 2001:db8:a::1 shutdown graceful 1200 local-preference 400
```

Related Commands

Command	Description
ip community-list	Creates a BGP community list.
neighbor maximum-prefix	Controls how many prefixes can be received from a neighbor.
show ip bgp community	Displays the neighbors that belong to various communities.
show ip bgp summary	Displays the status of all BGP connections.

neighbor slow-peer detection

To specify a threshold time that dynamically determines a slow peer, use the **neighbor slow-peer detection** command in address-family configuration mode. To remove dynamic slow peer detection for a neighbor, use the **no** form of this command.

neighbor {*neighbor-address*|*peer-group-name*} **slow-peer detection** [**disable**|**threshold** *seconds*]

no neighbor {*neighbor-address*|*peer-group-name*} **slow-peer detection**

Syntax Description

<i>neighbor-address</i>	IP address of a BGP neighbor whose update messages are being compared to the current time to determine slowness.
<i>peer-group-name</i>	Peer group name of the bgp neighbors whose update messages are being compared to the current time to determine slowness.
disable	(Optional) Disables slow peer detection for the specified neighbor even if slow peer detection is enabled at the global, address-family level.
threshold <i>seconds</i>	(Optional) Threshold time in seconds that the timestamp of the oldest message in a peers queue can be lagging behind the current time before the peer is determined to be a slow peer. The range is from 120 to 3600; the default is 300.

Command Default

No neighbor is configured as a dynamic slow peer.

Command Modes

Address-family configuration (config-router-af)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines

Update messages are timestamped when they are formatted. The timestamp of the oldest message in a peers queue is compared to the current time to determine if the peer is lagging more than the configured number of seconds. When a peer is dynamically detected to be a slow peer, the system will send a syslog message. The

peer will be marked as recovered and another syslog message will be generated only after the peer's update group converges.

You can use this command alone just to detect a slow peer, or you can use this command with the **neighbor slow-peer split-update-group dynamic** command to move the peer to a slow update group.

**Note**

The **neighbor slow-peer detection** command performs the same function as the **bgp slow-peer detection** command (at the address-family level). The **neighbor slow-peer detection** command overrides the global, address-family level command. If the **neighbor slow-peer detection** command is unconfigured or if **no neighbor slow-peer detection** is configured, the system will inherit the global, address-family level configuration.

**Note**

The **slow-peer detection** command performs the same function through a peer policy template.

Examples

The following example sets a threshold of 400 seconds for the BGP peer at 10.4.4.4. Once the current time is more than 400 seconds later than the timestamp on the oldest message in that peers queue, the peer is determined to be a slow peer.

```
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 10.4.4.4 slow-peer detection threshold 400
Router(config-router-af)# neighbor 10.4.4.4 slow-peer split-update-group dynamic
```

In the following example, both neighbors 4.4.4.4 and 6.6.6.6 have slow peer detection enabled for them due to the global command **bgp slow-peer detection**:

```
Router(config)# router bgp 100
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 4.4.4.4 remote-as 100
Router(config-router)# neighbor 6.6.6.6 remote-as 100
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp slow-peer detection
Router(config-router-af)# neighbor 4.4.4.4 activate
Router(config-router-af)# neighbor 6.6.6.6 activate
Router(config-router-af)# no auto-summary
Router(config-router-af)# exit-address-family
Router(config-router)#
```

To disable slow peer detection for a particular peer, use the **disable** keyword. The following example disables slow peer detection for the neighbor 4.4.4.4:

```
Router(config)# router bgp 100
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 4.4.4.4 remote-as 100
Router(config-router)# neighbor 6.6.6.6 remote-as 100
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp slow-peer detection
Router(config-router-af)# neighbor 4.4.4.4 activate
Router(config-router-af)# neighbor 4.4.4.4 slow-peer detection disable
Router(config-router-af)# neighbor 6.6.6.6 activate
Router(config-router-af)# no auto-summary
Router(config-router-af)# exit-address-family
Router(config-router)#
```

Related Commands

Command	Description
bgp slow-peer detection	Specifies a threshold time that dynamically determines a slow peer at the global, address family level.
clear ip bgp slow	Moves dynamically configured slow peers back to their original update groups.
neighbor slow-peer split-update-group dynamic	Moves a dynamically detected slow peer to a slow update group.

neighbor slow-peer split-update-group dynamic

To move a dynamically detected slow peer to a slow update group, use the **neighbor slow-peer split-update-group dynamic** command in address-family configuration mode. To cancel this method of moving dynamically detected slow peers to a slow update group, use the **no** form of this command.

neighbor {*neighbor-address*|*peer-group-name*} **slow-peer split-update-group dynamic** [**permanent** | **disable**]

no neighbor {*neighbor-address*|*peer-group-name*} **slow-peer split-update-group dynamic**

Syntax Description

<i>neighbor-address</i>	IP address of a BGP neighbor peer that is moved to the slow peer group if dynamically determined to be slow.
<i>peer-group-name</i>	Peer group name of the BGP neighbor peers that are moved to the slow peer group if dynamically determined to be slow.
permanent	(Optional) Specifies that after the slow peer becomes a regular peer (converges), it is not moved back to its original update group automatically. The network administrator can use one of the clear commands to move the peer to its original update group.
disable	(Optional) Disables slow peer protection for the specified neighbor even if slow peer protection is enabled at the global, address-family level.

Command Default

No dynamically detected slow peer is moved to a slow peer update group.

Command Modes

Address-family configuration (config-router-af)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines

When a peer is dynamically detected to be a slow peer, the slow peer is moved to a slow update group. If a *static* slow peer update group exists, the dynamic slow peer is moved to the static slow peer update group; otherwise, a new slow peer updated group is created and the peer is moved to that group.

- If the **permanent** keyword is not configured, the slow peer will be moved back to its regular original update group after it becomes a regular peer (converges).
- If the **permanent** keyword is configured, the peer is not automatically moved to its original update group. You can use one of the **clear** commands to move the peer back to its original update group.

If no slow peer detection is configured, the detection will be done at the default threshold of 300 seconds.

The **neighbor slow-peer split-update-group dynamic** command will override the global configuration. However, if the **no neighbor slow-peer split-update-group dynamic** command is configured, then the peers will inherit the global address family configuration specified by the **bgp slow-peer detection** command.

Examples

In the following example, the timestamp of the oldest message in a peers queue is compared to the current time to determine if the peer is lagging more than 360 seconds. If it is, the neighbor who sent the message is determined to be a slow peer, and is put in the slow peer update group. Because the **permanent** keyword is not configured, the slow peer will be moved back to its regular original update group after it becomes a regular peer (converges).

```
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 10.4.4.4 slow-peer detection threshold 360
Router(config-router-af)# neighbor 10.4.4.4 slow-peer split-update-group dynamic
```

In the following example, both neighbors 4.4.4.4 and 6.6.6.6 have slow peer protection enabled for them due to the global command **bgp slow-peer split-update-group dynamic**:

```
Router(config)# router bgp 100
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 4.4.4.4 remote-as 100
Router(config-router)# neighbor 6.6.6.6 remote-as 100
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp slow-peer split-update-group dynamic
Router(config-router-af)# neighbor 4.4.4.4 activate
Router(config-router-af)# neighbor 6.6.6.6 activate
Router(config-router-af)# no auto-summary
Router(config-router-af)# exit-address-family
Router(config-router)#
```

To disable slow peer protection for a particular peer, use the **disable** keyword. The following example disables slow peer protection for the neighbor 4.4.4.4:

```
Router(config)# router bgp 100
Router(config-router)# bgp log-neighbor-changes
Router(config-router)# neighbor 4.4.4.4 remote-as 100
Router(config-router)# neighbor 6.6.6.6 remote-as 100
Router(config-router)# address-family ipv4
Router(config-router-af)# bgp slow-peer detection
Router(config-router-af)# neighbor 4.4.4.4 activate
Router(config-router-af)# neighbor 4.4.4.4 slow-peer split-update-group dynamic disable
Router(config-router-af)# neighbor 6.6.6.6 activate
Router(config-router-af)# no auto-summary
Router(config-router-af)# exit-address-family
Router(config-router)#
```

Related Commands

Command	Description
clear ip bgp slow	Moves dynamically configured slow peers back to their original update groups.

Command	Description
neighbor slow-peer detection	Specifies a threshold time that dynamically determines a slow peer in neighbor address family configuration mode.

neighbor slow-peer split-update-group static

To mark a BGP neighbor as a slow peer and move it to a slow update group, use the **neighbor slow-peer split-update-group static** command in address-family configuration mode. To unmark the slow peer and return it to its original update group, use the **no** form of this command.

neighbor {*neighbor-address*|*peer-group-name*} **slow-peer split-update-group static**

no neighbor {*neighbor-address*|*peer-group-name*} **slow-peer split-update-group static**

Syntax Description

<i>neighbor-address</i>	IP address of a BGP neighbor peer that is marked as slow and moved to a slow peer group.
<i>peer-group-name</i>	Peer group name of the BGP neighbor peers that are marked as slow and moved to a slow peer group.

Command Default

No peer is statically marked as slow and moved to a slow peer update group, unless through a peer policy template or configured at neighbor or peer group.

Command Modes

Address-family configuration (config-router-af)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines

Configure a static slow peer when the peer is known to be slow (perhaps due to a slow link or low processing power).

The **slow-peer split-update-group static** command performs the same function through a peer policy template.

Examples

In the following example, the neighbor with the specified IP address is marked as a slow peer and is moved to a slow update group.

```
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 172.20.2.2 slow-peer split-update-group static
```

Related Commands

Command	Description
slow-peer split-update-group static	Marks a BGP neighbor as a static slow peer and moves it to a slow update group.

neighbor soft-reconfiguration

To configure the Cisco IOS software to start storing updates, use the **neighbor soft-reconfiguration** command in router configuration mode. To not store received updates, use the **no** form of this command.

neighbor {*ip-address*|*peer-group-name*} **soft-reconfiguration inbound**

no neighbor {*ip-address*|*peer-group-name*} **soft-reconfiguration inbound**

Syntax Description

<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
inbound	Indicates that the update to be stored is an incoming update.

Command Default

Soft reconfiguration is not enabled.

Command Modes

Router configuration (config-router)

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

Entering this command starts the storage of updates, which is required to do inbound soft reconfiguration. Outbound BGP soft reconfiguration does not require inbound soft reconfiguration to be enabled.

To use soft reconfiguration, or soft reset, without preconfiguration, both BGP peers must support the soft route refresh capability, which is advertised in the open message sent when the peers establish a TCP session. Routers running Cisco IOS software releases prior to Release 12.1 do not support the route refresh capability and must clear the BGP session using the **neighbor soft-reconfiguration** command. Clearing the BGP session using the **neighbor soft-reconfiguration** command has a negative effect on network operations and should only be used as a last resort. Routers running Cisco IOS software Release 12.1 or later releases support the route refresh capability and dynamic soft resets, and can use the **clear ip bgp**{*| *address*|*peer-group name*} **in** command to clear the BGP session.

To determine whether a BGP router supports this capability, use the **show ip bgp neighbors** command. If a router supports the route refresh capability, the following message is displayed:

```
Received route refresh capability from peer.
```

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

The following example enables inbound soft reconfiguration for the neighbor 10.108.1.1. All the updates received from this neighbor will be stored unmodified, regardless of the inbound policy. When inbound soft reconfiguration is done later, the stored information will be used to generate a new set of inbound updates.

```
router bgp 100
 neighbor 10.108.1.1 remote-as 200
 neighbor 10.108.1.1 soft-reconfiguration inbound
```

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection using BGP soft reconfiguration.
neighbor remote-as	Creates a BGP peer group.
show ip bgp neighbors	Display information about the TCP and BGP connections to neighbors.

neighbor soo

To set the site-of-origin (SoO) value for a Border Gateway Protocol (BGP) neighbor or peer group, use the **neighbor soo** command in address family IPv4 VRF configuration mode. To remove the SoO value for a BGP neighbor or peer group, use the **no** form of this command.

neighbor {*ip-address*|*peer-group-name*} **soo** *extended-community-value*

no neighbor {*ip-address*|*peer-group-name*} **soo**

Syntax Description

<i>ip-address</i>	IP address of a neighboring router.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>extended-community-value</i>	Specifies the VPN extended community value. The value takes one of the following formats: • A 16-bit autonomous system number, a colon, and a 32-bit number, for example: 45000:3 • A 32-bit IP address, a colon, and a 16-bit number, for example: 192.168.10.2:51 In Cisco IOS Release 12.4(24)T, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. In Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. For more details about autonomous system number formats, see the router bgp command.

Command Default

No SoO value is set for a BGP neighbor or peer group.

Command Modes

Address family IPv4 VRF configuration (config-router-af)

Command History

Release	Modification
12.4(11)T	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)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

Use this command to set the SoO value for a BGP neighbor. The SoO value is set under address family IPv4 VRF configuration mode either directly for a neighbor or for a BGP peer group.

The SoO extended community is a BGP extended community attribute that is used to identify routes that have originated from a site so that the readvertisement of that prefix back to the source site can be prevented. The SoO extended community uniquely identifies the site from which a router has learned a route. BGP can use the SoO value associated with a route to prevent routing loops.

In releases prior to Cisco IOS Release 12.4(11)T, 12.2(33)SRB, and 12.2(33)SB, the SoO extended community attribute is configured using an inbound route map that sets the SoO value during the update process. The introduction of the **neighbor soo** and **soo** commands simplifies the SoO value configuration.



Note

A BGP neighbor or peer policy template-based SoO configuration takes precedence over an SoO value configured in an inbound route map.

In Cisco IOS Release 12.4(24)T, the Cisco implementation of 4-byte autonomous system numbers uses asdot-1.2 for example--as the only configuration format, regular expression match, and output display, with no asplain support.

In Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain-65538 for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

Examples

The following example shows how to configure an SoO value for a BGP neighbor. Under address family IPv4 VRF, a neighbor is identified and an SoO value is configured for the neighbor.

```
router bgp 45000
 address-family ipv4 vrf VRF_SOO
  neighbor 192.168.1.2 remote-as 40000
  neighbor 192.168.1.2 activate
  neighbor 192.168.1.2 soo 45000:40
end
```

The following example shows how to configure an SoO value for a BGP peer group. Under address family IPv4 VRF, a BGP peer group is configured, an SoO value is configured for the peer group, a neighbor is identified, and the neighbor is configured as a member of the peer group.

```
router bgp 45000
 address-family ipv4 vrf VRF_SOO
  neighbor SOO_GROUP peer-group
  neighbor SOO_GROUP soo 45000:65
  neighbor 192.168.1.2 remote-as 40000
  neighbor 192.168.1.2 activate
  neighbor 192.168.1.2 peer-group SOO_GROUP
end
```

The following example shows how to configure an SoO value for a BGP neighbor using 4-byte autonomous system numbers. Under address family IPv4 VRF, a neighbor is identified and an SoO value of 1.2:1 is configured for the neighbor. This example requires Cisco IOS Release 12.4(24)T, Cisco IOS XE Release 2.4, or a later release.

```
router bgp 1.2
 address-family ipv4 vrf sitel
  neighbor 192.168.1.2 remote-as 1.14
  neighbor 192.168.1.2 activate
  neighbor 192.168.1.2 soo 1.2:1
end
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Enters address family configuration mode to configure a routing session using standard IP Version 4 address prefixes.
router bgp	Configures the BGP routing process.
soo	Sets the SoO value for a BGP peer policy template.

neighbor suppress-signaling-protocol

To suppress a Virtual Private LAN Service (VPLS) signaling protocol use the **neighbor suppress-signaling-protocol** command in address family configuration or router configuration mode. To remove the entry, use the **no** form of this command.

neighbor {*ipv4-address*|*ipv6-address*|*peer-group-name*} **suppress-signaling-protocol** **ldp**

no neighbor {*ipv4-address*|*ipv6-address*|*peer-group-name*} **suppress-signaling-protocol** **ldp**

Syntax Description

<i>ipv4-address</i>	IP address of the neighbor.
<i>ipv6-address</i>	IPv6 address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
ldp	Specifies that Label Distribution Protocol (LDP) signaling will be suppressed.

Command Default

LDP signaling is not suppressed.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

If you specify that LDP signaling is suppressed by using the **ldp** keyword, BGP signaling will be enabled.

Examples

```
Device(config-router-af)# neighbor 10.10.10.1 suppress-signaling-protocol ldp
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.

Command	Description
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions such as BGP that use standard IPv6 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
address-family vpnv6	Places the router in address family configuration mode for configuring routing sessions, such as BGP, that use standard VPNv6 address prefixes.
neighbor remote-as	Creates a BGP peer group.

neighbor timers

To set the timers for a specific BGP peer or peer group, use the **neighbor timers** command in address family or router configuration mode. To clear the timers for a specific BGP peer or peer group, use the **no** form of this command.

neighbor [*ip-address*| *peer-group-name*] **timers** *keepalive* *holdtime* [*min-holdtime*]

no neighbor [*ip-address*| *peer-group-name*] **timers**

Syntax Description

<i>ip-address</i>	(Optional) A BGP peer or peer group IP address.
<i>peer-group-name</i>	(Optional) Name of the BGP peer group.
<i>keepalive</i>	Frequency (in seconds) with which the Cisco IOS software sends <i>keepalive</i> messages to its peer. The default is 60 seconds. The range is from 0 to 65535.
<i>holdtime</i>	Interval (in seconds) after not receiving a <i>keepalive</i> message that the software declares a peer dead. The default is 180 seconds. The range is from 0 to 65535.
<i>min-holdtime</i>	(Optional) Interval (in seconds) specifying the minimum acceptable hold-time from a BGP neighbor. The minimum acceptable hold-time must be less than, or equal to, the interval specified in the <i>holdtime</i> argument. The range is from 0 to 65535.

Command Default *keepalive* : 60 seconds *holdtime*: 180 seconds

Command Modes Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0	This command was introduced.
12.0(26)S	The <i>min-holdtime</i> argument was added.
12.3(7)T	The <i>min-holdtime</i> argument was added.
12.2(22)S	The <i>min-holdtime</i> argument was added.

Release	Modification
12.2(27)SBC	The <i>min-holdtime</i> argument was added and this command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	The <i>min-holdtime</i> argument was added and this command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	The <i>min-holdtime</i> argument was added and this command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The timers configured for a specific neighbor or peer group override the timers configured for all BGP neighbors using the **timers bgp** command.

When configuring the *holdtime* argument for a value of less than twenty seconds, the following warning is displayed:

```
% Warning: A hold time of less than 20 seconds increases the chances of peer flapping
If the minimum acceptable hold-time interval is greater than the specified hold-time, a notification is displayed:
```

```
% Minimum acceptable hold time should be less than or equal to the configured hold time
```



Note

When the minimum acceptable hold-time is configured on a BGP router, a remote BGP peer session is established only if the remote peer is advertising a hold-time that is equal to, or greater than, the minimum acceptable hold-time interval. If the minimum acceptable hold-time interval is greater than the configured hold-time, the next time the remote session tries to establish, it will fail and the local router will send a notification stating "unacceptable hold time."

Examples

The following example changes the keepalive timer to 70 seconds and the hold-time timer to 210 seconds for the BGP peer 192.168.47.0:

```
router bgp 109
 neighbor 192.168.47.0 timers 70 210
```

The following example changes the keepalive timer to 70 seconds, the hold-time timer to 130 seconds, and the minimum hold-time interval to 100 seconds for the BGP peer 192.168.1.2:

```
router bgp 45000
 neighbor 192.168.1.2 timers 70 130 100
```

neighbor translate-update

To enable customer-edge (CE) devices, which are not capable of multicast BGP (mBGP) routing, to participate in a multicast session, use the **neighbor translate-update** command in address-family configuration mode. To disable mBGP routing on CE devices, use the **no** form of the command.

neighbor {*ipv4-address* | *ipv6-address*} **translate-update multicast** [**unicast**]

no neighbor {*ipv4-address* | *ipv6-address*} **translate-update multicast** [**unicast**]

Syntax Description

<i>ipv4-address</i>	Specifies the multicast IPv4 address for the BGP neighbor.
<i>ipv6-address</i>	Specifies the multicast IPv6 address for the BGP neighbor.
multicast	Specifies multicast address prefixes.
unicast	(Optional) Specifies unicast address prefixes.

Command Default

Command Modes

Address family configuration (config-router-af)

Command History

Release	Modification
12.0(26)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(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 introduced on Cisco ASR 1000 Series Routers.
15.4(1)S	This command was modified. Support for translate-update was extended to VRF address-families.

Release	Modification
Cisco IOS XE Release 3.11S	This command was modified. Support for translate-update was extended to VRF address-families.

Usage Guidelines

The **translate-update** keyword in the neighbor command enables CE devices, which cannot send BGP Reverse Path Forwarding (RPF) multicast routes, to advertise its routes to multicast VRF-Lite and multicast VPN (mVPN) for VPNv4 and VPNv6 neighbors. These routes are also advertised through IPv6 over IPv4 tunnel. The **translate-update** keyword is configured on the provider-edge (PE) devices for multicast routing to neighbor CE devices using the **address-family ipv4 vrf** or the **address-family ipv6 vrf** command. The PE devices translate the updates from unicast to multicast on CE devices and put them in the BGP VRF routing table of the PE devices, as multicast updates, for processing. If the optional keyword **unicast** is also configured, the updates that are not translated to multicast are also placed in the unicast queue of the PE devices and populate the unicast BGP VRF table. The translation from unicast to multicast occurs from CE devices to PE devices only. Prefixes are only advertised from CE devices to the multicast neighbors of the PE devices.

Prior to configuring the translate-update feature, you must enable multicast VRF on the PE devices, along with an active VRF session with the CE devices.

Examples

The following example shows how to configure the translate-update feature for an IPv4 VRF address-family named v1 and BGP neighbor n2:



Note

Peer-template configuration for BGP neighbor is not supported for this feature due to conflicts with the earlier versions of Cisco software.

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# address-family ipv4 vrf v1
Device(config-router-af)# neighbor n2 peer-group
Device(config-router-af)# neighbor n2 remote-as 4
Device(config-router-af)# neighbor 10.1.1.1 peer-group n2
Device(config-router-af)# neighbor 10.1.1.1 activate
Device(config-router-af)# neighbor 10.1.1.1 translate-update multicast unicast
Device(config-router-af)# end
```

The following is sample output from the **show bgp vpnv4 multicast vrf** command. If the “State/PfxRcd” field displays “NoNeg”, it indicates that the neighbor has a translate-update session:

```
Device# show bgp vpnv4 multicast vrf v1 summary

BGP router identifier 10.1.3.1, local AS number 65000
BGP table version is 8, main routing table version 8
7 network entries using 1792 bytes of memory
8 path entries using 960 bytes of memory
5/3 BGP path/bestpath attribute entries using 1280 bytes of memory
3 BGP AS-PATH entries using 88 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 4168 total bytes of memory
BGP activity 23/2 prefixes, 33/9 paths, scan interval 60 secs

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.1.1.1      4        4       5      10        1     0    00:01:10 (NoNeg)
```



```
10.1.3.2          4          2          12          10          8          0          0 00:01:33
```

Related Commands

Command	Description
address-family ipv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family ipv6	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv6 address prefixes.
neighbor peer-group	Creates a BGP or multiprotocol BGP peer group.
neighbor remote-as	Adds an entry to a BGP or multiprotocol BGP neighbor table.
neighbor activate	Enables exchange of information with a BGP neighbor.
show bgp vpnv4 multicast	Displays Virtual Private Network Version 4 (VPNv4) multicast entries in a BGP table.

neighbor transport

To enable a TCP transport session option for a Border Gateway Protocol (BGP) session, use the **neighbor transport** command in router or address family configuration mode. To disable a TCP transport session option for a BGP session, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **transport** {**connection-mode** {**active** | **passive**} | **path-mtu-discovery** [**disable**] | **multi-session**}

no neighbor {*ip-address* | *peer-group-name*} **transport** {**connection-mode** | **path-mtu-discovery** | **multi-session**}

Syntax Description

<i>ip-address</i>	IP address of the BGP neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
connection-mode	Specifies the type of connection (active or passive).
active	Specifies an active connection.
passive	Specifies a passive connection.
path-mtu-discovery	Enables TCP transport path maximum transmission unit (MTU) discovery. TCP path MTU discovery is enabled by default.
multi-session	Enables a separate TCP transport session for each address family.
disable	Disables TCP path MTU discovery.

Command Default

If this command is not configured, TCP path MTU discovery is enabled by default, but no other TCP transport session options are enabled.

Command Modes

Router configuration (config-router)
Address family configuration (config-router-af)

Command History

Release	Modification
12.4	This command was introduced.
12.2(33)SRA	This command was modified. The path-mtu-discovery keyword was added.

Release	Modification
12.2(33)SRB	This command was modified. The multi-session , single-session , and disable keywords were 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.
12.4(20)T	This command was modified. The path-mtu-discovery keyword was added.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.1(03)S	This command was modified. The single-session keyword was removed. Support for single-session and multi-session transport was integrated in this command.

Usage Guidelines

This command is used to specify various transport options. An active or passive transport connection can be specified for a BGP session. TCP transport path MTU discovery can be enabled to allow a BGP session to take advantage of larger MTU links. Use the **show ip bgp neighbors** command to determine whether TCP path MTU discovery is enabled.

In Cisco IOS Release 12.2(33)SRB and later releases, options can be specified for the transport of address family traffic using a single TCP session or to enable a separate TCP session for each address family. Multiple TCP sessions are used to support Multitopology Routing (MTR), and the single session option is available for backwards compatibility for non-MTR configurations and for scalability purposes.

In Cisco IOS Release 12.2(33)SRB and later releases, the ability to disable TCP path MTU discovery, for a single neighbor or for an inheriting peer or peer group, was added. If you use the **disable** keyword to disable discovery, discovery is also disabled on any peer or peer group that inherits the template in which you disabled discovery.

Examples:

The following example shows how to configure the TCP transport connection to be active for a single internal BGP (iBGP) neighbor:

```
router bgp 45000
neighbor 172.16.1.2 remote-as 45000
neighbor 172.16.1.2 activate
neighbor 172.16.1.2 transport connection-mode active
end
```

The following example shows how to configure the TCP transport connection to be passive for a single external BGP (eBGP) neighbor:

```
router bgp 45000
neighbor 192.168.1.2 remote-as 40000
neighbor 192.168.1.2 activate
neighbor 192.168.1.2 transport connection-mode passive
end
```

The following example shows how to disable TCP path MTU discovery for a single BGP neighbor:

```
router bgp 45000
neighbor 172.16.1.2 remote-as 45000
```

```
neighbor 172.16.1.2 activate
no neighbor 172.16.1.2 transport path-mtu-discovery
end
```

The following example shows how to reenable TCP path MTU discovery for a single BGP neighbor, if TCP path MTU discovery is disabled:

```
router bgp 45000
neighbor 172.16.1.2 remote-as 45000
neighbor 172.16.1.2 activate
neighbor 172.16.1.2 transport path-mtu-discovery
end
```

The following example shows how to enable a separate TCP session for each address family for an MTR topology configuration:

```
router bgp 45000
scope global
neighbor 172.16.1.2 remote-as 45000
neighbor 172.16.1.2 transport multi-session
address-family ipv4
topology VIDEO
bgp tid 100
neighbor 172.16.1.2 activate
end
```

The following example shows how to disable TCP path MTU discovery and verify that it is disabled:

```
router bgp 100
bgp log-neighbor-changes
timers bgp 0 0
redistribute static
neighbor 10.4.4.4 remote-as 100
neighbor 10.4.4.4 update-source Loopback 0
!end

Device# show ip bgp neighbors 10.4.4.4 | include path
Used as bestpath:          n/a          0
Used as multipath:         n/a          0
Transport(tcp) path-mtu-discovery is enabled
Option Flags: nagle, path mtu capable
Device#
Device# configure terminal
Device(config)# router bgp 100
Device(config-router)# neighbors 10.4.4.4 transport path-mtu-discovery disable
Device(config-router)# end
Device# show ip bgp neighbor 10.4.4.4 | include path
Used as bestpath:          n/a          0
Used as multipath:         n/a          0
Transport(tcp) path-mtu-discovery is disabled
```

Related Commands

Command	Description
bgp tid	Configures BGP to accept routes with a specified topology ID.
bgp transport	Enables transport session parameters globally for all BGP neighbor sessions.
scope	Defines the scope for a BGP routing session and enters router scope configuration mode.
show ip bgp neighbors	Displays information about BGP and TCP connections to neighbors.

Command	Description
topology (BGP)	Configures a process to route IP traffic under the specified topology instance.

neighbor ttl-security

To secure a Border Gateway Protocol (BGP) peering session and to configure the maximum number of hops that separate two external BGP (eBGP) peers, use the **neighbor ttl-security** command in address-family or router configuration mode. To disable this feature, use the **no** form of this command.

neighbor *neighbor-address* **ttl-security hops** *hop-count*

no neighbor *neighbor-address* **ttl-security hops** *hop-count*

Syntax Description

<i>neighbor-address</i>	IP address of the neighbor.
hops <i>hop-count</i>	Number of hops that separate the eBGP peers. The TTL value is calculated by the router from the configured <i>hop-count</i> argument. The value for the <i>hop-count</i> argument is a number between 1 and 254.

Command Default

No default behavior or values

Command Modes

Address-family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

The **neighbor ttl-security** command provides a lightweight security mechanism to protect BGP peering sessions from CPU utilization-based attacks. These types of attacks are typically brute force Denial of Service (DoS) attacks that attempt to disable the network by flooding the network with IP packets that contain forged source and destination IP addresses in the packet headers.

This feature leverages designed behavior of IP packets by accepting only IP packets with a TTL count that is equal to or greater than the locally configured value. Accurately forging the TTL count in an IP packet is

generally considered to be impossible. Accurately forging a packet to match the TTL count from a trusted peer is not possible without internal access to the source or destination network.

This feature should be configured on each participating router. It secures the BGP session in the incoming direction only and has no effect on outgoing IP packets or the remote router. When this feature is enabled, BGP will establish or maintain a session only if the TTL value in the IP packet header is equal to or greater than the TTL value configured for the peering session. This feature has no effect on the BGP peering session, and the peering session can still expire if keepalive packets are not received. If the TTL value in a received packet is less than the locally configured value, the packet is silently discarded and no Internet Control Message Protocol (ICMP) message is generated. This is designed behavior; a response to a forged packet is not necessary.

To maximize the effectiveness of this feature, the *hop-count* value should be strictly configured to match the number of hops between the local and external network. However, you should also take path variation into account when configuring this feature for a multihop peering session.

The following restrictions apply to the configuration of this command:

- This feature is not supported for internal BGP (iBGP) peers or iBGP peer groups.
- The **neighbor ttl-security** command cannot be configured for a peer that is already configured with the **neighbor ebgp-multihop** command. The configuration of these commands is mutually exclusive, and only one of these commands is needed to enable a multihop eBGP peering session. An error message will be displayed in the console if you attempt to configure both commands for the same peering session.
- The effectiveness of this feature is reduced in large-diameter multihop peerings. In the event of a CPU utilization-based attack against a BGP router that is configured for large-diameter peering, you may still need to shut down the affected peering sessions to handle the attack.
- This feature is not effective against attacks from a peer that has been compromised inside of your network. This restriction also includes peers that are on the network segment between the source and destination network.

Examples

The following example sets the hop count to 2 for a directly connected neighbor. Because the *hop-count* argument is set to 2, BGP will accept only IP packets with a TTL count in the header that is equal to or greater than 253. If a packet is received with any other TTL value in the IP packet header, the packet will be silently discarded.

```
neighbor 10.0.0.1 ttl-security hops 2
```

Related Commands

Command	Description
neighbor ebgp-multihop	Accepts or initiates BGP connections to external peers residing on networks that are not directly connected.
show ip bgp neighbors	Displays information about the TCP and BGP connections to neighbors.

neighbor unsuppress-map

To selectively advertise routes previously suppressed by the **aggregate-address** command, use the **neighbor unsuppress-map** command in address family or router configuration mode. To restore the system to the default condition, use the **no** form of this command.

neighbor {*ip-address*|*peer-group-name*} **unsuppress-map** *route-map-name*

no neighbor {*ip-address*|*peer-group-name*} **unsuppress-map** *route-map-name*

Syntax Description

<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>route-map-name</i>	Name of a route map.

Command Default

No routes are unsuppressed.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)T	Address family configuration mode 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.

Usage Guidelines

Use of the **neighbor unsuppress-map** command allows specified suppressed routes to be advertised.

Examples

The following BGP router configuration shows that routes specified by a route map named map1 are suppressed:

```
access-list 3 deny 172.16.16.6
access-list 3 permit any
route-map map1 permit 10
match ip address 3
!
```



```

router bgp 65000
network 172.16.0.0
neighbor 192.168.1.2 remote-as 40000
aggregate-address 172.0.0.0 255.0.0.0 suppress-map map1
neighbor 192.168.1.2 unsuppress-map map1
neighbor 192.168.1.2 activate

```

The following example shows the routes specified by internal-map being unsuppressed for neighbor 172.16.16.6:

```

router bgp 100
address-family ipv4 multicast
network 172.16.0.0
neighbor 172.16.16.6 unsuppress-map internal-map

```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the routing in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
aggregate-address	Creates an aggregate entry in a BGP routing table.
neighbor route-map	Applies a route map to inbound or outbound routes.

neighbor update-source

To have the Cisco software allow Border Gateway Protocol (BGP) sessions to use any operational interface for TCP connections, use the **neighbor update-source** command in router configuration mode. To restore the interface assignment to the closest interface, which is called the best local address, use the **no** form of this command.

neighbor {*ip-address* | *ipv6-address* [%] | *peer-group-name*} **update-source** *interface-type interface-number*

neighbor {*ip-address* | *ipv6-address* [%] | *peer-group-name*} **update-source** *interface-type interface-number*

Syntax Description

<i>ip-address</i>	IPv4 address of the BGP-speaking neighbor.
<i>ipv6-address</i>	IPv6 address of the BGP-speaking neighbor.
%	(Optional) IPv6 link-local address identifier. This keyword needs to be added whenever a link-local IPv6 address is used outside the context of its interface.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>interface-type</i>	Interface type.
<i>interface-number</i>	Interface number.

Command Default

Best local address

Command Modes

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.2(4)T	The <i>ipv6-address</i> argument was added.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
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.

Release	Modification
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The % 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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 series routers.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

This command can work in conjunction with the loopback interface feature described in the “Interface Configuration Overview” chapter of the Cisco IOS Interface and Hardware Component Configuration Guide.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

The **neighbor update-source** command must be used to enable IPv6 link-local peering for internal or external BGP sessions.

The % keyword is used whenever link-local IPv6 addresses are used outside the context of their interfaces and for these link-local IPv6 addresses you must specify the interface they are on. The syntax becomes <IPv6 local-link address>%<interface name>, for example, FE80::1%Ethernet1/0. Note that the interface type and number must not contain any spaces, and be used in full-length form because name shortening is not supported in this situation. The % keyword and subsequent interface syntax is not used for non-link-local IPv6 addresses.

Examples

The following example sources BGP TCP connections for the specified neighbor with the IP address of the loopback interface rather than the best local address:

```
router bgp 65000
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 110
 neighbor 172.16.2.3 update-source Loopback0
```

The following example sources IPv6 BGP TCP connections for the specified neighbor in autonomous system 65000 with the global IPv6 address of loopback interface 0 and the specified neighbor in autonomous system 65400 with the link-local IPv6 address of Fast Ethernet interface 0/0. Note that the link-local IPv6 address of FE80::2 is on Ethernet interface 1/0.

```
router bgp 65000
 neighbor 3ffe::3 remote-as 65000
 neighbor 3ffe::3 update-source Loopback0
 neighbor fe80::2%Ethernet1/0 remote-as 65400
 neighbor fe80::2%Ethernet1/0 update-source FastEthernet 0/0
 address-family ipv6
 neighbor 3ffe::3 activate
 neighbor fe80::2%Ethernet1/0 activate
 exit-address-family
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a BGP neighboring router.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.

neighbor version

To configure the Cisco IOS software to accept only a particular BGP version, use the **neighbor version** command in router configuration mode. To use the default version level of a neighbor, use the **no** form of this command.

neighbor *{ip-address| peer-group-name}* **version number**

no neighbor *{ip-address| peer-group-name}* **version number**

Syntax Description

<i>ip-address</i>	IP address of the BGP-speaking neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>number</i>	BGP version number. The version can be set to 2 to force the software to use only Version 2 with the specified neighbor. The default is to use Version 4 and dynamically negotiate down to Version 2 if requested.

Command Default

BGP Version 4

Command Modes

Router configuration (config-router)

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

Entering this command disables dynamic version negotiation.

**Note**

The Cisco implementation of BGP in Cisco IOS Release 12.0(5)T or earlier releases supports BGP Versions 2, 3, and 4, with dynamic negotiation down to Version 2 if a neighbor does not accept BGP Version 4 (the default version). The Cisco implementation of BGP in Cisco IOS Release 12.0(6)T or later releases supports BGP Version 4 only and does not support dynamic negotiation down to Version 2.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

The following example locks down to Version 4 of the BGP protocol:

```
router bgp 109
 neighbor 172.16.27.2 version 4
```

Related Commands

Command	Description
neighbor remote-as	Creates a BGP peer group.

neighbor weight

To assign a weight to a neighbor connection, use the **neighbor weight** command in address family or router configuration mode. To remove a weight assignment, use the **no** form of this command.

neighbor {*ip-address*|*peer-group-name*} **weight** *number*

no neighbor {*ip-address*|*peer-group-name*} **weight** *number*

Syntax Description

<i>ip-address</i>	IP address of the neighbor.
<i>peer-group-name</i>	Name of a BGP peer group.
<i>number</i>	Weight to assign. Acceptable values are from 0 to 65535.

Command Default

Routes learned through another BGP peer have a default weight of 0 and routes sourced by the local router have a default weight of 32768.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode 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.

Usage Guidelines

All routes learned from this neighbor will have the assigned weight initially. The route with the highest weight will be chosen as the preferred route when multiple routes are available to a particular network.

The weights assigned with the **set weight** route-map command override the weights assigned using the **neighbor weight** command.

**Note**

For weight changes to take effect, use of the **clear ip bgp peer-group *** command may be necessary.

If you specify a BGP peer group by using the *peer-group-name* argument, all the members of the peer group will inherit the characteristic configured with this command.

Examples

The following router configuration mode example sets the weight of all routes learned via 172.16.12.1 to 50:

```
router bgp 109
 neighbor 172.16.12.1 weight 50
```

The following address family configuration mode example sets the weight of all routes learned via 172.16.12.1 to 50:

```
router bgp 109
 address-family ipv4 multicast
 neighbor 172.16.12.1 weight 50
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard Virtual Private Network (VPN) Version 4 address prefixes.
neighbor distribute-list	Distributes BGP neighbor information as specified in an access list.
neighbor filter-list	Sets up a BGP filter.
neighbor remote-as	Creates a BGP peer group.

network (BGP and multiprotocol BGP)

To specify the networks to be advertised by the Border Gateway Protocol (BGP) and multiprotocol BGP routing processes, use the **network** command in address family or router configuration mode. To remove an entry from the routing table, use the **no** form of this command.

network {*network-number* [**mask** *network-mask*]} [*nsap-prefix*] [**route-map** *map-tag*]

no network {*network-number* [**mask** *network-mask*]} [*nsap-prefix*] [**route-map** *map-tag*]

Syntax Description

<i>network-number</i>	Network that BGP or multiprotocol BGP will advertise.
mask <i>network-mask</i>	(Optional) Network or subnetwork mask with mask address.
<i>nsap-prefix</i>	Network service access point (NSAP) prefix of the Connectionless Network Service (CLNS) network that BGP or multiprotocol BGP will advertise. This argument is used only under NSAP address family configuration mode.
route-map <i>map-tag</i>	(Optional) Identifier of a configured route map. The route map should be examined to filter the networks to be advertised. If not specified, all networks are advertised. If the keyword is specified, but no route map tags are listed, no networks will be advertised.

Command Default

No networks are specified.

Command Modes

Address family configuration (config-router-af)
Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0	The limit of 200 network commands per BGP router was removed.
11.1(20)CC	The nlri unicast , nlri multicast , and nlri unicast multicast keywords were added.

Release	Modification
12.0(7)T	The nlri unicast , nlri multicast , and nlri unicast multicast keywords were removed. Address family configuration mode was added.
12.2(8)T	The <i>nsap-prefix</i> argument was added to address family configuration mode.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

BGP and multiprotocol BGP networks can be learned from connected routes, from dynamic routing, and from static route sources.

The maximum number of **network** commands you can use is determined by the resources of the router, such as the configured NVRAM or RAM.

Examples

The following example sets up network 10.108.0.0 to be included in the BGP updates:

```
router bgp 65100
 network 10.108.0.0
```

The following example sets up network 10.108.0.0 to be included in the multiprotocol BGP updates:

```
router bgp 64800
 address family ipv4 multicast
 network 10.108.0.0
```

The following example advertises NSAP prefix 49.6001 in the multiprotocol BGP updates:

```
router bgp 64500
 address-family nsap
 network 49.6001
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Enters the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.

Command	Description
address-family vpnv4	Enters the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
default-information originate (BGP)	Allows the redistribution of network 0.0.0.0 into BGP.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
router bgp	Configures the BGP routing process.

network backdoor

To specify a backdoor route to a BGP-learned prefix that provides better information about the network, use the **network backdoor** command in address family or router configuration mode. To remove an address from the list, use the **no** form of this command.

network *ip-address* **backdoor**

no network *ip-address* **backdoor**

Syntax Description

<i>ip-address</i>	IP address of the network to which you want a backdoor route.

Command Default

No network is marked as having a back door.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	Address family configuration mode 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.

Usage Guidelines

A backdoor network is assigned an administrative distance of 200. The objective is to make Interior Gateway Protocol (IGP) learned routes preferred. A backdoor network is treated as a local network, except that it is not advertised. A network that is marked as a back door is not sourced by the local router, but should be learned from external neighbors. The BGP best path selection algorithm does not change when a network is configured as a back door.

Examples

The following address family configuration example configures network 10.108.0.0 as a local network and network 192.168.7.0 as a backdoor network:

```
router bgp 109
address-family ipv4 multicast
```

```
network 10.108.0.0
network 192.168.7.0 backdoor
```

The following router configuration example configures network 10.108.0.0 as a local network and network 192.168.7.0 as a backdoor network:

```
router bgp 109
network 10.108.0.0
network 192.168.7.0 backdoor
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.
distance bgp	Allows the use of external, internal, and local administrative distances that could be a better route to a node.
network (BGP and multiprotocol BGP)	Specifies networks to be advertised by the BGP and multiprotocol BGP routing processes.
router bgp	Assigns an absolute weight to a BGP network.

 network backdoor



BGP Commands: 0 through show bgp

- [redistribute \(BGP to ISO IS-IS\), page 541](#)
- [redistribute \(IP\), page 544](#)
- [redistribute \(ISO IS-IS to BGP\), page 554](#)
- [redistribute dvmrp, page 557](#)
- [router bgp, page 559](#)
- [route-server-context, page 565](#)
- [scope, page 567](#)
- [set as-path, page 569](#)
- [set comm-list delete, page 573](#)
- [set community, page 576](#)
- [set dampening, page 578](#)
- [set extcomm-list delete, page 581](#)
- [set extcommunity cost, page 583](#)
- [set extcommunity rt, page 587](#)
- [set extcommunity soo, page 592](#)
- [set extcommunity vpn-distinguisher, page 596](#)
- [set ip dscp \(bmp\), page 599](#)
- [set ip next-hop self \(BGP\), page 601](#)
- [set ip next-hop \(BGP\), page 602](#)
- [set ipv6 next-hop \(BGP\), page 605](#)
- [set metric \(BGP-OSPF-RIP\), page 608](#)
- [set metric-type internal, page 611](#)
- [set origin \(BGP\), page 613](#)
- [set traffic-index, page 615](#)

- [set weight, page 617](#)
- [show bgp all community, page 620](#)
- [show bgp all neighbors, page 624](#)
- [show bgp ipv6, page 630](#)
- [show bgp l2vpn evpn, page 635](#)
- [show bgp l2vpn vpls, page 639](#)
- [show bgp mvpn, page 643](#)
- [show bgp nsap, page 645](#)
- [show bgp nsap community, page 648](#)
- [show bgp nsap community-list, page 652](#)
- [show bgp nsap dampened-paths, page 655](#)
- [show bgp nsap dampening, page 657](#)
- [show bgp nsap filter-list, page 661](#)
- [show bgp nsap flap-statistics, page 664](#)
- [show bgp nsap inconsistent-as, page 667](#)
- [show bgp nsap neighbors, page 670](#)
- [show bgp nsap paths, page 679](#)
- [show bgp nsap quote-regexp, page 681](#)
- [show bgp nsap regexp, page 684](#)
- [show bgp nsap summary, page 687](#)
- [show bgp vpnv6 multicast, page 690](#)
- [show bgp vpnv6 unicast, page 692](#)

redistribute (BGP to ISO IS-IS)

To redistribute routes from a Border Gateway Protocol (BGP) autonomous system into an International Organization for Standardization (ISO) Intermediate System-to-Intermediate System (IS-IS) routing process, use the **redistribute** command in router configuration mode. To remove the **redistribute** command from the configuration file and restore the system to its default condition where the software does not redistribute BGP routes into IS-IS, use the **no** form of this command.

redistribute *protocol autonomous-system-number* [*route-type*] [**route-map** *map-tag*]

no redistribute *protocol autonomous-system-number* [*route-type*] [**route-map** *map-tag*]

Syntax Description

<i>protocol</i>	Source protocol from which routes are being redistributed. It must be the bgp keyword. The bgp keyword is used to redistribute dynamic routes.
<i>autonomous-system-number</i>	The autonomous system number of the BGP routing process from which BGP routes are redistributed into IS-IS. The range of values for this argument is any valid autonomous system number from 1 to 65535. - In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. - In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the router bgp command.
<i>route-type</i>	(Optional) The type of route to be redistributed. It can be one of the following keywords: clns or ip. The default is ip. - The clns keyword is used to redistribute BGP routes with network service access point (NSAP) addresses into IS-IS. - The ip keyword is used to redistribute BGP routes with IP addresses into IS-IS.

route-map <i>map-tag</i>	(Optional) Identifier of a configured route map. The route map should be examined to filter the importation of routes from this source routing protocol to IS-IS. If not specified, all routes are redistributed. If the keyword is specified, but no route map tags are listed, no routes will be imported.

Command Default

Route redistribution from BGP to ISO IS-IS is disabled.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
12.2(8)T	This command was modified. The clns keyword was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added. Support for changing autonomous system number of the BGP routing process was removed.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

The **clns** keyword must be specified to redistribute NSAP prefix routes from BGP into an ISO IS-IS routing process. This version of the **redistribute** command is used only under router configuration mode for IS-IS processes.

**Note**

Be aware that when you configure the **no redistribute bgp autonomous-system route-map map-name** command under the **router isis** router configuration command, IS-IS removes the entire **redistribute** command, not just the route map. This behavior differs from the **no redistribute isis** command configured under the **router bgp** router configuration command, which removes a keyword.

Examples

The following example configures NSAP prefix routes from BGP autonomous system 64500 to be redistributed into the IS-IS routing process called osi-proc-17:

```
router isis osi-proc-17
 redistribute bgp 64500 clns
```

Related Commands

Command	Description
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
router bgp	Configures the BGP routing process.
show route-map	Displays all route maps configured or only the one specified.

redistribute (IP)

To redistribute routes from one routing domain into another routing domain, use the **redistribute** command in the appropriate configuration mode. To disable all or some part of the redistribution (depending on the protocol), use the **no** form of this command. See the “Usage Guidelines” section for detailed, protocol-specific behaviors.

redistribute *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*autonomous-system-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] [**nssa-only**]

no redistribute *protocol* [*process-id*] {**level-1** | **level-1-2** | **level-2**} [*autonomous-system-number*] [**metric** {*metric-value* | **transparent**}] [**metric-type** *type-value*] [**match** {**internal** | **external 1** | **external 2**}] [**tag** *tag-value*] [**route-map** *map-tag*] [**subnets**] [**nssa-only**]

Syntax Description

<i>protocol</i>	Source protocol from which routes are being redistributed. It can be one of the following keywords: bgp, connected, eigrp, isis, mobile, ospf, rip, or static [ip]. The static [ip] keyword is used to redistribute IP static routes. The optional ip keyword is used when redistributing into the Intermediate System-to-Intermediate System (IS-IS) protocol. The connected keyword refers to routes that are established automatically by virtue of having enabled IP on an interface. For routing protocols such as Open Shortest Path First (OSPF) and IS-IS, these routes will be redistributed as external to the autonomous system.
<i>process-id</i>	(Optional) For the bgp or eigrp keyword, this is an autonomous system number, which is a 16-bit decimal number. For the isis keyword, this is an optional <i>tag</i> value that defines a meaningful name for a routing process. You can specify only one IS-IS process per router. Creating a name for a routing process means that you use names when configuring routing. For the ospf keyword, this is an appropriate OSPF process ID from which routes are to be redistributed. This identifies the routing process. This value takes the form of a nonzero decimal number. For the rip keyword, no <i>process-id</i> value is needed. By default, no process ID is defined.
level-1	Specifies that, for IS-IS, Level 1 routes are redistributed into other IP routing protocols independently.

level-1-2	Specifies that, for IS-IS, both Level 1 and Level 2 routes are redistributed into other IP routing protocols.
level-2	Specifies that, for IS-IS, Level 2 routes are redistributed into other IP routing protocols independently.
<i>autonomous-system-number</i>	(Optional) Autonomous system number for the redistributed route. The range is from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the router bgp command.
metric <i>metric-value</i>	(Optional) When redistributing from one OSPF process to another OSPF process on the same router, the metric will be carried through from one process to the other if no metric value is specified. When redistributing other processes to an OSPF process, the default metric is 20 when no metric value is specified. The default value is 0.
metric transparent	(Optional) Causes Routing Information Protocol (RIP) to use the routing table metric for redistributed routes as the RIP metric.
metric-type <i>type value</i>	(Optional) For OSPF, specifies the external link type associated with the default route advertised into the OSPF routing domain. It can be one of two values: • 1—Type 1 external route • 2—Type 2 external route If a metric-type is not specified, the Cisco IOS software adopts a Type 2 external route. For IS-IS, it can be one of two values: • internal—IS-IS metric that is < 63. • external—IS-IS metric that is > 64 < 128. The default is internal.

match { internal external1 external2 }	(Optional) Specifies the criteria by which OSPF routes are redistributed into other routing domains. It can be one of the following: • internal—Routes that are internal to a specific autonomous system. • external 1—Routes that are external to the autonomous system, but are imported into OSPF as Type 1 external routes. • external 2—Routes that are external to the autonomous system, but are imported into OSPF as Type 2 external routes. The default is internal.
tag <i>tag-value</i>	(Optional) Specifies the 32-bit decimal value attached to each external route. This is not used by OSPF itself. It may be used to communicate information between Autonomous System Boundary Routers (ASBRs). If none is specified, the remote autonomous system number is used for routes from Border Gateway Protocol (BGP) and Exterior Gateway Protocol (EGP); for other protocols, zero (0) is used.
route-map	(Optional) Specifies the route map that should be interrogated to filter the importation of routes from this source routing protocol to the current routing protocol. If not specified, all routes are redistributed. If this keyword is specified, but no route map tags are listed, no routes will be imported.
<i>map-tag</i>	(Optional) Identifier of a configured route map.
subnets	(Optional) For redistributing routes into OSPF, the scope of redistribution for the specified protocol. By default, no subnets are defined.
nssa-only	(Optional) Sets the nssa-only attribute for all routes redistributed into OSPF.

Command Default

Route redistribution is disabled.

Command Modes

Router configuration (config-router)

Address family configuration (config-af)

Address family topology configuration (config-router-af-topology)

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	This command was modified. Address family configuration mode was added.
12.0(22)S	This command was modified. Address family support under EIGRP was added.
12.2(15)T	This command was modified. Address family support under EIGRP was added.
12.2(18)S	This command was modified. Address family support under EIGRP was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. Address family topology support under EIGRP was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added, and the default format for 4-byte autonomous system numbers is asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added, and the default format for 4-byte autonomous system numbers is asplain.
15.0(1)M	This command was modified. The nssa-only keyword was added.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
15.1(1)SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

Using the no Form of the redistribute Command



Caution

Removing options that you have configured for the **redistribute** command requires careful use of the **no** form of the **redistribute** command to ensure that you obtain the result that you are expecting. Changing or disabling any keyword may or may not affect the state of other keywords, depending on the protocol.

It is important to understand that different protocols implement the **no** version of the **redistribute** command differently:

- In BGP, OSPF, and RIP configurations, the **no redistribute** command removes only the specified keywords from the **redistribute** commands in the running configuration. They use the *subtractive keyword* method when redistributing from other protocols. For example, in the case of BGP, if you configure **no redistribute static route-map interior**, *only the route map* is removed from the redistribution, leaving **redistribute static** in place with no filter.
- The **no redistribute isis** command removes the IS-IS redistribution from the running configuration. IS-IS removes the entire command, regardless of whether IS-IS is the redistributed or redistributing protocol.
- EIGRP used the subtractive keyword method prior to EIGRP component version rel5. Starting with EIGRP component version rel5, the **no redistribute** command removes the entire **redistribute** command when redistributing from any other protocol.

Additional Usage Guidelines for the redistribute Command

A router receiving a link-state protocol with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.

Routes learned from IP routing protocols can be redistributed at Level 1 into an attached area or at Level 2. The **level-1-2** keyword allows both Level 1 and Level 2 routes in a single command.

Redistributed routing information must be filtered by the **distribute-list out** router configuration command. This guideline ensures that only those routes intended by the administrator are passed along to the receiving routing protocol.

Whenever you use the **redistribute** or the **default-information** router configuration commands to redistribute routes into an OSPF routing domain, the router automatically becomes an ASBR. However, an ASBR does not, by default, generate a default route into the OSPF routing domain.

When routes are redistributed into OSPF from protocols other than OSPF or BGP, and no metric has been specified with the **metric-type** keyword and *type-value* argument, OSPF will use 20 as the default metric. When routes are redistributed into OSPF from BGP, OSPF will use 1 as the default metric. When routes are redistributed from one OSPF process to another OSPF process, autonomous system external and not-so-stubby-area (NSSA) routes will use 20 as the default metric. When intra-area and inter-area routes are redistributed between OSPF processes, the internal OSPF metric from the redistribution source process is advertised as the external metric in the redistribution destination process. (This is the only case in which the routing table metric will be preserved when routes are redistributed into OSPF.)

When routes are redistributed into OSPF, only routes that are not subnetted are redistributed if the **subnets** keyword is not specified.

On a router internal to an NSSA area, the **nssa-only** keyword causes the originated type-7 NSSA LSAs to have their propagate (P) bit set to zero, which prevents area border routers from translating these LSAs into type-5 external LSAs. On an area border router that is connected to an NSSA and normal areas, the **nssa-only** keyword causes the routes to be redistributed only into the NSSA areas.

Routes configured with the **connected** keyword affected by this **redistribute** command are the routes not specified by the **network** router configuration command.

You cannot use the **default-metric** command to affect the metric used to advertise connected routes.

**Note**

The **metric** value specified in the **redistribute** command supersedes the **metric** value specified using the **default-metric** command.

The default redistribution of interior gateway protocol (IGP) or Exterior Gateway Protocol (EGP) into BGP is not allowed unless the **default-information originate** router configuration command is specified.

Release 12.2(33)SRB

If you plan to configure the Multi-Topology Routing (MTR) feature, you need to enter the **redistribute** command in address family topology configuration mode in order for this OSPF configuration command to become topology-aware.

4-Byte Autonomous System Number Support

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2, for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Examples

The following example shows how OSPF routes are redistributed into a BGP domain:

```
Router(config)# router bgp 109
Router(config-router)# redistribute ospf
```

The following example shows how to redistribute EIGRP routes into an OSPF domain:

```
Router(config)# router ospf 110
Router(config-router)# redistribute eigrp
```

The following example shows how to redistribute the specified EIGRP process routes into an OSPF domain. The EIGRP-derived metric will be remapped to 100 and RIP routes to 200.

```
Router(config)# router ospf 109
Router(config-router)# redistribute eigrp 108 metric 100 subnets
Router(config-router)# redistribute rip metric 200 subnets
```

The following example shows how to configure BGP routes to be redistributed into IS-IS. The link-state cost is specified as 5, and the metric type is set to external, indicating that it has lower priority than internal metrics.

```
Router(config)# router isis
Router(config-router)# redistribute bgp 120 metric 5 metric-type external
```

In the following example, network 172.16.0.0 will appear as an external LSA in OSPF 1 with a cost of 100 (the cost is preserved):

```
Router(config)# interface ethernet 0
Router(config-if)# ip address 172.16.0.1 255.0.0.0
Router(config-if)# exit
Router(config)# ip ospf cost 100
Router(config)# interface ethernet 1
Router(config-if)# ip address 10.0.0.1 255.0.0.0
!
Router(config)# router ospf 1
Router(config-router)# network 10.0.0.0 0.255.255.255 area 0
Router(config-if)# exit
Router(config-router)# redistribute ospf 2 subnet
Router(config)# router ospf 2
Router(config-router)# network 172.16.0.0 0.255.255.255 area 0
```

The following example shows how BGP routes are redistributed into OSPF and assigned the local 4-byte autonomous system number in asplain format. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or a later release.

```
Router(config)# router ospf 2
Router(config-router)# redistribute bgp 65538
```

The following example shows how to remove the **connected metric 1000 subnets** options from the **redistribute connected metric 1000 subnets** command and leave the **redistribute connected** command in the configuration:

```
Router(config-router)# no redistribute connected metric 1000 subnets
```

The following example shows how to remove the **metric 1000** options from the **redistribute connected metric 1000 subnets** command and leave the **redistribute connected subnets** command in the configuration:

```
Router(config-router)# no redistribute connected metric 1000
```

The following example shows how to remove the **subnets** option from the **redistribute connected metric 1000 subnets** command and leave the **redistribute connected metric 1000** command in the configuration:

```
Router(config-router)# no redistribute connected subnets
```

The following example shows how to remove the **redistribute connected** command, and any of the options that were configured for the **redistribute connected** command, from the configuration:

```
Router(config-router)# no redistribute connected
```

The following example shows how EIGRP routes are redistributed into an EIGRP process in a named EIGRP configuration:

```
Router(config)# router eigrp virtual-name
Router(config-router)# address-family ipv4 autonomous-system 1
Router(config-router-af)# topology base
Router(config-router-af-topology)# redistribute eigrp 6473 metric 1 1 1 1 1
```

The following example shows how to set and disable the redistributions in EIGRP configuration. Note that, in the case of EIGRP, the **no** form of the commands removes the entire set of **redistribute** commands from the running configuration.

```
Router(config)# router eigrp 1
Router(config-router)# network 0.0.0.0
Router(config-router)# redistribute eigrp 2 route-map x
Router(config-router)# redistribute ospf 1 route-map x
Router(config-router)# redistribute bgp 1 route-map x
Router(config-router)# redistribute isis level-2 route-map x
Router(config-router)# redistribute rip route-map x

Router(config)# router eigrp 1
Router(config-router)# no redistribute eigrp 2 route-map x
Router(config-router)# no redistribute ospf 1 route-map x
Router(config-router)# no redistribute bgp 1 route-map x
Router(config-router)# no redistribute isis level-2 route-map x
Router(config-router)# no redistribute rip route-map x
Router(config-router)# end

Router# show running-config | section router eigrp 1

router eigrp 1
 network 0.0.0.0
```

The following example shows how to set and disable the redistributions in OSPF configuration. Note that the **no** form of the commands removes only the specified keywords from the **redistribute** command in the running configuration.

```
Router(config)# router ospf 1
Router(config-router)# network 0.0.0.0
Router(config-router)# redistribute eigrp 2 route-map x
Router(config-router)# redistribute ospf 1 route-map x
Router(config-router)# redistribute bgp 1 route-map x
Router(config-router)# redistribute isis level-2 route-map x
Router(config-router)# redistribute rip route-map x

Router(config)# router ospf 1
Router(config-router)# no redistribute eigrp 2 route-map x
Router(config-router)# no redistribute ospf 1 route-map x
Router(config-router)# no redistribute bgp 1 route-map x
Router(config-router)# no redistribute isis level-2 route-map x
Router(config-router)# no redistribute rip route-map x
Router(config-router)# end

Router# show running-config | section router ospf 1
```

```

router ospf 1
 redistribute eigrp 2
 redistribute ospf 1
 redistribute bgp 1
 redistribute rip
 network 0.0.0.0

```

The following example shows how to remove only the route map filter from the redistribution in BGP; redistribution itself remains in force without a filter:

```

Router(config)# router bgp 65000
Router(config-router)# no redistribute eigrp 2 route-map x

```

The following example shows how to remove the EIGRP redistribution to BGP:

```

Router(config)# router bgp 65000
Router(config-router)# no redistribute eigrp 2

```

Related Commands

Command	Description
address-family (EIGRP)	Enters address family configuration mode to configure an EIGRP routing instance.
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IPv4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPNv4 address prefixes.
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
default-information originate (BGP)	Allows the redistribution of network 0.0.0.0 into BGP.
default-information originate (IS-IS)	Generates a default route into an IS-IS routing domain.
default-information originate (OSPF)	Generates a default route into an OSPF routing domain.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
router bgp	Configures the BGP routing process.

Command	Description
router eigrp	Configures the EIGRP address-family process.
show route-map	Displays all route maps configured or only the one specified.
topology (EIGRP)	Configures an EIGRP process to route IP traffic under the specified topology instance and enters address family topology configuration mode.

redistribute (ISO IS-IS to BGP)

To redistribute routes from an International Organization for Standardization (ISO) Intermediate System-to-Intermediate System (IS-IS) routing process into a Border Gateway Protocol (BGP) autonomous system, use the **redistribute** command in address family or router configuration mode. To remove the **redistribute** command from the configuration file and restore the system to its default condition where the software does not redistribute IS-IS routes into BGP, use the **no** form of this command.

redistribute *protocol* [*process-id*] [*route-type*] [**route-map** [*map-tag*]]

no redistribute *protocol* [*process-id*] [*route-type*] [**route-map** [*map-tag*]]

Syntax Description

<i>protocol</i>	Source protocol from which routes are being redistributed. It can be one of the following keywords: isis or static . • The isis keyword is used to redistribute dynamic routes. • The static keyword is used to redistribute static routes.
<i>process-id</i>	(Optional) When IS-IS is used as a source protocol, this argument defines a meaningful name for a routing process. The <i>process-id</i> argument identifies from which IS-IS routing process routes will be redistributed. • Routes can be redistributed only from IS-IS routing processes that involve Level 2 routes, including IS-IS Level 1-2 and Level 2 routing processes. • The <i>process-id</i> argument is not used when the static keyword is used as the <i>protocol</i>.
<i>route-type</i>	(Optional) The type of route to be redistributed. It can be one of the following keywords: clns or ip . The default is ip . • The clns keyword is used to redistribute Connectionless Network Service (CLNS) routes with network service access point (NSAP) addresses into BGP. • The ip keyword is used to redistribute IS-IS routes with IP addresses into BGP.
route-map <i>map-tag</i>	(Optional) Identifier of a configured route map. The route map is examined to filter the importation of routes from this source routing protocol to BGP. If no route map is specified, all routes are redistributed. If the route-map keyword is specified, but no <i>map-tag</i> value is entered, no routes are imported.

Command Default

Route redistribution from ISO IS-IS to BGP is disabled.

route-type : **ip**

Command Modes

Address family configuration (config-router-af) (Cisco IOS 12.3(8)T and later releases)

Router configuration (config-router) (T-releases after Cisco IOS 12.3(8)T)

Command History

Release	Modification
12.2(8)T	The clns keyword was added.
12.3(8)T	Beginning with Cisco IOS Release 12.3(8)T this version of the redistribute command should be entered under address family mode rather than router configuration mode.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **clns** keyword must be specified to redistribute NSAP prefix routes from an ISO IS-IS routing process into BGP. Beginning with Cisco IOS Release 12.3(8)T, this version of the **redistribute** command is entered only in address family configuration mode for BGP processes.

Examples**Examples**

The following example configures CLNS NSAP routes from the IS-IS routing process called *osi-proc-6* to be redistributed into BGP:

```
Router(config)# router bgp 64352
Router(config-router)# redistribute isis osi-proc-6 clns
```

Examples

The following example configures CLNS NSAP routes from the IS-IS routing process called *osi-proc-15* to be redistributed into BGP:

```
Router(config)# router bgp 404
Router(config-router)# address-family nsap
Router(config-router-af)# redistribute isis osi-proc-15 clns
```

Related Commands

Command	Description
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.

Command	Description
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
show route-map	Displays all route maps configured or only the one specified.

redistribute dvmrp

To configure redistribution of Distance Vector Multicast Routing Protocol (DVMRP) routes into multiprotocol BGP, use the **redistribute dvmrp** command in address family or router configuration mode. To stop such redistribution, use the **no** form of this command.

redistribute dvmrp [**route-map** *map-name*]

no redistribute dvmrp [**route-map** *map-name*]

Syntax Description

route-map <i>map-name</i>	(Optional) Name of the route map that contains various BGP attribute settings.

Command Default

DVMRP routes are not redistributed into multiprotocol BGP.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
11.1(20)CC	This command was introduced.
12.0(7)T	Address family configuration mode 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.

Usage Guidelines

Use this command if you have a subset of DVMRP routes in an autonomous system that you want to take the multiprotocol BGP path. Define a route map to further specify which DVMRP routes get redistributed.

Examples

The following router configuration mode example redistributes DVMRP routes to BGP peers that match access list 1:

```
router bgp 109
 redistribute dvmrp route-map dvmrp-into-mbgp
 route-map dvmrp-into-mbgp
 match ip address 1
```

The following address family configuration mode example redistributes DVMRP routes to multiprotocol BGP peers that match access list 1:

```
router bgp 109
address-family ipv4 multicast
  redistribute dvmrp route-map dvmrp-into-mbgp
route-map dvmrp-into-mbgp
  match ip address 1
```

router bgp

To configure the Border Gateway Protocol (BGP) routing process, use the **router bgp** command in global configuration mode. To remove a BGP routing process, use the **no** form of this command.

router bgp *autonomous-system-number*

no router bgp *autonomous-system-number*

Syntax Description

<i>autonomous-system-number</i>	Number of an autonomous system that identifies the router to other BGP routers and tags the routing information that is passed along. Number in the range from 1 to 65535. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the “Usage Guidelines” section.

Command Default No BGP routing process is enabled by default.

Command Modes Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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.

Release	Modification
12.2(33)SRB	This command was modified. Support for IPv6 was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.2(33)SB	This command was modified. Support for IPv6 was added.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(1)SG	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 3.3SG	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

This command allows you to set up a distributed routing core that automatically guarantees the loop-free exchange of routing information between autonomous systems.

Prior to January 2009, BGP autonomous system numbers that were allocated to companies were 2-octet numbers in the range from 1 to 65535 as described in RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*. Due to increased demand for autonomous system numbers, the Internet Assigned Number Authority (IANA) will start in January 2009 to allocate four-octet autonomous system numbers in the range from 65536 to 4294967295. RFC 5396, *Textual Representation of Autonomous System (AS) Numbers*, documents three methods of representing autonomous system numbers. Cisco has implemented the following two methods:

- **Asplain**—Decimal value notation where both 2-byte and 4-byte autonomous system numbers are represented by their decimal value. For example, 65526 is a 2-byte autonomous system number and 234567 is a 4-byte autonomous system number.
- **Asdot**—Autonomous system dot notation where 2-byte autonomous system numbers are represented by their decimal value and 4-byte autonomous system numbers are represented by a dot notation. For example, 65526 is a 2-byte autonomous system number and 1.169031 is a 4-byte autonomous system number (this is dot notation for the 234567 decimal number).

For details about the third method of representing autonomous system numbers, see RFC 5396.



Note

In Cisco IOS releases that include 4-byte ASN support, command accounting and command authorization that include a 4-byte ASN number are sent in the asplain notation irrespective of the format that is used on the command-line interface.

Asdot Only Autonomous System Number Formatting

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, Cisco IOS XE Release 2.3, and later releases, the 4-octet (4-byte) autonomous system numbers are entered and displayed only in asdot notation, for example, 1.10 or 45000.64000. When using regular expressions to match 4-byte autonomous system numbers the asdot format includes a period which is a special character in regular expressions. A backslash must be entered before the period for example, 1\.14, to ensure the regular expression match does not fail. The table below shows the format in which 2-byte and 4-byte autonomous system numbers are configured, matched in regular expressions, and displayed in **show** command output in Cisco IOS images where only asdot formatting is available.

Table 7: Asdot Only 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535

Asplain as Default Autonomous System Number Formatting

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain as the default display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain and asdot format. In addition, the default format for matching 4-byte autonomous system numbers in regular expressions is asplain, so you must ensure that any regular expressions to match 4-byte autonomous system numbers are written in the asplain format. If you want to change the default **show** command output to display 4-byte autonomous system numbers in the asdot format, use the **bgp asnotation dot** command under router configuration mode. When the asdot format is enabled as the default, any regular expressions to match 4-byte autonomous system numbers must be written using the asdot format,

or the regular expression match will fail. The tables below show that although you can configure 4-byte autonomous system numbers in either asplain or asdot format, only one format is used to display **show** command output and control 4-byte autonomous system number matching for regular expressions, and the default is asplain format. To display 4-byte autonomous system numbers in **show** command output and to control matching for regular expressions in the asdot format, you must configure the **bgp asnotation dot** command. After enabling the **bgp asnotation dot** command, a hard reset must be initiated for all BGP sessions by entering the **clear ip bgp *** command.

**Note**

If you are upgrading to an image that supports 4-byte autonomous system numbers, you can still use 2-byte autonomous system numbers. The **show** command output and regular expression match are not changed and remain in asplain (decimal value) format for 2-byte autonomous system numbers regardless of the format configured for 4-byte autonomous system numbers.

Table 8: Default Asplain 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 65535 4-byte: 65536 to 4294967295	2-byte: 1 to 65535 4-byte: 65536 to 4294967295
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 65536 to 4294967295

Table 9: Asdot 4-Byte Autonomous System Number Format

Format	Configuration Format	Show Command Output and Regular Expression Match Format
asplain	2-byte: 1 to 65535 4-byte: 65536 to 4294967295	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535
asdot	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535	2-byte: 1 to 65535 4-byte: 1.0 to 65535.65535

Reserved and Private Autonomous System Numbers

In Cisco IOS Release 12.0(32)S12, 12.0(32)SY8, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, 12.4(24)T, Cisco IOS XE Release 2.3 and later releases, the Cisco implementation of BGP supports RFC 4893. RFC 4893 was developed to allow BGP to support a gradual transition from 2-byte autonomous system numbers to 4-byte autonomous system numbers. A new reserved (private) autonomous system number, 23456, was created by RFC 4893 and this number cannot be configured as an autonomous system number in the Cisco IOS CLI.

RFC 5398, *Autonomous System (AS) Number Reservation for Documentation Use*, describes new reserved autonomous system numbers for documentation purposes. Use of the reserved numbers allow configuration examples to be accurately documented and avoids conflict with production networks if these configurations

are literally copied. The reserved numbers are documented in the IANA autonomous system number registry. Reserved 2-byte autonomous system numbers are in the contiguous block, 64496 to 64511 and reserved 4-byte autonomous system numbers are from 65536 to 65551 inclusive.

Private 2-byte autonomous system numbers are still valid in the range from 64512 to 65534 with 65535 being reserved for special use. Private autonomous system numbers can be used for internal routing domains but must be translated for traffic that is routed out to the Internet. BGP should not be configured to advertise private autonomous system numbers to external networks. Cisco IOS software does not remove private autonomous system numbers from routing updates by default. We recommend that ISPs filter private autonomous system numbers.

**Note**

Autonomous system number assignment for public and private networks is governed by the IANA. For information about autonomous-system numbers, including reserved number assignment, or to apply to register an autonomous system number, see the following URL: <http://www.iana.org/>.

Examples

The following example configures a BGP process for autonomous system 45000 and configures two external BGP neighbors in different autonomous systems using 2-byte autonomous system numbers:

```
router bgp 45000
 neighbor 192.168.1.2 remote-as 40000
 neighbor 192.168.3.2 remote-as 50000
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
 exit-address-family
```

The following example configures a BGP process for autonomous system 65538 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asplain notation. This example is supported in Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases.

```
router bgp 65538
 neighbor 192.168.1.2 remote-as 65536
 neighbor 192.168.3.2 remote-as 65550
 neighbor 192.168.3.2 description finance
 !
 address-family ipv4
  neighbor 192.168.1.2 activate
  neighbor 192.168.3.2 activate
  no auto-summary
  no synchronization
  network 172.17.1.0 mask 255.255.255.0
 exit-address-family
```

The following example configures a BGP process for autonomous system 1.2 and configures two external BGP neighbors in different autonomous systems using 4-byte autonomous system numbers in asdot notation. This example is supported in Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, 12.4(24)T, and Cisco IOS XE Release 2.3, and later releases.

```
router bgp 1.2
 neighbor 192.168.1.2 remote-as 1.0
 neighbor 192.168.3.2 remote-as 1.14
 neighbor 192.168.3.2 description finance
 !
```

 router bgp

```
address-family ipv4
neighbor 192.168.1.2 activate
neighbor 192.168.3.2 activate
no auto-summary
no synchronization
network 172.17.1.0 mask 255.255.255.0
exit-address-family
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
neighbor remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
network (BGP and multiprotocol BGP)	Specifies the list of networks for the BGP routing process.

route-server-context

To create a route-server context in order to provide flexible policy handling for a BGP route server, use the **route-server-context** command in router configuration mode. To remove the route server context, use the **no** form of this command.

route-server-context *context-name*

no route-server-context *context-name*

Syntax Description

<i>context-name</i>	Name of the route server context.

Command Default

No route server context exists.

Command Modes

Router configuration (config-router)

Command History

Release	Modification
Cisco IOS XE 3.3S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

Flexible (customized) policy support for a BGP route server is made possible with the use of the **route-server-context** command. The **route-server-context** command creates a context, which represents the virtual table used to store prefixes and paths that require special handling due to individualized policy configurations.

The context is referenced by the BGP neighbors assigned to use that context (in the **neighbor route-server-client** command). Thus, multiple neighbors sharing the same policy can share the same route server context.

In order to configure flexible policy handling, create a route server context, which includes an import map. The import map references a standard route map.

Examples

In the following example, the local router is a BGP route server. Its neighbors at 10.10.10.12 and 10.10.10.13 are its route server clients. A route server context named ONLY_AS27_CONTEXT is created and applied to the neighbor at 10.10.10.13. The context uses an import map that references a route map named only_AS27_routemap. The route map matches routes permitted by access list 27. Access list 27 permits routes that have 27 in the autonomous system path.

```
router bgp 65000
  route-server-context ONLY_AS27_CONTEXT
  address-family ipv4 unicast
```

```

import-map only_AS27_routemap
exit-address-family
exit-route-server-context
!
neighbor 10.10.10.12 remote-as 12
neighbor 10.10.10.12 description Peer12
neighbor 10.10.10.13 remote-as 13
neighbor 10.10.10.13 description Peer13
neighbor 10.10.10.21 remote-as 21
neighbor 10.10.10.27 remote-as 27
!
address-family ipv4
neighbor 10.10.10.12 activate
neighbor 10.10.10.12 route-server-client
neighbor 10.10.10.13 activate
neighbor 10.10.10.13 route-server-client context ONLY_AS27_CONTEXT
neighbor 10.10.10.21 activate
neighbor 10.10.10.27 activate
exit-address-family
!
ip as-path access-list 27 permit 27
!
route-map only_AS27_routemap permit 10
match as-path 27
!

```

Related Commands

Command	Description
description (route-server-context)	Specifies a description for a route-server-context.
neighbor route-server-client	Specifies on a BGP route server that a neighbor is a route server client.

scope

To define the scope for a Border Gateway Protocol (BGP) routing session and to enter router scope configuration mode, use the **scope** command in router configuration mode. To remove the scope configuration, use the **no** form of this command.

scope {**global**|**vrf** *vrf-name*}

no scope {**global**|**vrf** *vrf-name*}

Syntax Description

global	Configures BGP to use the global routing table or a specific topology table.
vrf	Configures BGP to use a specific VRF routing table.
<i>vrf-name</i>	Name of an existing VRF.

Command Default

No scope is defined for a BGP routing session.

Command Modes

Router configuration (config-router)

Command History

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

Usage Guidelines

A new configuration hierarchy, named scope, has been introduced into the BGP protocol. To implement Multi-Topology Routing (MTR) support for BGP, the scope hierarchy is required, but the scope hierarchy is not limited to MTR use. The scope hierarchy introduces some new configuration modes such as router scope configuration mode. Router scope configuration mode is entered by configuring the **scope** command in router configuration mode, and a collection of routing tables is created when this command is entered. The scope is configured to isolate routing calculation for a single network (globally) or on a per-VRF basis, and BGP commands configured in routing scope configuration mode are referred to as scoped commands. The scope hierarchy can contain one or more address families.

The BGP command-line interface (CLI) has been modified to provide backwards compatibility for pre-MTR BGP configuration and to provide a hierarchal implementation of MTR. From router scope configuration mode, MTR is configured first by entering the **address-family** command to enter the desired address family and then by entering the **topology** command to define the topology



Note

Configuring a scope for a BGP routing process removes CLI support for pre-MTR-based configuration.

Examples

The following example defines a global scope that includes both unicast and multicast topology configurations. Another scope is specifically defined only for the VRF named DATA.

```
Router(config)# router bgp 45000
Router(config-router)# scope global
Router(config-router-scope)# bgp default ipv4-unicast
Router(config-router-scope)# neighbor 172.16.1.2 remote-as 45000

Router(config-router-scope)# neighbor 192.168.3.2 remote-as 50000

Router(config-router-scope)# address-family ipv4 unicast
Router(config-router-scope-af)# topology VOICE
Router(config-router-scope-af)# bgp tid 100
Router(config-router-scope-af)# neighbor 172.16.1.2 activate

Router(config-router-scope-af)# exit
Router(config-router-scope)# address-family ipv4 multicast

Router(config-router-scope-af)# topology base
Router(config-router-scope-af-topo)# neighbor 192.168.3.2 activate

Router(config-router-scope-af-topo)# exit

Router(config-router-scope-af)# exit

Router(config-router-scope)# exit

Router(config-router)# scope vrf DATA

Router(config-router-scope)# neighbor 192.168.1.2 remote-as 40000

Router(config-router-scope)# address-family ipv4
Router(config-router-scope-af)# neighbor 192.168.1.2 activate

Router(config-router-scope-af)# end
```

Related Commands

Command	Description
bgp tid	Configures BGP to accept routes with a specified topology ID.
topology (BGP)	Configures a process to route IP traffic under the specified topology instance.

set as-path

To modify an autonomous system path for BGP routes, use the **set as-path** command in route-map configuration mode. To not modify the autonomous system path, use the **no** form of this command.

set as-path {tag| prepend *as-path-string*}

no set as-path {tag| prepend *as-path-string*}

Syntax Description

tag	Converts the tag of a route into an autonomous system path. Applies only when redistributing routes into BGP.
prepend	Appends the string following the keyword prepend to the autonomous system path of the route that is matched by the route map. Applies to inbound and outbound BGP route maps.
<i>as-path-string</i>	Number of an autonomous system to prepend to the AS_PATH attribute. The range of values for this argument is any valid autonomous system number from 1 to 65535. Multiple values can be entered; up to 10 AS numbers can be entered. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the router bgp command.

Command Default An autonomous system path is not modified.

Command Modes Route-map configuration (config-route-map)

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.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(1)SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

The only global BGP metric available to influence the best path selection is the autonomous system path length. By varying the length of the autonomous system path, a BGP speaker can influence the best path selection by a peer further away.

By allowing you to convert the tag into an autonomous system path, the **set as-path tag** variation of this command modifies the autonomous system length. The **set as-path prepend** variation allows you to “prepend” an arbitrary autonomous system path string to BGP routes. Usually the local autonomous system number is prepended multiple times, increasing the autonomous system path length.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain--65538 for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot--1.2 for example--as the only configuration format, regular expression match, and output display, with no asplain support.

Examples

The following example converts the tag of a redistributed route into an autonomous system path:

```
route-map set-as-path-from-tag
  set as-path tag
!
router bgp 100
  redistribute ospf 109 route-map set-as-path-from-tag
```

The following example prepends 100 100 100 to all the routes that are advertised to 10.108.1.1:

```
route-map set-as-path
  match as-path 1
  set as-path prepend 100 100 100
!
router bgp 100
  neighbor 10.108.1.1 route-map set-as-path out
```

The following example prepends 65538, 65538, and 65538 to all the routes that are advertised to 192.168.1.2. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or a later release.

```
route-map set-as-path
  match as-path 1.1
  set as-path prepend 65538 65538 65538
exit
router bgp 65538
  neighbor 192.168.1.2 route-map set-as-path out
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
router bgp	Configures the BGP routing process.
set tag (IP)	Sets a tag value of the destination routing protocol.

set comm-list delete

To remove communities from the community attribute of an inbound or outbound update, use the **set comm-list delete** command in route-map configuration mode. To remove a previous **set comm-list delete** command, use the **no** form of this command.

set comm-list {*community-list-number*| *community-list-name*} **delete**

no set comm-list {*community-list-number*| *community-list-name*} **delete**

Syntax Description

<i>community-list-number</i>	A standard or expanded community list number. The range of standard community list numbers is from 1 to 99. The range of expanded community list number is from 100 to 500.
<i>community-list-name</i>	A standard or expanded community list name.

Command Default

No communities are removed.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.0	This command was introduced.
12.0(10)S	Named community list support was added.
12.0(16)ST	Named community list support was integrated into Cisco IOS Release 12.0(16)ST.
12.1(9)E	Named community list support was integrated into Cisco IOS Release 12.1(9)E.
12.2(8)T	Named community list support was integrated into Cisco IOS Release 12.2(8)T.
12.0(22)S	The maximum number of expanded community lists was increased from 199 to 500 in Cisco IOS Release 12.0(22)S.
12.2(14)S	The maximum number of expanded community lists was increased from 199 to 500 and named community list support were integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	The maximum number of expanded community lists was increased from 199 to 500 in Cisco IOS Release 12.2(15)T.

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

This **set** route-map configuration command removes communities from the community attribute of an inbound or outbound update using a route map to filter and determine the communities to be deleted. Depending upon whether the route map is applied to the inbound or outbound update for a neighbor, each community that passes the route map **permit** clause and matches the given community list will be removed from the community attribute being received from or sent to the Border Gateway Protocol (BGP) neighbor.

Each entry of a standard community list should list only one community when used with the **set comm-list delete** command. For example, in order to be able to delete communities 10:10 and 10:20, you must use the following format to create the entries:

```
ip community-list 500 permit 10:10
ip community-list 500 permit 10:20
```

The following format for a community list entry, while acceptable otherwise, does not work with the **set comm-list delete** command:

```
config ip community-list 500 permit 10:10 10:20
```

When both the **set community community-number** and **set comm-list delete** commands are configured in the same sequence of a route map attribute, the deletion operation (**set comm-list delete**) is performed before the set operation (**set community community-number**).

Examples

In the following example, the communities 100:10 and 100:20 (if present) will be deleted from updates received from 172.16.233.33. Also, except for 100:50, all communities beginning with 100: will be deleted from updates sent to 172.16.233.33.

```
router bgp 100
 neighbor 172.16.233.33 remote-as 120
 neighbor 172.16.233.33 route-map ROUTEMAPIN in
 neighbor 172.16.233.33 route-map ROUTEMAPOUT out
!
ip community-list 500 permit 100:10
ip community-list 500 permit 100:20
!
ip community-list 120 deny 100:50
ip community-list 120 permit 100:.*
!
route-map ROUTEMAPIN permit 10
 set comm-list 500 delete
!
route-map ROUTEMAPOUT permit 10
 set comm-list 120 delete
```

Related Commands

Command	Description
set community	Sets the BGP communities attribute.

set community

To set the BGP communities attribute, use the **set community** route map configuration command. To delete the entry, use the **no** form of this command.

set community {*community-number* [**additive**] [*well-known-community*]| **none**}

no set community

Syntax Description

<i>community-number</i>	Specifies that community number. Valid values are from 1 to 4294967200, no-export , or no-advertise .
additive	(Optional) Adds the community to the already existing communities.
<i>well-known-community</i>	(Optional) Well know communities can be specified by using the following keywords: • internet • local-as • no-advertise • no-export
none	(Optional) Removes the community attribute from the prefixes that pass the route map.

Command Default

No BGP communities attributes exist.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
10.3	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

You must have a match clause (even if it points to a “permit everything” list) if you want to set tags.

Use the **route-map** global configuration command, and the **match** and **set** route map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria* --the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions* --the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-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. When all match criteria are met, all set actions are performed.

Examples

In the following example, routes that pass the autonomous system path access list 1 have the community set to 109. Routes that pass the autonomous system path access list 2 have the community set to no-export (these routes will not be advertised to any external BGP [eBGP] peers).

```
route-map set_community 10 permit
 match as-path 1
 set community 109
route-map set_community 20 permit
 match as-path 2
 set community no-export
```

In the following similar example, routes that pass the autonomous system path access list 1 have the community set to 109. Routes that pass the autonomous system path access list 2 have the community set to local-as (the router will not advertise this route to peers outside the local autonomous system).

```
route-map set_community 10 permit
 match as-path 1
 set community 109
route-map set_community 20 permit
 match as-path 2
 set community local-as
```

Related Commands

Command	Description
ip community-list	Creates a community list for BGP and control access to it.
match community	Matches a BGP community.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set comm-list delete	Removes communities from the community attribute of an inbound or outbound update.
show ip bgp community	Displays routes that belong to specified BGP communities.

set dampening

To set the BGP route dampening factors, use the **set dampening** route map configuration command. To disable this function, use the **no** form of this command.

set dampening *half-life reuse suppress max-suppress-time*

no set dampening

Syntax Description

<i>half-life</i>	Time (in minutes) after which a penalty is decreased. Once the route has been assigned a penalty, the penalty is decreased by half after the half life period (which is 15 minutes by default). The process of reducing the penalty happens every 5 seconds. The range of the half life period is from 1 to 45 minutes. The default is 15 minutes.
<i>reuse</i>	Unsuppresses the route if the penalty for a flapping route decreases enough to fall below this value. The process of unsuppressing routes occurs at 10-second increments. The range of the reuse value is from 1 to 20000; the default is 750.
<i>suppress</i>	Suppresses a route when its penalty exceeds this limit. The range is from 1 to 20000; the default is 2000.
<i>max-suppress-time</i>	Maximum time (in minutes) a route can be suppressed. The range is from 1 to 20000; the default is four times the <i>half-life</i> value. If the <i>half-life</i> value is allowed to default, the maximum suppress time defaults to 60 minutes.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration (config-route-map)

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.

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 **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria* --the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions* --the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

When a BGP peer is reset, the route is withdrawn and the flap statistics cleared. In this instance, the withdrawal does not incur a penalty even though route flap dampening is enabled.

Examples

The following example sets the half life to 30 minutes, the reuse value to 1500, the suppress value to 10000; and the maximum suppress time to 120 minutes:

```
route-map tag
 match as path 10
 set dampening 30 1500 10000 120
!
router bgp 100
 neighbor 172.16.233.52 route-map tag in
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.

Command	Description
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set ip next-hop	Specifies the address of the next hop.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set origin (BGP)	Sets the BGP origin code.
set tag (IP)	Sets the value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.
show route-map	Displays all route maps configured or only the one specified.

set extcomm-list delete

To allow the deletion of extended community attributes based on an extended community list, use the **set extcomm-list delete** command in route-map configuration mode. To negate a previous **set extcomm-list detect** command, use the **no** form of this command.

set extcomm-list *extended-community-list-number* **delete**

no set extcomm-list *extended-community-list-number* **delete**

Syntax Description

<i>extended-community-list-number</i>	An extended community list number.

Command Default

Extended community attributes based on an extended community list cannot be deleted.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.0(26)S	This command was introduced.
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(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

This command removes extended community attributes of an inbound or outbound Border Gateway Protocol (BGP) update using a route map to filter and determine the extended community attribute to be deleted and replaced. Depending upon whether the route map is applied to the inbound or outbound update for a neighbor, each extended community that passes the route map permit clause and matches the given extended community list will be removed and replaced from the extended community attribute being received from or sent to the BGP neighbor.

For information about how to use this command when translating a route target to a VPN distinguisher and vice versa, see the “BGP—VPN Distinguisher Attribute” module in the *IP Routing: BGP Configuration Guide*.

Examples

The following example shows how to replace a route target 100:3 on an incoming update with a route target of 100:4 using an inbound route map named extmap:

```
.
.
.
Device(config-af)# neighbor 10.10.10.10 route-map extmap in
.
.
.
Device(config)# ip extcommunity-list 1 permit rt 100:3
Device(config)# route-map extmap permit 10
Device(config-route-map)# match extcommunity 1
Device(config-route-map)# set extcomm-list 1 delete
Device(config-route-map)# set extcommunity rt 100:4 additive
```

The following example shows how to configure more than one replacement rule using the route-map configuration **continue** command. Prefixes with RT 100:2 are rewritten to RT 200:3 and prefixes with RT 100:4 are rewritten to RT 200:4. With the **continue** command, route-map evaluation proceeds even if a match is found in a previous sequence.

```
Device(config)# ip extcommunity-list 1 permit rt 100:3
Device(config)# ip extcommunity-list 2 permit rt 100:4
Device(config)# route-map extmap permit 10
Device(config-route-map)# match extcommunity 1
Device(config-route-map)# set extcomm-list 1 delete
Device(config-route-map)# set extcommunity rt 200:3 additive
Device(config-route-map)# continue 20
Device(config)# route-map extmap permit 20
Device(config-route-map)# match extcommunity 2
Device(config-route-map)# set extcomm-list 2 delete
Device(config-route-map)# set extcommunity rt 200:4 additive
Device(config-route-map)# exit
Device(config)# route-map extmap permit 30
```

Related Commands

Command	Description
ip community-list	Creates an extended community access list and controls access to it.
match extcommunity	Matches BGP extended community list attributes.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set extcommunity	Sets BGP extended community attributes.
set extcommunity vpn-distinguisher	Sets a VPN distinguisher attribute to routes.

set extcommunity cost

To create a set clause to apply the cost community attribute to routes that pass through a route map, use the **set extcommunity cost** command in route-map configuration mode. To remove all **set extcommunity cost**, **set extcommunity rt**, **set extcommunity soo**, and **set extcommunity vpn-distinguisher** clauses from the route-map clause, use the **no** form of this command.

set extcommunity cost [**igp**| **pre-bestpath**] *community-id cost-value*

no set extcommunity

Syntax Description

igp	(Optional) Specifies the IGP point of insertion (POI). The configuration of this keyword forces the cost community to be evaluated after the IGP distance to the next hop has been compared. If this keyword is not specified, IGP is the default POI.
<i>community-id</i>	The ID for the configured extended community. The range is from 0 to 255.
<i>cost-value</i>	The configured cost that is set for matching paths in the route map. The range is from 0 to 4294967295.

Command Default

The default cost value is applied to routes that are not configured with the cost community attribute when cost community filtering is enabled. The default *cost-value* is half of the maximum value (4294967295) or 2147483647.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.0(24)S	This command was introduced into Cisco IOS Release 12.0(24)S.
12.3(2)T	This command was integrated.
12.2(18)S	This command was integrated.
12.0(27)S	Support for mixed EIGRP MPLS VPN network topologies that contain back door routes was introduced into Cisco IOS Release 12.0(27)S.
12.3(8)T	Support for mixed EIGRP MPLS VPN network topologies that contain back door routes was introduced into Cisco IOS Release 12.3(8)T.

Release	Modification
12.2(25)S	Support for mixed EIGRP MPLS VPN network topologies that contain back door routes was introduced into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	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.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

The cost community attribute is applied to internal routes by configuring the **set extcommunity cost** command in a route map. The cost community set clause is configured with a cost community ID number (0-255) and a cost community number value (0-4294967295). The path with the lowest cost community number is preferred. In the case where two paths have been configured with the same cost community value, the path selection process will then prefer the path with the lower community ID.

The BGP Cost Community feature can be configured only within the same autonomous-system or confederation. The cost community is a non-transitive extended community. The cost community is passed to internal BGP (iBGP) and confederation peers only and is not passed to external BGP (eBGP) peers. The cost community allows you to customize the local preference and best path selection process for specific paths. The cost extended community attribute is propagated to iBGP peers when extended community exchange is enabled with the **neighbor send-community** command.

The following commands can be used to apply the route map with the cost community set clause:

- **aggregate-address**
- **neighbor default-originate route-map {in | out}**
- **neighbor route-map**
- **network route-map**
- **redistribute route-map**

Multiple cost community set clauses may be configured with the **set extcommunity cost** command in a single route map block or sequence. However, each set clause must be configured with a different ID value for each point of insertion (POI).

Aggregate routes and multipaths are supported by the BGP Cost Community feature. The cost community attribute can be applied to either type of route. The cost community attribute is passed to the aggregate or multipath route from component routes that carry the cost community attribute. Only unique IDs are passed, and only the highest cost of any individual component route will be applied to the aggregate on a per-ID basis. If multiple component routes contain the same ID, the highest configured cost is applied to the route. If one or more component routes does not carry the cost community attribute or if the component routes are configured with different IDs, then the default value (2147483647) will be advertised for the aggregate or multipath route.

**Note**

The BGP cost community attribute must be supported on all routers in an autonomous system or confederation before cost community filtering is configured. The cost community should be applied consistently throughout the local autonomous system or confederation to avoid potential routing loops.

**Note**

The **no** form of this command removes any **set extcommunity cost** clause, **set extcommunity rt** clause, **set extcommunity soo** clause, and **set extcommunity vpn-distinguisher** clause from the route-map clause.

Support for EIGRP MPLS VPN Back Door Links

The “pre-bestpath” point of insertion (POI) has been introduced in the BGP Cost Community feature to support mixed EIGRP VPN network topologies that contain VPN and backdoor links. This POI is applied automatically to EIGRP routes that are redistributed into BGP. The “pre-best path” POI carries the EIGRP route type and metric. This POI influences the best path calculation process by influencing BGP to consider this POI before any other comparison step. No configuration is required. This feature is enabled automatically for EIGRP VPN sites when a supporting is installed to a PE, CE, or back door router.

Examples

The following example configuration shows the configuration of the **set extcommunity cost** command. The following example applies the cost community ID of 1 and cost community value of 100 to routes that are permitted by the route map. This configuration will cause the best path selection process to prefer this route over other equal cost paths that were not permitted by this route map sequence.

```
Router(config)# router bgp 50000
Router(config-router)# neighbor 10.0.0.1 remote-as 50000
Router(config-router)# neighbor 10.0.0.1 update-source Loopback 0
Router(config-router)# address-family ipv4
Router(config-router-af)# neighbor 10.0.0.1 activate
Router(config-router-af)# neighbor 10.0.0.1 route-map COST1 in
Router(config-router-af)# neighbor 10.0.0.1 send-community both
Router(config-router-af)# exit
Router(config)# route-map COST1 permit 10
Router(config-route-map)# match ip-address 1
Router(config-route-map)# set extcommunity cost 1 100
```

Related Commands

Command	Description
aggregate-address	Creates an aggregate entry in a BGP or multicast BGP database.
bgp bestpath cost-community ignore	Configures a router that is running BGP to not evaluate the cost community attribute during the best path selection process.
neighbor default-originate	Allows a BGP speaker (the local router) to send the default route 0.0.0.0 to a neighbor for use as a default route.
neighbor route-map	Applies a route map to incoming or outgoing routes.

Command	Description
network (BGP and multiprotocol BGP)	Specifies the networks to be advertised by the BGP and multiprotocol BGP routing processes.
set extcommunity rt	Sets BGP extended community attributes for route target.
set extcommunity soo	Sets a BGP extended community attribute for site of origin.
set extcommunity vpn-distinguisher	Creates a set clause that applies a VPN distinguisher attribute to routes that pass through an outbound route map.
redistribute (IP)	Redistributes routes from one routing domain into another routing domain.
show ip bgp	Displays entries in the BGP routing table.

set extcommunity rt

To set Border Gateway Protocol (BGP) extended community attributes for route target, use the **set extcommunity rt** command in route-map configuration mode. To remove all **set extcommunity cost**, **set extcommunity rt**, **set extcommunity soo**, and **set extcommunity vpn-distinguisher** clauses from the route-map clause, use the **no** form of this command.

set extcommunity rt {*extended-community-value-1* [...*extended-community-value-n*]} **range** *start-range-value end-range-value* [**additive**]

no set extcommunity

Syntax Description

<i>extended-community-value-1</i>	Specifies the value to be set. More than one value can be specified following the rt keyword. The value can be one of the following combinations: • <i>autonomous-system-number:network-number</i> • <i>ip-address:network-number</i> • <i>ipv6-address:network-number</i> The colon is used to separate the autonomous system number and network number, the IP address and network number, or the IPv6 address and network number. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the router bgp command.
range	Specifies that the RT extended community values being set are in a contiguous range, from the <i>start-range-value</i> through the <i>end-range-value</i>, inclusive.

<i>start-range-value</i>	Starting value of a range of contiguous RT extended community values. • The formats allowed are the same as those for the <i>extended-community-value</i> shown above.
<i>end-range-value</i>	Ending value of a range of contiguous RT extended community values. • The formats allowed are the same as those for the <i>extended-community-value</i> shown above.
additive	(Optional) Adds a route target to the existing route target list without replacing any existing route targets.

Command Default

No RT extended community attributes are set.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	Support for IPv6 was added and this command was integrated into Cisco IOS Release 12.2(33)SB.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(1)SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.3(2)S	This command was modified. The range keyword and the <i>start-range-value</i> and <i>end-range-value</i> arguments were added.
Cisco IOS XE Release 3.9S	This command was modified. The range keyword and the <i>start-range-value</i> and <i>end-range-value</i> arguments were added.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).

The **set extcommunity** commands are used to configure set clauses that use extended community attributes in route maps. All of the standard rules of match and set clauses apply to the configuration of extended community attributes.



Note

The **no** form of this command removes any **set extcommunity cost** clause, **set extcommunity rt** clause, **set extcommunity soo** clause, and **set extcommunity vpn-distinguisher** clause from the route-map clause.

The route target (RT) extended community attribute is configured with the **rt** keyword. This attribute is used to identify a set of sites and VRFs that may receive routes that are tagged with the configured route target. Configuring the route target extended attribute with a route allows that route to be placed in the per-site forwarding tables that are used for routing traffic that is received from corresponding sites.

More than one route target extended community attribute can be specified in a single **set extcommunity rt** command, as indicated by the optional *extended-community-value-n* argument.

Specifying many RT extended community values individually can be time-consuming. If the RTs being attached to the prefixes are consecutive, the configuration can be simplified by specifying a range of RTs, thereby saving time and reducing complexity.

By default, specifying route targets causes the system to *replace* existing route targets with the new route targets, unless the **additive** keyword is used. The use of the **additive** keyword causes the system to *add* the new route targets to the existing route target list, but does not replace any existing route targets.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Examples

The following example sets the route targets to extended community attributes 100:2 and 100:3 for routes that are permitted by the route map. In this example, the route targets will *replace* existing route targets because the **additive** keyword was not used.

```
Router(config)# access-list 2 permit 192.168.78.0 255.255.255.0
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match ip address 2
Router(config-route-map)# set extcommunity rt 100:2 100:3
```

The following example sets the route target to extended community attribute 100:3 for routes that are permitted by the route map. In this example, the route target 100:3 is *added to* the existing route target list, and does not replace any existing route targets, because the **additive** keyword was used.

```
Router(config)# access-list 3 permit 192.168.79.0 255.255.255.0
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match ip address 3
Router(config-route-map)# set extcommunity rt 100:3 additive
```

The following example sets a range of additional route targets to extended community attributes 100:3, 100:4, 100:5, and 100:6 for routes that are permitted by the route map.

```
Router(config)# access-list 3 permit 192.168.79.0 255.255.255.0
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match ip address 3
Router(config-route-map)# set extcommunity rt range 100:3 100:6 additive
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, shows how to create a VRF with a route-target that uses a 4-byte autonomous system number, 65537 in asplain format, and how to set the RT to extended community value 65537:100 for routes that are permitted by the route map.

```
Router(config)# ip vrf vpn_red
Router(config-vrf)# rd 64500:100
Router(config-vrf)# route-target both 65537:100
Router(config-vrf)# exit
Router(config)# route-map rt_map permit 10
Router(config-route-map)# set extcommunity rt 65537:100
Router(config-route-map)# end
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, 12.4(24)T, Cisco IOS XE Release 2.3, and later releases, shows how to create a VRF with an

RT that uses a 4-byte autonomous system number, 1.1 in asdot format, and how to set the SoO to extended community attribute 1.1:100 for routes that are permitted by the route map.

```
Router(config)# ip vrf vpn_red
Router(config-vrf)# rd 64500:100
Router(config-vrf)# route-target both 1.1:100
Router(config-vrf)# exit
Router(config)# route-map soo_map permit 10
Router(config-route-map)# set extcommunity soo 1.1:100
Router(config-route-map)# end
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
ip extcommunity-list	Creates an extended community list and controls access to it.
match extcommunity	Matches a BGP VPN extended community list.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
router bgp	Configures the BGP routing process.
route-target	Creates a route target extended community for a VRF.
set extcommunity cost	Creates a set clause to apply the cost community attribute to routes that pass through a route map.
set extcommunity soo	Creates a set clause to apply the site of origin attribute to routes that pass through a route map.
set extcommunity vpn-distinguisher	Creates a set clause that applies a VPN distinguisher attribute to routes that pass through an outbound route map.
show ip extcommunity-list	Displays routes that are permitted by the extended community list.
show route-map	Displays all route maps configured or only the one specified.

set extcommunity soo

To set Border Gateway Protocol (BGP) extended community attribute for site of origin, use the **set extcommunity soo** command in route-map configuration mode. To remove all **set extcommunity cost**, **set extcommunity rt**, **set extcommunity soo**, and **set extcommunity vpn-distinguisher** clauses from the route-map clause, use the **no** form of this command.

set extcommunity soo *extended-community-value*

no set extcommunity

Syntax Description

<i>extended-community-value-1</i>	Specifies the value to be set. Only one value can be specified following the soo keyword. The value can be one of the following combinations: • <i>autonomous-system-number:network-number</i> • <i>ip-address:network-number</i> • <i>ipv6-address:network-number</i> The colon is used to separate the autonomous system number and network number, the IP address and network number, or the IPv6 address and network number. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the router bgp command.

Command Default No SOO extended community attribute is set.

Command Modes Route-map configuration (config-route-map)

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	Support for IPv6 was added.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	Support for IPv6 was added and this command was integrated into Cisco IOS Release 12.2(33)SB.
12.0(32)S12	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(1)SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

Extended community attributes are used to configure, filter, and identify routes for virtual routing and forwarding instances (VRFs) and Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs).

The **set extcommunity** commands are used to configure set clauses that use extended community attributes in route maps. All of the standard rules of match and set clauses apply to the configuration of extended community attributes.



Note

The **no** form of this command removes any **set extcommunity cost** clause, **set extcommunity rt** clause, **set extcommunity soo** clause, and **set extcommunity vpn-distinguisher** clause from the route-map clause.

The site of origin (SOO) extended community attribute is configured with the **soo** keyword. This attribute uniquely identifies the site from which the Provider Edge (PE) router learned the route. All routes learned from a particular site must be assigned the same SOO extended community attribute, whether a site is connected to a single PE router or multiple PE routers. Configuring this attribute prevents routing loops from occurring when a site is multihomed. The SOO extended community attribute is configured on the interface and is propagated into BGP through redistribution. The SOO can be applied to routes that are learned from VRFs. The SOO should not be configured for stub sites or sites that are not multihomed.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Examples

The following example sets the site of origin to extended community attribute 100:4 for routes that are permitted by the route map:

```
Router(config)# access-list 4 permit 192.168.80.0 255.255.255.0
Router(config)# route-map MAP_NAME permit 10
Router(config-route-map)# match ip address 4
Router(config-route-map)# set extcommunity soo 100:4
```

In IPv6, the following example sets the SoO to extended community attribute 100:28 for routes that are permitted by the route map:

```
Router(config)# router bgp 100
Router(config-router)# address-family ipv6 vrf red
Router(config-router-af)# neighbor 2001:db8::72a remote-as 200
Router(config-router-af)# neighbor 2001:db8::72a activate
Router(config-router-af)# neighbor 2001:db8::72a route-map setsoo in
Router(config-router-af)# exit
Router(config-router)# exit
Router(config)# route-map setsoo permit 10
Router(config-route-map)# set extcommunity soo 100:28
```

The following example available in Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, 12.4(24)T, Cisco IOS XE Release 2.3, and later releases, shows how to create a VRF with an RT that uses a 4-byte autonomous system number, 1.1 in asdot format, and how to set the SoO to extended community attribute 1.1:100 for routes that are permitted by the route map.

```
Router(config)# ip vrf vpn_red
Router(config-vrf)# rd 64500:100
Router(config-vrf)# route-target both 1.1:100
Router(config-vrf)# exit
Router(config)# route-map soo_map permit 10
Router(config-route-map)# set extcommunity soo 1.1:100
Router(config-route-map)# end
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
ip extcommunity-list	Creates an extended community list and controls access to it.
match extcommunity	Matches a BGP VPN extended community list.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
router bgp	Configures the BGP routing process.
route-target	Creates a route target extended community for a VRF.
set extcommunity cost	Creates a set clause to apply the cost community attribute to routes that pass through a route map.
set extcommunity rt	Creates a set clause to apply the route target community attributes to routes that pass through a route map.
set extcommunity vpn-distinguisher	Creates a set clause that applies a VPN distinguisher attribute to routes that pass through an outbound route map.
show ip extcommunity-list	Displays routes that are permitted by the extended community list.
show route-map	Displays all route maps configured or only the one specified.

set extcommunity vpn-distinguisher

To create a set clause that applies a VPN distinguisher attribute to routes that pass through an outbound route map, use the **set extcommunity vpn-distinguisher** command in route-map configuration mode. To remove all **set extcommunity cost**, **set extcommunity rt**, **set extcommunity soo**, and **set extcommunity vpn-distinguisher** clauses from the route-map clause, use the **no** form of this command.

set extcommunity vpn-distinguisher {*vpn-extended-community-value*| **range** *start-range-value end-range-value*}

no set extcommunity

Syntax Description

<i>vpn-extended-community-value</i>	Specifies the VPN distinguisher extended community value to be set. The value can be one of the following formats: <i>autonomous-system-number:network-number</i> <i>ip-address:network-number</i> The colon separates the autonomous system number and network number, or the IP address and network number.
range	Specifies that the VPN distinguisher values being set are in a contiguous range, from the <i>start-range-value</i> through the <i>end-range-value</i> , inclusive.
<i>start-range-value</i>	Starting value of a range of VPN distinguisher extended community values. The formats allowed are the same as those for the <i>vpn-extended-community-value</i> shown above.
<i>end-range-value</i>	Ending value of a range of VPN distinguisher extended community values. The formats allowed are the same as those for the <i>vpn-extended-community-value</i> shown above.

Command Default

There is no default value.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.
15.3(2)S	This command was modified. The extended community values can be specified as a range of values.
Cisco IOS XE Release 3.9S	This command was modified. The range keyword and the <i>start-range-value</i> and <i>end-range-value</i> arguments were added.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

Configure this command on an egress ASBR for the purpose of replacing a route target (RT) with a VPN distinguisher attribute. Thus, the RT is kept hidden from the neighboring ASBR in another AS.

**Note**

The **no** form of this command removes all **set extcommunity cost**, **set extcommunity rt**, **set extcommunity soo**, and **set extcommunity vpn-distinguisher** clauses from the route-map clause.

Examples

The following example shows the egress ASBR configuration to replace a route target (RT) with a VPN distinguisher extended community attribute. IP extended community list 1 is configured to filter VPN routes by permitting only routes with RT 101:100. A route map named vpn-id-map1 says that any route that matches on routes that are allowed by IP extended community list 1 is subject to two **set** commands. The first **set** command deletes the RT from the route. The second **set** command sets the VPN distinguisher attribute to 111:100. In autonomous system 2000, for the VPNv4 address family, the route map vpn-id-map1 is applied to routes going out to the neighbor at 192.168.101.1.

```
ip extcommunity-list 1 permit rt 101:100
!
route-map vpn-id-map1 permit 10
 match extcommunity 1
 set extcomm-list 1 delete
 set extcommunity vpn-distinguisher 111:100
!
route-map vpn-id-map1 permit 20
!
router bgp 2000
 address-family vpnv4
  neighbor 192.168.101.1 route-map vpn-id-map1 out
 exit-address-family
!
```

In the following example, on an egress ASBR, routes that have RT 201:100 are in the extended community list 22. A route map named rt-mapping matches on extended community list 22 and deletes the RT from routes in the community list. Routes that match the community list have their VPN distinguisher set to VPN distinguishers in the range from 600:1 to 600:8. The route map is applied to the neighbor 192.168.103.1.

```
ip extcommunity-list 22 permit rt 201:100
!
route-map rt-mapping permit 10
```

set extcommunity vpn-distinguisher

```

match extcommunity 22
set extcomm-list 22 delete
set extcommunity vpn-distinguisher range 600:1 600:8
!
route-map rt-mapping permit 20
!
router bgp 3000
neighbor 192.168.103.1 remote-as 3000
address-family vpnv4
neighbor 192.168.103.1 activate
neighbor 192.168.103.1 route-map rt-mapping out
exit-address-family
!
```

Related Commands

Command	Description
set extcommunity cost	Sets the cost extended community attribute for routes that pass a route map.
set extcommunity rt	Sets a route target extended community attribute for routes that pass a route map.
set extcommunity soo	Sets a site of origin extended community value for routes that pass a route map.
set extcomm-list delete	Deletes a route target (RT) or a VPN distinguisher attribute from routes in the specified list that pass a route map.
show ip bgp	Displays entries in the BGP routing table.

set ip dscp (bmp)

To configure the IP Differentiated Services Code Point (DSCP) values for BGP Monitoring Protocol (BMP) servers, use the **set ip dscp** command in BMP server configuration mode. To disable IP DSCP configuration, use the **no** form of the command.

set ip dscp *dscp-value*

no set ip dscp *dscp-value*

Syntax Description

<i>dscp-value</i>	Specifies the DSCP value used for IP precedence (assigning a priority to each IP packet). The DSCP value ranges from 0 to 7.

Command Default

The IP precedence value is not configured for the BMP servers.

Command Modes

BMP server configuration (config-router-bmpsrvr)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use the **bmp server** command to enter BMP server configuration mode and configure a specific BMP server. To configure BGP BMP neighbors to which the BMP servers establish a connection, use the **neighbor bmp-activate** command in router configuration mode. Use the **show ip bgp bmp** command to verify the IP DSCP value that has been configured. The DSCP values that range from 0 to 7, define the priority levels that are assigned to the IP packets send from the BMP servers to the BGP BMP neighbors. The priority level represented by the IP DSCP values are:

- 0—Routine
- 1—Priority
- 2—Immediate
- 3—Flash
- 4—Flash override
- 5—Critical Enhanced Communications Port (ECP)
- 6—Internetwork Control

- 7—Network Control

Examples

The following example show how to enter BMP server configuration mode and configure IP DSCP values for BMP servers 1 and 2:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp server 1
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 10.1.1.1 port-number 8000
Device(config-router-bmpsrvr)# set ip dscp 5
Device(config-router-bmpsrvr)# exit-bmp-server-mode
Device(config-router)# bmp server 2
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 20.1.1.1 port-number 9000
Device(config-router-bmpsrvr)# set ip dscp 7
Device(config-router-bmpsrvr)# end
```

The following is sample output from the **show ip bgp bmp server** command for BMP server number 1 and 2. The “IP Precedence value” field in the output display the IP DSCP values configured for the BMP servers 1 and 2:

```
Device# show ip bgp bmp server detail | include Precedence

IP Precedence value : 5
IP Precedence value : 7
```

Related Commands

Command	Description
bmp server	Enters BMP server configuration mode to configure specific BMP servers.
neighbor bmp-activate	Activates BMP monitoring for BGP neighbors.
show ip bgp bmp	Displays information about BMP servers and neighbors.

set ip next-hop self (BGP)

To configure local routes with next hop of self (for Border Gateway Protocol (BGP) only), use the **set ip next-hop self** command in route-map configuration mode. To delete the configuration of local routes with a next hop of self, use the **no** form of this command.

set ip next-hop self

no set ip next-hop self

Command Default No local routes with next hop of self are configured for BGP.

Command Modes Route-map configuration (config-route-map)

Command History	Release	Modification
	12.2(33)SRE	This command was introduced.

Usage Guidelines The **set ip next-hop self** command configures local routes with next hop of self (for BGP only). This command is applicable to VPNv4 and VPNv6 address families only. Routes distributed by protocols other than BGP are not affected.

Examples The following example shows how to configure a next hop of self for static routes:

```
route-map set-peer-address permit 10
match source-protocol static
set ip next-hop self
```

Related Commands	Command	Description
	bgp route-map priority	Configures the route-map priority for a local BGP routing process.

set ip next-hop (BGP)

To indicate where to output packets that pass a match clause of a route map for policy routing, use the **set ip next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set ip next-hop *ip-address*[...*ip-address*][*peer-address*]

no set ip next-hop *ip-address*[...*ip-address*][*peer-address*]

Syntax Description

<i>ip-address</i>	IP address of the next hop to which packets are output. It need not be an adjacent router.
peer-address	(Optional) Sets the next hop to be the BGP peering address.

Command Default

This command is disabled by default.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
11.0	This command was introduced.
12.0	The peer-address keyword 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 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the *ip-address* argument.

Use the **ip policy route-map** interface configuration command, the **route-map** global configuration command, and the **match** and **set** route-map configuration commands to define the conditions for policy routing packets. The **ip policy route-map** command identifies a route map by name. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria* --the conditions under which policy routing occurs. The **set** commands specify the *set actions* --the particular routing actions to perform if the criteria enforced by the **match** commands are met.

If the first next hop specified with the **set ip next-hop** command is down, the optionally specified IP addresses are tried in turn.

When the **set ip next-hop** command is used with the **peer-address** keyword in an inbound route map of a BGP peer, the next hop of the received matching routes will be set to be the neighbor peering address, overriding any third-party next hops. So the same route map can be applied to multiple BGP peers to override third-party next hops.

When the **set ip next-hop** command is used with the **peer-address** keyword in an outbound route map of a BGP peer, the next hop of the advertised matching routes will be set to be the peering address of the local router, thus disabling the next hop calculation. The **set ip next-hop** command has finer granularity than the (per-neighbor) **neighbor next-hop-self** command, because you can set the next hop for some routes, but not others. The **neighbor next-hop-self** command sets the next hop for all routes sent to that neighbor.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

- 1 **set ip next-hop**
- 2 **set interface**
- 3 **set ip default next-hop**
- 4 **set default interface**



Note

To avoid a common configuration error for reflected routes, do not use the **set ip next-hop** command in a route map to be applied to BGP route reflector clients.

Configuring the **set ip next-hop ...ip-address** command on a VRF interface allows the next hop to be looked up in a specified VRF address family. In this context, the *...ip-address* argument matches that of the specified VRF instance.

Examples

In the following example, three routers are on the same FDDI LAN (with IP addresses 10.1.1.1, 10.1.1.2, and 10.1.1.3). Each is in a different autonomous system. The **set ip next-hop peer-address** command specifies that traffic from the router (10.1.1.3) in remote autonomous system 300 for the router (10.1.1.1) in remote autonomous system 100 that matches the route map is passed through the router bgp 200, rather than sent directly to the router (10.1.1.1) in autonomous system 100 over their mutual connection to the LAN.

```
router bgp 200
 neighbor 10.1.1.3 remote-as 300
 neighbor 10.1.1.3 route-map set-peer-address out
 neighbor 10.1.1.1 remote-as 100
 route-map set-peer-address permit 10
 set ip next-hop peer-address
```

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.

Command	Description
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match length	Bases policy routing on the Level 3 length of a packet.
neighbor next-hop-self	Disables next hop processing of BGP updates on the router.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol to another, or enables policy routing.
set default interface	Indicates where to output packets that pass a match clause of a route map for policy routing and that have no explicit route to the destination.
set interface	Indicates where to output packets that pass a match clause of a route map for policy routing.
set ip default next-hop	Indicates where to output packets that pass a match clause of a route map for policy routing and for which the Cisco IOS software has no explicit route to a destination.

set ipv6 next-hop (BGP)

To indicate where to output IPv6 packets that pass a match clause of a route map for policy routing, use the **set ipv6 next-hop** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set ipv6 next-hop {*ipv6-address* [*link-local-address*]} **encapsulate l3vpn** *profile name* | **peer-address**}
no set ipv6 next-hop {*ipv6-address* [*link-local-address*]} **encapsulate l3vpn** *profile name* | **peer-address**}

Syntax Description

<i>ipv6-address</i>	IPv6 global address of the next hop to which packets are output. It need not be an adjacent router. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
<i>link-local-address</i>	(Optional) IPv6 link-local address of the next hop to which packets are output. It must be an adjacent router. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
encapsulate l3vpn	Sets the encapsulation profile for VPN nexthop.
<i>profile name</i>	Name of the Layer 3 encapsulation profile.
peer-address	(Optional) Sets the next hop to be the BGP peering address.

Command Default IPv6 packets are forwarded to the next hop router in the routing table.

Command Modes Route-map configuration (config-route-map)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
12.2(33)SRE	This command was modified. The encapsulate l3vpn keyword was added.

Usage Guidelines

The **set ipv6 next-hop** command is similar to the **set ip next-hop** command, except that it is IPv6-specific. The **set** commands specify the *set actions* --the particular routing actions to perform if the criteria enforced by the **match** commands are met.

When the **set ipv6 next-hop** command is used with the **peer-address** keyword in an inbound route map of a BGP peer, the next hop of the received matching routes will be set to be the neighbor peering address, overriding any third-party next hops. So the same route map can be applied to multiple BGP peers to override third-party next hops.

When the **set ipv6 next-hop** command is used with the **peer-address** keyword in an outbound route map of a BGP peer, the next hop of the advertised matching routes will be set to be the peering address of the local router, thus disabling the next hop calculation. The **set ipv6 next-hop** command has finer granularity than the per-neighbor **neighbor next-hop-self** command, because you can set the next hop for some routes, but not others. The **neighbor next-hop-self** command sets the next hop for all routes sent to that neighbor.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

- 1 **set ipv6 next-hop**
- 2 **set interface**
- 3 **set ipv6 default next-hop**
- 4 **set default interface**

Configuring the **set ipv6 next-hop ipv6-address** command on a VRF interface allows the next hop to be looked up in a specified VRF address family. In this context, the *ipv6-address* argument matches that of the specified VRF instance.

Examples

The following example configures the IPv6 multiprotocol BGP peer FE80::250:BFF:FE0E:A471 and sets the route map named nh6 to include the IPv6 next hop global addresses of Fast Ethernet interface 0 of the neighbor in BGP updates. The IPv6 next hop link-local address can be sent to the neighbor by the nh6 route map or from the interface specified by the **neighbor update-source** router configuration command.

```
router bgp 170
 neighbor FE80::250:BFF:FE0E:A471 remote-as 150
 neighbor FE80::250:BFF:FE0E:A471 update-source fastether 0
 address-family ipv6
  neighbor FE80::250:BFF:FE0E:A471 activate
  neighbor FE80::250:BFF:FE0E:A471 route-map nh6 out
 route-map nh6
  set ipv6 next-hop 3FFE:506::1
```

**Note**

If you specify only the global IPv6 next hop address (the *ipv6-address* argument) with the **set ipv6 next-hop** command after specifying the neighbor interface (the *interface-type* argument) with the **neighbor update-source** command, the link-local address of the neighbor interface is included as the next hop in the BGP updates. Therefore, only one route map that sets the global IPv6 next hop address in BGP updates is required for multiple BGP peers that use link-local addresses.

Related Commands

Command	Description
ip policy route-map	Identifies a route map to use for policy routing on an interface.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
match ipv6 next-hop	Distributes IPv6 routes that have a next hop prefix permitted by a prefix list.
match ipv6 route-source	Distributes IPv6 routes that have been advertised by routers at an address specified by a prefix list.
neighbor next-hop-self	Disables next-hop processing of BGP updates on the router.
neighbor update-source	Specifies that the Cisco IOS software allow BGP sessions to use any operational interface for TCP connections
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

set metric (BGP-OSPF-RIP)

To set the metric value for a routing protocol, use the **setmetric** command in route-map configuration mode. To return to the default metric value, use the **no** form of this command.

set metric *metric-value*

no set metric *metric-value*

Syntax Description

<i>metric-value</i>	Metric value; an integer from -294967295 to 294967295. This argument applies to all routing protocols except Enhanced Interior Gateway Routing Protocol (EIGRP).

Command Default

The dynamically learned metric value.

Command Modes

Route-map configuration (config-route-map)

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

We recommend that you consult your Cisco technical support representative before changing the default value.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria* --the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions* --the particular redistribution 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 *setactions* to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

The following example sets the metric value for the routing protocol to 100:

```
route-map set-metric
 set metric 100
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set ip next-hop	Specifies the address of the next hop.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.

Command	Description
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set origin (BGP)	Sets the BGP origin code.
set tag (IP)	Sets the value of the destination routing protocol.

set metric-type internal

To set the Multi Exit Discriminator (MED) value on prefixes advertised to external BGP (eBGP) neighbors to match the Interior Gateway Protocol (IGP) metric of the next hop, use the **set metric-type internal** command in route-map configuration mode. To return to the default, use the **no** form of this command.

set metric-type internal

no set metric-type internal

Syntax Description This command has no arguments or keywords.

Command Default This command is disabled by default.

Command Modes Route-map configuration (config-route-map)

Command History	Release	Modification
	10.3	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 will cause BGP to advertise a MED value that corresponds to the IGP metric associated with the next hop of the route. This command applies to generated, internal BGP (iBGP)-, and eBGP-derived routes.

If this command is used, multiple BGP speakers in a common autonomous system can advertise different MED values for a particular prefix. Also, note that if the IGP metric changes, BGP will readvertise the route every 10 minutes.

Use the **route-map** global configuration command and the **match** and **set** route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria* --the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions* --the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-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 the route map are met. When all match criteria are met, all set actions are performed.

**Note**

This command is not supported for redistributing routes into Border Gateway Protocol (BGP).

Examples

In the following example, the MED value for all the advertised routes to neighbor 172.16.2.3 is set to the corresponding IGP metric of the next hop:

```
router bgp 109
 network 172.16.0.0
 neighbor 172.16.2.3 remote-as 200
 neighbor 172.16.2.3 route-map setMED out
!
route-map setMED permit 10
 match as-path 1
 set metric-type internal
!
ip as-path access-list 1 permit .*
```

Related Commands

Command	Description
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

set origin (BGP)

To set the BGP origin code, use the **set origin** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set origin {**igp**|**egp** *autonomous-system-number*|**incomplete**}

no set origin {**igp**|**egp** *autonomous-system-number*|**incomplete**}

Syntax Description

igp	Remote Interior Gateway Protocol (IGP) system.
egp	Local Exterior Gateway Protocol (EGP) system.
<i>autonomous-system-number</i>	Number of a remote autonomous system number. The range of values for this argument is any valid autonomous system number from 1 to 65535.
incomplete	Unknown heritage.

Command Default

The origin of the route is based on the path information of the route in the main IP routing table.

Command Modes

Route-map configuration (config-route-map)

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.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.4(2)T	This command was modified. The egp keyword and <i>autonomous-system-number</i> argument were removed.
12.0(33)S3	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

You must have a match clause (even if it points to a “permit everything” list) if you want to set the origin of a route. Use this command to set a specific origin when a route is redistributed into BGP. When routes are redistributed, the origin is usually recorded as incomplete, identified with a ? in the BGP table.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria* --the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions* --the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-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. When all match criteria are met, all set actions are performed.

Examples

The following example sets the origin of routes that pass the route map to IGP:

```
route-map set_origin
match as-path 10
set origin igp
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
router bgp	Configures the BGP routing process.
set as-path	Modifies an autonomous system path for BGP routes.

set traffic-index

To indicate how to classify packets that pass a match clause of a route map for Border Gateway Protocol (BGP) policy accounting, use the **set traffic-index** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set traffic-index *bucket-number*

no set traffic-index *bucket-number*

Syntax Description

<i>bucket-number</i>	Number that represents a bucket into which packet and byte statistics are collected for a specific traffic classification. The range is from 1 to 64.

Command Default

Routing traffic is not classified.

Command Modes

Route-map configuration (config-route-map)

Command History

Release	Modification
12.0(9)S	This command was introduced.
12.0(17)ST	This command was integrated into Cisco IOS Release 12.0(17)ST.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.0(22)S	Support for 64 buckets was added for the Cisco 12000 series Internet router.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T and support for 64 buckets was added for all platforms.
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 **set traffic-index** route-map configuration command, the **route-map** global configuration command, and a **match** route-map configuration command to define the conditions for BGP policy accounting. The **match** commands specify the *match criteria* --the conditions under which policy routing occurs. The **set**

traffic-index command specifies the *set actions* --the particular routing actions to perform if the criteria specified by the **match** commands are met.

Examples

In the following example, an index for BGP policy accounting is set according to autonomous system path criteria:

```
route-map buckets permit 10
  match as-path 1
  set traffic-index 1
```

Related Commands

Command	Description
bgp-policy	Enables BGP policy accounting or policy propagation on an interface.
route-map	Defines the conditions for redistributing routes from one routing protocol to another, or enables policy routing.

set weight

To specify the BGP weight for the routing table, use the **set weight** command in route-map configuration mode. To delete an entry, use the **no** form of this command.

set weight *number*

no set weight *number*

Syntax Description

<i>number</i>	Weight value. It can be an integer ranging from 0 to 65535.

Command Default

The weight is not changed by the specified route map.

Command Modes

Route-map configuration (config-route-map)

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

The implemented weight is based on the first matched autonomous system path. Weights indicated when an autonomous system path is matched override the weights assigned by global **neighbor** commands. In other words, the weights assigned with the **set weight** route-map configuration command override the weights assigned using the **neighbor weight** command.

Examples

The following example sets the BGP weight for the routes matching the autonomous system path access list to 200:

```
route-map set-weight  
match as-path 10  
set weight 200
```

Related Commands

Command	Description
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a BGP community.
match interface (IP)	Distributes routes that have their next hop out one of the interfaces specified.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
match ip next-hop	Redistributes any routes that have a next hop router address passed by one of the access lists specified.
match ip route-source	Redistributes routes that have been advertised by routers and access servers at the address specified by the access lists.
match metric (IP)	Redistributes routes with the metric specified.
match route-type (IP)	Redistributes routes of the specified type.
match tag	Redistributes routes in the routing table that match the specified tags.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
set automatic-tag	Automatically computes the tag value.
set community	Sets the BGP communities attribute.
set ip next-hop	Specifies the address of the next hop.
set level (IP)	Indicates where to import routes.
set local-preference	Specifies a preference value for the autonomous system path.
set metric (BGP, OSPF, RIP)	Sets the metric value for a routing protocol.
set metric-type	Sets the metric type for the destination routing protocol.
set origin (BGP)	Sets the BGP origin code.

Command	Description
set tag (IP)	Sets the value of the destination routing protocol.
set weight	Specifies the BGP weight for the routing table.

show bgp all community

To display routes for all address families belonging to a particular Border Gateway Protocol (BGP) community, use the **show bgp all community** command in user EXEC or privileged EXEC configuration mode.

show bgp all

community[*community-number*...[*community-number*]][**local-as**][**no-advertise**][**no-export**][**exact-match**]

Syntax Description

<i>community-number</i>	(Optional) Displays the routes pertaining to the community numbers specified. • You can specify multiple community numbers. The range is from 1 to 4294967295 or AA:NN (autonomous system:community number, which is a 2-byte number).
local-as	(Optional) Displays only routes that are not sent outside of the local autonomous system (well-known community).
no-advertise	(Optional) Displays only routes that are not advertised to any peer (well-known community).
no-export	(Optional) Displays only routes that are not exported outside of the local autonomous system (well-known community).
exact-match	(Optional) Displays only routes that match exactly with the BGP community list specified. Note The availability of keywords in the command depends on the command mode. The exact-match keyword is not available in user EXEC mode.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.

Release	Modification
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

You can enter the **local-as**, **no-advertise** and **no-export** keywords in any order. You can set the communities using the **set community** command.

When using the **show bgp all community** command, be sure to enter the numerical communities before the well-known communities.

For example, the following string is not valid:

```
Router# show bgp all community local-as 111:12345
Use the following string instead:
```

```
Router# show bgp all community 111:12345 local-as
```

Examples

The following is sample output from the **show bgp all community** command, specifying communities of 1, 2345, and 6789012:

```
Router# show bgp all community 1 2345 6789012 no-advertise local-as no-export exact-match
For address family: IPv4 Unicast
BGP table version is 5, local router ID is 30.0.0.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
*> 10.0.3.0/24      10.0.0.4                 0           0 4 3 ?
*> 10.1.0.0/16      10.0.0.4                 0           0 4 ?
*> 10.12.34.0/24    10.0.0.6                 0           0 6 ?
```

The table below describes the significant fields shown in the display.

Table 10: show bgp all community Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	The router ID of the router on which the BGP communities are set to display. A 32-bit number written as 4 octets separated by periods (dotted-decimal format).

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s--The table entry is suppressed. d--The table entry is dampened. h--The table entry is history. *--The table entry is valid. >--The table entry is the best entry to use for that network. i--The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e--Entry originated from the Exterior Gateway Protocol (EGP). ?--Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	The network address and network mask of a network entity. The type of address depends on the address family.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. The type of address depends on the address family.
Metric	The value of the inter autonomous system metric. This field is not used frequently.
LocPrf	Local preference value as set with the set local-preference command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

Related Commands

Command	Description
set community	Sets BGP communities.

Command	Description
set local-preference	Specifies a preference value for the autonomous system path.

show bgp all neighbors

To display information about Border Gateway Protocol (BGP) connections to neighbors of all address families, use the **show bgp all neighbors** command in user EXEC or privileged EXEC mode.

show bgp all neighbors [*ip-address*|*ipv6-address*] [**advertised-routes**|**dampened-routes**|**flap-statistics**|**paths** [*reg-exp*]|**policy** [**detail**]|**received prefix-filter**|**received-routes**|**routes**]

Syntax Description

<i>ip-address</i>	(Optional) IP address of a neighbor. If this argument is omitted, information about all neighbors is displayed.
<i>ipv6-address</i>	(Optional) Address of the IPv6 BGP-speaking neighbor. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
advertised-routes	(Optional) Displays all routes that have been advertised to neighbors.
dampened-routes	(Optional) Displays the dampened routes received from the specified neighbor (for external BGP peers only).
flap-statistics	(Optional) Displays the flap statistics of the routes learned from the specified neighbor (for external BGP peers only).
paths <i>reg-exp</i>	(Optional) Displays autonomous system paths learned from the specified neighbor. An optional regular expression can be used to filter the output.
policy	(Optional) Displays the policies applied to neighbor per address family.
detail	(Optional) Displays detailed policy information such as route maps, prefix lists, community lists, Access Control Lists (ACLs), and autonomous system path filter lists.
received prefix-filter	(Optional) Displays the prefix-list (outbound route filter [ORF]) sent from the specified neighbor.
received-routes	(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.

routes	(Optional) Displays all routes that are received and accepted. The output displayed when this keyword is entered is a subset of the output displayed by the received-routes keyword.

Command Default The output of this command displays information for all neighbors.

Command Modes User EXEC (>)
Privileged EXEC (#)

Command History	Release	Modification
	12.3(26)	This command was introduced.
	12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S and was made available in privileged EXEC mode.
	12.2(19)S	This command was made available in user EXEC mode.
	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(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
	12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T. The policy keyword was added.
	12.2(33)SRB	The policy keyword was integrated into Cisco IOS Release 12.2(33)SRB.
	Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines Use the **show bgp all neighbors** command to display BGP and TCP connection information for neighbor sessions specific to address families such as IPv4, IPv6, Network Service Access Point (NSAP), Virtual Private Network (VPN) v4, and VPNv6.

Examples The following example shows output of the **show bgp all neighbors** command:

```
Router# show bgp all neighbors
For address family: IPv4 Unicast
BGP neighbor is 172.16.232.53, remote AS 100, external link
Member of peer-group internal for session parameters
BGP version 4, remote router ID 172.16.232.53
BGP state = Established, up for 13:40:17
Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
```

show bgp all neighbors

```

Message statistics:
  InQ depth is 0
  OutQ depth is 0

                Sent      Rcvd
Opens:           3         3
Notifications:   0         0
Updates:         0         0
Keepalives:     113       112
Route Refresh:   0         0
Total:          116       11
Default minimum time between advertisement runs is 5 seconds
Connections established 22; dropped 21
Last reset 13:47:05, due to BGP Notification sent, hold time expired
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 3FFE:700:20:1::12, Local port: 55345
Foreign host: 3FFE:700:20:1::11, Foreign port: 179
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x1A0D543C):
Timer           Starts    Wakeups      Next
Retrans         1218        5            0x0
TimeWait         0          0            0x0
AckHold         3327       3051         0x0
SendWnd         0          0            0x0
KeepAlive       0          0            0x0
GiveUp          0          0            0x0
PmtuAger        0          0            0x0
DeadWait        0          0            0x0
iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354  sndwnd: 15531
irs: 821333727  rcvnxt: 821591465  rcvwnd: 15547  delrcvwnd: 837
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle
Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent: 4445 (retransmit: 5), with data: 4445, total data bytes: 244128
For address family: IPv6 Unicast
For address family: IPv4 MDT
For address family: VPNv4 Unicast
For address family: VPNv6 Unicast
For address family: IPv4 Multicast
For address family: IPv6 Multicast
For address family: NSAP Unicast

```

The table below describes the significant fields shown in the display.

Table 11: show bgp all neighbors Field Descriptions

Field	Description
For address family:	Address family to which the following fields refer.
BGP neighbor	IP address of the BGP neighbor and its autonomous system number.
remote AS	Autonomous system number of the neighbor.
external link	External Border Gateway Protocol (eBGP) peer.
BGP version	BGP version being used to communicate with the remote router.
remote router ID	IP address of the neighbor.
BGP state	State of this BGP connection.

Field	Description
up for	Time, in hh:mm:ss, that the underlying TCP connection has been in existence.
Last read	Time, in hh:mm:ss, since BGP last received a message from this neighbor.
hold time	Time, in seconds, that BGP will maintain the session with this neighbor without receiving messages.
keepalive interval	Time interval, in seconds, at which keepalive messages are transmitted to this neighbor.
Message statistics	Statistics organized by message type.
InQ depth is	Number of messages in the input queue.
OutQ depth is	Number of messages in the output queue.
Sent	Total number of transmitted messages.
Rcvd	Total number of received messages.
Opens	Number of open messages sent and received.
Notifications	Number of notification (error) messages sent and received.
Updates	Number of update messages sent and received.
Keepalives	Number of keepalive messages sent and received.
Route Refresh	Number of route refresh request messages sent and received.
Total	Total number of messages sent and received.
Default minimum time between...	Time, in seconds, between advertisement transmissions.
Connections established	Number of times a TCP and BGP connection has been successfully established.
dropped	Number of times that a valid session has failed or been taken down.
Last reset	Time, in hh:mm:ss, since this peering session was last reset. The reason for the reset is displayed on this line.

Field	Description
External BGP neighbor may be...	Indicates that the BGP Time-to-live (TTL) security check is enabled. The maximum number of hops that can separate the local and remote peer is displayed on this line.
Connection state	Connection status of the BGP peer.
Local host, Local port	IP address of the local BGP speaker and the port number.
Foreign host, Foreign port	Neighbor address and BGP destination port number.
Enqueued packets for retransmit:	Packets queued for retransmission by TCP.
Event Timers	TCP event timers. Counters are provided for starts and wakeups (expired timers).
Retrans	Number of times a packet has been retransmitted.
TimeWait	Time waiting for the retransmission timers to expire.
AckHold	Acknowledgment hold timer.
SendWnd	Transmission (send) window.
KeepAlive	Number of keepalive packets.
GiveUp	Number times a packet is dropped due to no acknowledgment.
PmtuAger	Path MTU discovery timer.
DeadWait	Expiration timer for dead segments.
iss:	Initial packet transmission sequence number.
snduna:	Last transmission sequence number that has not been acknowledged.
sndnxt:	Next packet sequence number to be transmitted.
sndwnd:	TCP window size of the remote host.
irs:	Initial packet receive sequence number.
rcvnxt:	Last receive sequence number that has been locally acknowledged.
rcvwnd:	TCP window size of the local host.

Field	Description
delrcvwnd:	Delayed receive window--data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT:	A calculated smoothed round-trip timeout.
RTTO:	Round-trip timeout.
RTV:	Variance of the round-trip time.
KRTT:	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.
minRTT:	Smallest recorded round-trip timeout (hard-wire value used for calculation).
maxRTT:	Largest recorded round-trip timeout.
ACK hold:	Length of time the local host will delay an acknowledgment to carry (piggyback) additional data.
IP Precedence value:	IP precedence of the BGP packets.
Datagrams	Number of update packets received from a neighbor.
Rcvd:	Number of received packets.
with data	Number of update packets sent with data.
total data bytes	Total amount of data received, in bytes.
Sent	Number of update packets sent.
with data	Number of update packets received with data.
total data bytes	Total amount of data sent, in bytes.

Related Commands

Command	Description
router bgp	Configures the BGP routing process.

show bgp ipv6

To display entries in the IPv6 Border Gateway Protocol (BGP) routing table, use the **show bgp ipv6** command in user EXEC or privileged EXEC mode.

show bgp ipv6 {**unicast**|**multicast**} [*ipv6-prefix/prefix-length*] [**longer-prefixes**] [**labels**]

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
multicast	Specifies IPv6 multicast address prefixes.
<i>ipv6-prefix</i>	(Optional) IPv6 network number, entered to display a particular network in the IPv6 BGP routing table. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
<i>/ prefix-length</i>	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
longer-prefixes	(Optional) Displays the route and more specific routes.
labels	(Optional) Displays Multiprotocol Label Switching (MPLS) label information.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	MPLS label information was added to the display.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	MPLS label value advertised for the IPv6 prefix was added to the display.
12.0(26)S	The unicast and multicast keywords were added.

Release	Modification
12.2(25)S	6PE multipath information was added to the display.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
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 introduced on Cisco ASR 1000 series routers.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

The **show bgp ipv6** command provides output similar to the **show ip bgp** command, except that it is IPv6-specific.

Examples

The following is sample output from the **show bgp ipv6** command:

```
Router# show bgp ipv6 unicast
BGP table version is 12612, local router ID is 172.16.7.225
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network                Next Hop           Metric LocPrf Weight Path
*
*                3FFE:C00:E:C::2                0 3748 4697 1752 i
*                3FFE:1100:0:CC00::1                0 1849 1273 1752 i
* 2001:618:3::/48 3FFE:C00:E:4::2                1 0 4554 1849 65002 i
*>                3FFE:1100:0:CC00::1                0 1849 65002 i
* 2001:620::/35    2001:0DB8:0:F004::1                0 3320 1275 559 i
*                3FFE:C00:E:9::2                0 1251 1930 559 i
*                3FFE:3600::A                0 3462 10566 1930 559 i
*                3FFE:700:20:1::11                0 293 1275 559 i
*                3FFE:C00:E:4::2                1 0 4554 1849 1273 559 i
*                3FFE:C00:E:B::2                0 237 3748 1275 559 i
```

The table below describes the significant fields shown in the display.

Table 12: show bgp ipv6 Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted decimal format).

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s--The table entry is suppressed. • d--The table entry is dampened. • h--The table entry is history. • *--The table entry is valid. • >--The table entry is the best entry to use for that network. • i--The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i--Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. • e--Entry originated from the Exterior Gateway Protocol (EGP). • ?--Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IPv6 address of a network entity.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.

Field	Description
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show bgp ipv6** command, showing information for prefix 3FFE:500::/24:

```
Router# show bgp ipv6 unicast 3FFE:500::/24
BGP routing table entry for 3FFE:500::/24, version 19421
Paths: (6 available, best #1)
  Advertised to peer-groups:
    6BONE
  293 3425 2500
    3FFE:700:20:1::11 from 3FFE:700:20:1::11 (192.168.2.27)
      Origin IGP, localpref 100, valid, external, best
  4554 293 3425 2500
    3FFE:C00:E:4::2 from 3FFE:C00:E:4::2 (192.168.1.1)
      Origin IGP, metric 1, localpref 100, valid, external
  33 293 3425 2500
    3FFE:C00:E:5::2 from 3FFE:C00:E:5::2 (209.165.18.254)
      Origin IGP, localpref 100, valid, external
      Dampinfo: penalty 673, flapped 429 times in 10:47:45
  6175 7580 2500
    3FFE:C00:E:1::2 from 3FFE:C00:E:1::2 (209.165.223.204)
      Origin IGP, localpref 100, valid, external
  1849 4697 2500, (suppressed due to dampening)
    3FFE:1100:0:CC00::1 from 3FFE:1100:0:CC00::1 (172.31.38.102)
      Origin IGP, localpref 100, valid, external
      Dampinfo: penalty 3938, flapped 596 times in 13:03:06, reuse in 00:59:10
  237 10566 4697 2500
    3FFE:C00:E:B::2 from 3FFE:C00:E:B::2 (172.31.0.3)
      Origin IGP, localpref 100, valid, external
```

The following is sample output from the **show bgp ipv6** command, showing MPLS label information for an IPv6 prefix that is configured to be an IPv6 edge router using MPLS:

```
Router# show bgp ipv6 unicast 2001:0DB8::/32
BGP routing table entry for 2001:0DB8::/32, version 15
Paths: (1 available, best #1)
  Not advertised to any peer
  Local
    ::FFFF:192.168.99.70 (metric 20) from 192.168.99.70 (192.168.99.70)
      Origin IGP, localpref 100, valid, internal, best, mpls label 17
```

To display the top of the stack label with label switching information, enter the **show bgp ipv6EXEC** command with the **labels** keyword:

```
Router# show bgp ipv6 unicast labels
Network      Next Hop      In tag/Out tag
2001:0DB8::/32  ::FFFF:192.168.99.70  notag/20
```



Note

If a prefix has not been advertised to any peer, the display shows "Not advertised to any peer."

The following is sample output from the **show bgp ipv6** command, showing 6PE multipath information. The prefix 4004::/64 is received by BGP from two different peers and therefore two different paths:

```
Router# show bgp ipv6 unicast
BGP table version is 28, local router ID is 172.10.10.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
```

```

internal,
      r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          Next Hop          Metric LocPrf Weight Path
*>i4004::/64          ::FFFF:172.11.11.1
                                0      100      0 ?
* i                   ::FFFF:172.30.30.1
                                0      100      0 ?

```

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection or session.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

show bgp l2vpn evpn

To display Layer 2 Virtual Private Network (L2VPN) Ethernet Virtual Private Network (EVPN) address family information from the Border Gateway Protocol (BGP) table, use the **show bgp l2vpn evpn** command in user EXEC or privileged EXEC mode.

```
show bgp l2vpn evpn [all| rd route-distinguisher] [route-type {ethernet-ad| ethernet-segment|
inclusive-mcast| mac-advertisement| nn}] [ bgp-keyword ]
```

Syntax Description

all	(Optional) Displays the complete L2VPN EVPN database.
rd <i>route-distinguisher</i>	(Optional) Displays routes that match the specified route distinguisher (RD).
route-type	(Optional) Displays route type information.
ethernet-ad	Displays Ethernet auto discovery route type information.
ethernet-segment	Displays Ethernet segment route type information.
inclusive-mcast	Displays Ethernet inclusive multicast route type information.
mac-advertisement	Displays Ethernet MAC advertisement route type information.
<i>nn</i>	L2VPN EVPN Network Layer Reachability Information (NLRI) route type information.
<i>bgp-keyword</i>	(Optional) Argument representing a show ip bgp command keyword that can be added to this command. See the table below.

Command Default

If no arguments or keywords are specified, this command displays the complete L2VPN EVPN database.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Release	Modification
15.4(1)S	This command was integrated into Cisco IOS Release 15.4(1)S.

Usage Guidelines

The table below displays optional **show ip bgp** command keywords that can be configured with the **show bgp l2vpn evpn** command. Replace the *bgp-keyword* argument with the appropriate keyword from the table. For more details about each command in its **show ip bgp *bgp-keyword*** form, see the *Cisco IOS IP Routing Protocols Command Reference*.

Table 13: Optional show ip bgp Command Keywords and Descriptions

Keyword	Description
bmp	Displays information about the BGP Monitoring Protocol (BMP) servers and neighbors.
cluster-ids	Displays configured cluster IDs.
community	Displays routes that match a specified community.
community-list	Displays routes that match a specified community list.
dampening	Displays paths suppressed because of dampening (BGP route from peer is up and down).
extcommunity-list	Displays routes that match a specified extcommunity list.
filter-list	Displays routes that conform to the filter list.
inconsistent-as	Displays only routes that have inconsistent autonomous systems of origin.
neighbors	Displays details about TCP and BGP neighbor connections.
nexthops	Displays nexthop address table.
path-attribute	Displays path attribute-specific information.
paths [<i>regexp</i>]	Displays autonomous system path information. If the optional <i>regexp</i> argument is entered, the autonomous system paths that are displayed match the autonomous system path regular expression.
peer-group	Displays information about peer groups.

Keyword	Description
pending-prefixes	Displays prefixes that are pending deletion.
quote-regexp	Displays routes that match the quoted autonomous system path regular expression.
regexp	Displays routes that match the autonomous system path regular expression.
replication	Displays the replication status update groups.
rib-failure	Displays BGP routes that failed to install in the routing table (RIB).
sso	Displays BGP SSO information.
summary	Displays a summary of BGP neighbor status.
update-group	Displays information on update groups.
update-sources	Displays update source interface table.
version	Displays prefixes with matching version numbers.

Examples

Device# **show bgp l2vpn evpn all**

```

BGP table version is 5, local router ID is 19.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

      Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 100.100.100.100:11111
  *>i [1][100.100.100.100:11111][AAAABBBBCCCCDDDEEEEE][23456789][101234]/25
      19.0.101.1                      100          0 i
Route Distinguisher: 100.100.100.101:65535
  *>i
[2][100.100.100.101:65535][AAABBBBCCCCDDDEEEEE][12345678][48][AABCCCCDEEEE][16][1111:1111:1111:1111:1111:1111:1004][234567]/49
      19.0.101.1                      100          0 i
Route Distinguisher: 3.3.3.3:400
  *>i [3][3.3.3.3:400][5678][4][123.123.123.123]/17
      19.0.101.1                      100          0 i
Route Distinguisher: 19.0.101.1:100
  *>i [4][19.0.101.1:100][AAAABBBBCCCCDDDEEEEE]/18
      19.0.101.1                      100          0 i

```

The table below describes the significant fields shown in the display.

Table 14: show bgp l2vpn vpls all Field Descriptions

Field	Description
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the device has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.
Route Distinguisher	Route distinguisher that identifies a set of routing and forwarding tables used in virtual private networks.

Device# **show bgp l2vpn evpn all route-type 1**

```

BGP routing table entry for
[1][100.100.100.100:11111][AAAABBBBCCCCDDDEEEE][23456789][101234]/25, version 2
Paths: (1 available, best #1, table EVPN-BGP-Table)
  Advertised to update-groups:
    1          2          3
  Refresh Epoch 1
  Local, (Received from a RR-client)
    19.0.101.1 from 19.0.101.1 (19.0.101.1)
      Origin IGP, localpref 100, valid, internal, best
      Extended Community: RT:100:101 EVPN LABEL:0x1:Label-101234
      rx pathid: 0, tx pathid: 0x0

```

Related Commands

Command	Description
address-family l2vpn	Enters address family configuration mode to configure a routing session using L2VPN endpoint provisioning information.
show ip bgp l2vpn	Displays L2VPN address family information from the BGP table.

show bgp l2vpn vpls

To display Layer 2 Virtual Private Network (L2VPN) Virtual Private LAN Service (VPLS) address family information from the Border Gateway Protocol (BGP) table, use the **show bgp l2vpn vpls** command in user EXEC or privileged EXEC mode.

show bgp l2vpn vpls [**all**| **rd** *route-distinguisher*] [*bgp-keyword*]

Syntax Description

all	Displays the complete L2VPN VPLS database.
rd <i>route-distinguisher</i>	Displays routes that match the specified route distinguisher (RD).
<i>bgp-keyword</i>	(Optional) Argument representing a show ip bgp command keyword that can be added to this command. See the table below.

Command Default

If no arguments or keywords are specified, this command displays the complete L2VPN VPLS database.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

The table below displays optional **show ip bgp** command keywords that can be configured with the **show bgp l2vpn vpls** command. Replace the *bgp-keyword* argument with the appropriate keyword from the table. For more details about each command in its **show ip bgp** *bgp-keyword* form, see the *Cisco IOS IP Routing Protocols Command Reference*.

Table 15: Optional show ip bgp Command Keywords and Descriptions

Keyword	Description
cluster-ids	Displays configured cluster IDs.
community	Displays routes that match a specified community

Keyword	Description
community-list	Displays routes that match a specified community list.
dampening	Displays paths suppressed because of dampening (BGP route from peer is up and down).
extcommunity-list	Displays routes that match a specified extcommunity list.
filter-list	Displays routes that conform to the filter list.
inconsistency	Displays all the inconsistent paths.
inconsistent-as	Displays only routes that have inconsistent autonomous systems of origin.
neighbors	Displays details about TCP and BGP neighbor connections.
nexthops	Displays nexthop address table.
oer-paths	Displays all OER-managed path information.
paths [<i>regex</i>]	Displays autonomous system path information. If the optional <i>regex</i> argument is entered, the autonomous system paths that are displayed match the autonomous system path regular expression.
peer-group	Displays information about peer groups.
pending-prefixes	Displays prefixes that are pending deletion.
prefix-list	Displays routes that match a specified prefix list.
quote-regex	Displays routes that match the quoted autonomous system path regular expression.
regex	Displays routes that match the autonomous system path regular expression.
replication	Displays the replication status update groups.
route-map	Displays routes that match the specified route map.
rt-filter-list	Displays the specified inbound route target filter list.
summary	Displays a summary of BGP neighbor status.
update-group	Displays information on update groups.

Keyword	Description
update-sources	Displays update source interface table.
ve-id	Displays information that match the specified VE ID.
version	Displays prefixes with matching version numbers.

Examples

```
show bgp l2vpn vpls all
```

```

Network                               Next Hop                               Metric LocPrf Weight Path
Route Distinguisher: 200:100
*>i200:100:VEID-6000:Blk-6000/136    80.0.0.2                               100          0 i
Route Distinguisher: 200:101
*>i200:101:VEID-6001:Blk-6000/136    80.0.0.2                               100          0 i
Route Distinguisher: 200:102
*>i200:102:VEID-6002:Blk-6000/136    80.0.0.2                               100          0 i

```

The table below describes the significant fields shown in the display.

Table 16: show bgp l2vpn vpls all Field Descriptions

Field	Description
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.
Route Distinguisher	Route distinguisher that identifies a set of routing and forwarding tables used in virtual private networks.

Related Commands

Command	Description
address-family l2vpn	Enters address family configuration mode to configure a routing session using L2VPN endpoint provisioning information.
show ip bgp l2vpn vpls	Displays L2VPN address family information from the BGP table.

show bgp mvpn

To display entries in the Border Gateway Protocol (BGP) routing table for multicast VPN (MVPN) sessions on the Cisco 10000 series router, use the **show bgp mvpn** command in privileged EXEC mode.

show bgp {**ipv4** | **ipv6**} **mvpn** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} [**dampening** {**dampened-paths** | **parameters** | **flap-statistics** [**filter-list** *access-list-number* | **quote-regexp** *regexp* | **regexp** *regexp*]}]

Syntax Description

ipv4	Specifies IPv4 MVPN address prefixes.
ipv6	Specifies IPv6 MVPN address prefixes.
all	Displays all the entries in the routing table.
rd <i>route-distinguisher</i>	Displays information about the specified VPN route distinguisher.
vrf <i>vrf-name</i>	Displays information about the specified VRF.
dampened-paths	(Optional) Displays information about BGP dampened routes.
parameters	(Optional) Displays detailed BGP dampening information.
flap-statistics	(Optional) Displays BGP flap statistics information.
filter-list <i>access-list-number</i>	(Optional) Displays flap statistics for routes that conform to the specified autonomous system (AS) path access list number.
quote-regexp <i>regexp</i>	(Optional) Filters output based on the specified quoted expression.
regexp <i>regexp</i>	(Optional) Filters output based on the specified regular expression.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Examples

The following is output from the **show bgp mvpn** command for the VRF named blue:

```
Device# show bgp ipv4 mvpn vrf blue route-type 7 111.111.111.111:11111 55 202.100.0.6
232.1.1.1

BGP routing table entry for [7][111.111.111.111:11111][55][202.100.0.6/32][232.1.1.1/32]/22,
version 17
Paths: (1 available, no best path)
Flag: 0x820
    Not advertised to any peer
    Refresh Epoch 1
    Local, (suppressed due to dampening)
        0.0.0.0 from 0.0.0.0 (205.3.0.3)
        Origin incomplete, localpref 100, weight 32768, valid, sourced, local
        Extended Community: RT:205.1.0.1:1
        Dampinfo: penalty 3472, flapped 4 times in 00:04:42, reuse in 00:00:23
        rx pathid: 0, tx pathid: 0
```

The table below describes the significant fields shown in the display.

Table 17: show bgp mvpn Field Descriptions

Field	Description
localpref	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
weight	Weight of the route as set via autonomous system filters.
Dampinfo	Penalty and reuse information if the path is dampened.
penalty	Current penalty for the path.
flapped	Number of times the path has flapped and the time since the first flap.
reuse in	Time until the path is re-used (undampened).
rx pathid	ID of path received from neighbor.
tx pathid	ID of path announcing to neighbors.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.

show bgp nsap

To display entries in the Border Gateway Protocol (BGP) routing table for the network service access point (NSAP) address family, use the **show bgp nsap** command in EXEC mode.

show bgp nsap [*nsap-prefix*]

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast [*nsap-prefix*]

Syntax Description

unicast	Specifies NSAP unicast address prefixes.
<i>nsap-prefix</i>	(Optional) NSAP prefix number, entered to display a particular network in the BGP routing table for the NSAP address family. This argument may be any length up to 20 octets.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The unicast keyword was added and this command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **show bgp nsap** command provides output similar to the **show ip bgp** command, except that it is specific to the NSAP address family.

Examples

The following is sample output from the **show bgp nsap** command:

```
Router# show bgp nsap
BGP table version is 6, local router ID is 10.1.57.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
*> 49.0101        49.0101.1111.1111.1111.00
                                     0 65101 i
* i49.0202.2222   49.0202.3333.3333.3333.00
```

```

          100      0 ?
*>          49.0202.2222.2222.2222.2222.00
          32768 ?
* i49.0202.3333      49.0202.3333.3333.3333.3333.00
          100      0 ?
*>          49.0202.2222.2222.2222.2222.00
          32768 ?
*> 49.0303      49.0303.4444.4444.4444.4444.00
          0 65303 i
* 49.0404      49.0303.4444.4444.4444.4444.00
          0 65303 65404 i
*>i          49.0404.9999.9999.9999.9999.00
          100      0 65404 i

```

The table below describes the significant fields shown in the display.

Table 18: show bgp nsap Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s--The table entry is suppressed. d--The table entry is dampened. h--The table entry is history. *--The table entry is valid. >--The table entry is the best entry to use for that network. i--The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i--Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e--Entry originated from an Exterior Gateway Protocol (EGP). ?--Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	NSAP prefix address of a network entity.

Field	Description
Next Hop	CLNS network entity title (NET) consisting of area address and system ID of the next system that is used when forwarding a packet to the destination network. This entry may cause a line break with the values of the following fields being displayed on the next line under their respective titles.
Metric	If shown, the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show bgp nsap** command, showing information for NSAP prefix 49.6005.1234.4567:

```
Router# show bgp nsap 49.6005.1234.4567
BGP routing table entry for 49.6005.1234.4567, version 2
Paths: (1 available, best #1)
  Not advertised to any peer
    Local
      49.6005.1234.4567.5678.1111.2222.3333.00 from 0.0.0.0 (10.1.1.1)
        Origin IGP, localpref 100, weight 32768, valid, sourced, local, best
```



Note

If a prefix has not been advertised to any peer, the display shows “Not advertised to any peer.”

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Rou
ter# show bgp nsap unicast
```

show bgp nsap community

To display routes that belong to specified network service access point (NSAP) Border Gateway Protocol (BGP) communities, use the **show bgp nsap community** command in EXEC mode.

show bgp nsap community [*community-number*] [**exact-match** | **local-as** | **no-advertise** | **no-export**]

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast community [*community-number*] [**exact-match** | **local-as** | **no-advertise** | **no-export**]

Syntax Description

<i>community-number</i>	(Optional) Valid value is a community number in the range from 1 to 4294967295 or AA:NN (autonomous system-community number/2-byte number).
exact-match	(Optional) Displays only routes that have an exact match.
local-as	(Optional) Displays only routes that are not sent outside of the local autonomous system (well-known community).
no-advertise	(Optional) Displays only routes that are not advertised to any peer (well-known community).
no-export	(Optional) Displays only routes that are not exported outside of the local autonomous system (well-known community).
unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The unicast keyword was added and this command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **show bgp nsap community** command provides output similar to the **show ip bgp community** command, except that it is specific to the NSAP address family.

Communities are set with the **route-map** and **set community** commands. Communities are sent using the **neighbor send-community** and **neighbor route-map out** commands. You must enter the numerical communities before the well-known communities. For example, the following string does not work:

```
Router> show bgp nsap community local-as 111:12345
Use the following string instead:
```

```
Router> show bgp nsap community 111:12345 local-as
```

Examples

The following is sample output from the **show bgp nsap community** command:

```
Rou
ter# show bgp nsap community no-export
BGP table version is 5, local router ID is 10.1.57.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*> 49.0101.11       49.0101.2222.2222.2222.00
                                     0 101 i
```

The table below describes the significant fields shown in the display.

Table 19: show bgp nsap community Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s--The table entry is suppressed. d--The table entry is dampened. h--The table entry is history. *--The table entry is valid. >--The table entry is the best entry to use for that network. i--The table entry was learned via an internal BGP (iBGP) session.

Field	Description
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i--Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e--Entry originated from an Exterior Gateway Protocol (EGP). ?--Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	NSAP prefix address of a network entity.
Next Hop	CLNS network entity title (NET) consisting of area address and system ID of the next system that is used when forwarding a packet to the destination network. This entry may cause a line break with the values of the following fields being displayed on the next line under their respective titles.
Metric	If shown, the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast community no-export
```

Related Commands

Command	Description
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another.
set community	Sets the BGP communities attribute.

Command	Description
show bgp nsap community-list	Displays BGP community list information for the NSAP address family.

show bgp nsap community-list

To display routes that are permitted by the Border Gateway Protocol (BGP) community list for network service access point (NSAP) prefixes, use the **show bgp nsap community-list** command in EXEC mode.

show bgp nsap community-list *community-list-number* [**exact-match**]

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast community-list *community-list-number* [**exact-match**]

Syntax Description

<i>community-list-number</i>	Community list number in the range from 1 to 199.
exact-match	(Optional) Displays only routes that have an exact match.
unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The unicast keyword was added and this command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **show bgp nsap community-list** command provides output similar to the **show ip bgp community-list** command, except that it is specific to the NSAP address family.

Examples

The following is sample output of the **show bgp nsap community-list** command:

```
Router# show bgp nsap community-list 1
BGP table version is 6, local router ID is 10.0.22.33
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network        Next Hop           Metric LocPrf Weight Path
*> 49.0a0a.bb       49.0a0a.bbbb.bbbb.bbbb.bbbb.00
                                         0 606
```

The table below describes the significant fields shown in the display.

Table 20: show bgp nsap community-list Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s--The table entry is suppressed. d--The table entry is dampened. h--The table entry is history. *--The table entry is valid. >--The table entry is the best entry to use for that network. i--The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i--Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e--Entry originated from an Exterior Gateway Protocol (EGP). ?--Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	NSAP prefix address of a network entity.
Next Hop	CLNS network entity title (NET) consisting of area address and system ID of the next system that is used when forwarding a packet to the destination network. This entry may cause a line break with the values of the following fields being displayed on the next line under their respective titles.
Metric	If shown, the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.

Field	Description
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast community-list 1
```

show bgp nsap dampened-paths

Effective with Cisco IOS Release 12.2(33)SRB, the **show bgp nsap dampened-paths** command is replaced by the **show bgp nsap dampening** command. See the **show bgp nsap dampening** command for more information.

To display network service access point (NSAP) address family Border Gateway Protocol (BGP) dampened routes in the BGP routing table, use the **show bgp nsap dampened-paths** command in EXEC mode.

show bgp nsap dampened-paths

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	This command was replaced by the show bgp nsap dampening command in Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

In Cisco IOS Release 12.2(33)SRB and later releases, the **show bgp nsap dampened-paths** command is replaced by the **show bgp nsap dampening** command. A keyword, **dampened-paths**, can be used with the new **show bgp nsap dampened-paths** command to display NSAP address family BGP dampened routes.

Examples

The following is sample output from the **show bgp nsap dampened-paths** command in privileged EXEC mode:

```
Router# show bgp nsap dampened-paths
BGP table version is 20, local router ID is 10.1.57.13
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          From      Reuse    Path
*d 49.0404         10.2.4.2    00:25:50 65202 65404 i
The table below describes the significant fields shown in the display.
```

Table 21: show bgp nsap dampened-paths Field Descriptions

Field	Description
BGP table version	Internal version number for the table. This number is incremented whenever the table changes.
local router ID	IP address of the router where route dampening is enabled.
*d	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear bgp nsap dampening	Clears BGP NSAP prefix route dampening information and unsuppresses the suppressed routes.

show bgp nsap dampening

To display network service access point (NSAP) address family Border Gateway Protocol (BGP) dampened routes in the BGP routing table, use the **show bgp nsap dampening** command in user EXEC or privileged EXEC mode.

show bgp nsap unicast dampening {**dampened-paths**|**flap-statistics** [**regex** *regex*|**quote-regex** *regex*|**filter-list** *access-list-number*| *nsap-prefix*]} **parameters**}

Syntax Description

unicast	Specifies NSAP unicast address prefixes.
dampened-paths	Displays paths suppressed due to dampening.
flap-statistics	Displays flap statistics of routes.
regex <i>regex</i>	(Optional) Displays flap statistics for all the paths that match the regular expression.
quote-regex <i>regex</i>	(Optional) Displays flap statistics for all the paths that match the regular expression as a quoted string of characters.
filter-list <i>access-list-number</i>	(Optional) Displays flap statistics for all the paths that pass the access list.
<i>nsap-prefix</i>	(Optional) Displays flap statistics for a single entry at this NSAP network number.
parameters	Displays details of configured dampening parameters.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the **show bgp nsap dampened-paths** command in privileged EXEC mode:

```
Router# show bgp nsap unicast dampening dampened-paths
```

```

BGP table version is 20, local router ID is 10.1.57.13
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          From          Reuse      Path
*d 49.0404            10.2.4.2          00:25:50 65202 65404 i

```

The table below describes the significant fields shown in the display.

Table 22: show bgp nsap unicast dampening dampened-paths Field Descriptions

Field	Description
BGP table version	Internal version number for the table. This number is incremented whenever the table changes.
local router ID	IP address of the router where route dampening is enabled.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s--The table entry is suppressed. d--The table entry is dampened. h--The table entry is history. *--The table entry is valid. >--The table entry is the best entry to use for that network. i--The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i--Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e--Entry originated from an Exterior Gateway Protocol (EGP). ?--Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

The following is sample output from the **show bgp nsap unicast dampening flap-statistics** command:

```
Router# show bgp nsap unicast dampening flap-statistics
BGP table version is 20, local router ID is 10.1.57.13
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          From          Flaps Duration Reuse      Path
*d 49.0404            10.2.4.2            3    00:09:45 00:23:40 65202 65404
```

The table below describes the significant fields shown in the display.

Table 23: show bgp nsap unicast dampening flap-statistics Field Descriptions

Field	Description
BGP table version	Internal version number for the table. This number is incremented whenever the table changes.
local router ID	IP address of the router where route dampening is enabled.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s--The table entry is suppressed. d--The table entry is dampened. h--The table entry is history. *--The table entry is valid. >--The table entry is the best entry to use for that network. i--The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i--Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e--Entry originated from an Exterior Gateway Protocol (EGP). ?--Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.

Field	Description
Flaps	Number of times the route has flapped.
Duration	Time (in hours:minutes:seconds) since the router noticed the first flap.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear bgp nsap dampening	Clears BGP NSAP prefix route dampening information and unsuppresses the suppressed routes.

show bgp nsap filter-list

To display routes in the Border Gateway Protocol (BGP) routing table for the network service access point (NSAP) address family that conform to a specified filter list, use the **show bgp nsap filter-list** command in privileged EXEC mode.

show bgp nsap filter-list *access-list-number*

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast filter-list *access-list-number*

Syntax Description

<i>access-list-number</i>	Number of an autonomous system path access list. It can be a number from 1 to 199.
unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The unicast keyword was added and this command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Examples

The following is sample output from the **show bgp nsap filter-list** command:

```
Router# show bgp nsap filter-list 1

BGP table version is 3, local router ID is 10.0.11.33
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*> 49.0b0b          49.0b0b.bbbb.bbbb.bbbb.bbbb.00
                                         0 707 i
```

The table below describes the significant fields shown in the display.

Table 24: show bgp nsap filter-list Field Descriptions

Field	Description
BGP table version	Internal version number for the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s--The table entry is suppressed. d--The table entry is dampened. h--The table entry is history. *--The table entry is valid. >--The table entry is the best entry to use for that network. i--The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i--Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e--Entry originated from an Exterior Gateway Protocol (EGP). ?--Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	NSAP prefix address of a network entity.
Next Hop	CLNS network entity title (NET) consisting of area address and system ID of the next system that is used when forwarding a packet to the destination network. This entry may cause a line break with the values of the following fields being displayed on the next line under their respective titles.
Metric	If shown, the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.

Field	Description
Weight	Set through the use of autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast filter-list 1
```

show bgp nsap flap-statistics

To display Border Gateway Protocol (BGP) flap statistics for network service access point (NSAP) prefixes, use the **show bgp nsap flap-statistics** command in EXEC mode.

show bgp nsap flap-statistics [**regex** *regex*|**quote-regex** *regex*|**filter-list** *access-list-number*|*nsap-prefix*]

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast flap-statistics [**regex** *regex*|**quote-regex** *regex*|**filter-list** *access-list-number*|*nsap-prefix*]

Syntax Description

regex <i>regex</i>	(Optional) Displays flap statistics for all the paths that match the regular expression.
quote-regex <i>regex</i>	(Optional) Displays flap statistics for all the paths that match the regular expression as a quoted string of characters.
filter-list <i>access-list-number</i>	(Optional) Displays flap statistics for all the paths that pass the access list.
<i>nsap-prefix</i>	(Optional) Displays flap statistics for a single entry at this NSAP network number.
unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The unicast keyword was added and this command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **show bgp nsap flap-statistics** command provides output similar to the **show ip bgp flap-statistics** command, except that it is specific to the NSAP address family.

If no arguments or keywords are specified, the router displays flap statistics for all NSAP prefix routes.

Examples

The following is sample output from the **show bgp nsap flap-statistics** command without arguments or keywords:

```
Router# show bgp nsap flap-statistics
BGP table version is 20, local router ID is 10.1.57.13
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          From          Flaps Duration Reuse      Path
*d 49.0404          10.2.4.2           3    00:09:45 00:23:40 65202 65404
```

The table below describes the significant fields shown in the display.

Table 25: show bgp nsap flap-statistics Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s--The table entry is suppressed. d--The table entry is damped. h--The table entry is history. *--The table entry is valid. >--The table entry is the best entry to use for that network. i--The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i--Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e--Entry originated from an Exterior Gateway Protocol (EGP). ?--Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.

Field	Description
Flaps	Number of times the route has flapped.
Duration	Time (in hours:minutes:seconds) since the router noticed the first flap.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	AS-path of the route that is being dampened.

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast flap-statistics
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear bgp nsap flap-statistics	Clears BGP flap statistics for NSAP prefix routes.

show bgp nsap inconsistent-as

To display Border Gateway Protocol (BGP) network service access point (NSAP) prefix routes with inconsistent originating autonomous systems, use the **show bgp nsap inconsistent-as** command in EXEC mode.

show bgp nsap inconsistent-as

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast inconsistent-as

Syntax Description

unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The unicast keyword was added and this command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **show bgp nsap inconsistent-as** command provides output similar to the **show ip bgp inconsistent-as** command, except that it is specific to the NSAP address family.

Use the **show bgp nsap inconsistent-as** command to discover any BGP routing table entries that contain inconsistent autonomous system path information. Inconsistent autonomous path information is useful for troubleshooting networks because it highlights a configuration error in the network.

Examples

The following is sample output from the **show bgp nsap inconsistent-as** command. In this example, the network prefix of 49.0a0a has two entries in the BGP routing table showing different originating paths. The originating path information should be the same in both entries.

```
Router# show bgp nsap inconsistent-as
BGP table version is 3, local router ID is 10.1.57.17
Status codes: s suppressed, d damped, h history, * valid, > best, i -internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
*  49.0a0a        49.0a0a.cccc.cccc.cccc.00
                                     0 30 i
```

```
*>                               49.0a0a.aaaa.aaaa.aaaa.00
                                0 10 i
```

The table below describes the significant fields shown in the display.

Table 26: show bgp nsap inconsistent-as Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s--The table entry is suppressed. d--The table entry is dampened. h--The table entry is history. *--The table entry is valid. >--The table entry is the best entry to use for that network. i--The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i--Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e--Entry originated from an Exterior Gateway Protocol (EGP). ?--Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	NSAP prefix address of a network entity.
Next Hop	CLNS network entity title (NET) consisting of area address and system ID of the next system that is used when forwarding a packet to the destination network. This entry may cause a line break with the values of the following fields being displayed on the next line under their respective titles.
Metric	If shown, the value of the interautonomous system metric. This field is frequently not used.

Field	Description
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast inconsistent-as
```

show bgp nsap neighbors

To display information about Border Gateway Protocol (BGP) network service access point (NSAP) prefix connections to neighbors, use the **show bgp nsap neighbors** command in EXEC mode.

show bgp nsap neighbors [*ip-address* [**routes**| **flap-statistics**| **advertised-routes**| **paths** *regex*| **dampened-routes**]]

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast neighbors [*ip-address* [**routes**| **flap-statistics**| **advertised-routes**| **paths** *regex*| **dampened-routes**]]

Syntax Description

<i>ip-address</i>	(Optional) IP address of the BGP-speaking neighbor. If you omit this argument, all neighbors are displayed.
routes	(Optional) Displays all routes received and accepted.
flap-statistics	(Optional) Displays flap statistics for the routes learned from the neighbor.
advertised-routes	(Optional) Displays all the routes the networking device advertised to the neighbor.
paths <i>regex</i>	(Optional) Regular expression used to match the paths received.
dampened-routes	(Optional) Displays the dampened routes to the neighbor at the NSAP prefix address specified.
unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The unicast keyword was added and this command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **show bgp nsap neighbors** command provides output similar to the **show ip bgp neighbors** command, except that it is specific to the NSAP address family.

Examples

The following is sample output from the **show bgp nsap neighbors** command:

```
Router# show bgp nsap neighbors 10.0.2.3
BGP neighbor is 10.0.2.3, remote AS 64500, external link
  BGP version 4, remote router ID 172.17.1.2
  BGP state = Established, up for 00:12:50
  Last read 00:00:50, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family NSAP Unicast: advertised and received
  Received 17 messages, 0 notifications, 0 in queue
  Sent 17 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Default minimum time between advertisement runs is 30 seconds
For address family: NSAP Unicast
  BGP table version 5, neighbor version 5
  Index 2, Offset 0, Mask 0x4
  2 accepted prefixes consume 114 bytes
  Prefix advertised 2, suppressed 0, withdrawn 0
  Number of NLRI in the update sent: max 1, min 0
  Connections established 1; dropped 0
  Last reset never
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 10.0.2.2, Local port: 11000
Foreign host: 10.0.2.3, Foreign port: 179
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x115940):
Timer           Starts      Wakeups      Next
Retrans         22          1            0x0
TimeWait        0           0            0x0
AckHold         19          7            0x0
SendWnd         0           0            0x0
KeepAlive       0           0            0x0
GiveUp          0           0            0x0
PmtuAger        0           0            0x0
DeadWait        0           0            0x0
iss: 2052706884  snduna: 2052707371  sndnxt: 2052707371  sndwnd: 15898
irs: 1625021348  rcvnxt: 1625021835  rcvwnd: 15898  delrcvwnd: 486
SRTT: 279 ms, RTTO: 446 ms, RTV: 167 ms, KRTT: 0 ms
minRTT: 0 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle
```

Datagrams (max data segment is 1460 bytes):
 Rcvd: 30 (out of order: 0), with data: 19, total data bytes: 486
 Sent: 29 (retransmit: 1, fastretransmit: 0), with data: 20, total data bytes: 46
 The table below describes the significant fields shown in the display.

Table 27: show bgp nsap neighbors Field Descriptions

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number.
remote AS	Autonomous system of the neighbor.

Field	Description
link	If the neighbor is in the same autonomous system as the router, then the link between them is internal; otherwise, it is considered external.
BGP version	BGP version being used to communicate with the remote router; the router ID (an IP address) of the neighbor is also specified.
remote router ID	A 32-bit number written as 4 octets separated by periods (dotted decimal format).
BGP state	Internal state of this BGP connection.
up for	Amount of time (in hours:minutes:seconds) that the underlying TCP connection has been in existence.
Last read	Time (in hours:minutes:seconds) that BGP last read a message from this neighbor.
hold time	Maximum amount of time, in seconds, that can elapse between messages from the peer.
keepalive interval	Time period, in seconds, between sending keepalive packets, which help ensure that the TCP connection is up.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor.
Route refresh	Indicates that the neighbor supports dynamic soft reset using the route refresh capability.
Address family NSAP Unicast	NSAP unicast-specific properties of this neighbor.
Received	Number of total BGP messages received from this peer, including keepalives.
notifications	Number of error messages received from the peer.
Sent	Total number of BGP messages that have been sent to this peer, including keepalives.
notifications	Number of error messages the router has sent to this peer.
Route refresh request	Number of route refresh requests sent and received from this neighbor.
advertisement runs	Value of minimum advertisement interval.

Field	Description
For address family	Address family to which the following fields refer.
BGP table version	Indicates that the neighbor has been updated with this version of the primary BGP routing table.
neighbor version	Number used by the software to track the prefixes that have been sent and those that must be sent to this neighbor.
Community attribute (not shown in sample output)	Appears if the neighbor send-community command is configured for this neighbor.
Inbound path policy (not shown in sample output)	Indicates that an inbound filter list or route map is configured.
Outbound path policy (not shown in sample output)	Indicates that an outbound filter list, route map, or unsuppress map is configured.
bgp-in (not shown in sample output)	Name of the inbound update prefix filter list for the NSAP unicast address family.
aggregate (not shown in sample output)	Name of the outbound update prefix filter list for the NSAP unicast address family.
uni-out (not shown in sample output)	Name of the outbound route map for the NSAP unicast address family.
accepted prefixes	Number of prefixes accepted.
Prefix advertised	Number of prefixes advertised.
suppressed	Number of prefixes suppressed.
withdrawn	Number of prefixes withdrawn.
history paths (not shown in sample output)	Number of path entries held to remember history.
Connections established	Number of times the router has established a TCP connection and the two peers have agreed to speak BGP with each other.
dropped	Number of times that a good connection has failed or been taken down.
Last reset	Elapsed time since this peering session was last reset.
Connection state	State of the BGP peer.
unread input bytes	Number of bytes of packets still to be processed.

Field	Description
Local host, Local port	Peering address of local router, plus port.
Foreign host, Foreign port	Peering address of the neighbor.
Event Timers	Table that displays the number of starts and wakeups for each timer.
iss	Initial send sequence number.
snduna	Last send sequence number the local host sent but for which it has not received an acknowledgment.
sndnxt	Sequence number the local host will send next.
sndwnd	TCP window size of the remote host.
irs	Initial receive sequence number.
rcvnxt	Last receive sequence number the local host has acknowledged.
rcvwnd	TCP window size of the local host.
delrcvwnd	Delayed receive window--data the local host has read from the connection but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT	A calculated smoothed round-trip timeout.
RTTO	Round-trip timeout.
RTV	Variance of the round-trip time.
KRTT	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.
minRTT	Smallest recorded round-trip timeout (hard wire value used for calculation).
maxRTT	Largest recorded round-trip timeout.
ACK hold	Time (in milliseconds) the local host will delay an acknowledgment in order to "piggyback" data on it.
Flags	IP precedence of the BGP packets.

Field	Description
Datagrams: Rcvd	Number of update packets received from neighbor.
with data	Number of update packets received with data.
total data bytes	Total bytes of data.
Sent	Number of update packets sent.
with data	Number of update packets with data sent.
total data bytes	Total number of data bytes.

The following is sample output from the **show bgp nsap neighbors** command with the **advertised-routes** keyword:

```
Router# show bgp nsap neighbors 10.0.2.3 advertised-routes
BGP table version is 5, local router ID is 172.17.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*> 49.0101          49.0101.1111.1111.1111.1111.00
                                     0 101 i
*> 49.0202          49.0202.2222.2222.2222.2222.00
                                     32768 i
```

The following is sample output from the **show bgp nsap neighbors** command with the **routes** keyword:

```
Router# show bgp nsap neighbors 10.0.2.3 routes
BGP table version is 5, local router ID is 172.17.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*> 49.0303          49.0303.3333.3333.3333.3333.00
                                     0 303 i
*> 49.0404          49.0303.3333.3333.3333.3333.00
                                     0 303 404 i

Total number of prefixes 2
```

The table below describes the significant fields shown in the display.

Table 28: show bgp nsap neighbors Field Descriptions with advertised-routes and routes keywords

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s--The table entry is suppressed. d--The table entry is dampened. h--The table entry is history. *--The table entry is valid. >--The table entry is the best entry to use for that network. i--The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i--Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e--Entry originated from an Exterior Gateway Protocol (EGP). ?--Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	NSAP prefix address of a network entity.
Next Hop	CLNS network entity title (NET) consisting of area address and system ID of the next system that is used when forwarding a packet to the destination network. This entry may cause a line break with the values of the following fields being displayed on the next line under their respective titles.
Metric	If shown, the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show bgp nsap neighbors** command with the **paths** keyword:

```
Router# show bgp nsap neighbors 10.0.3.3 paths ^101
Address      Refcount Metric Path
0x62281590      1          0 101 i
```



Note

The caret (^) symbol in the example is a regular expression that is entered by simultaneously pressing the Shift and 6 keys on your keyboard. A caret (^) symbol at the beginning of a regular expression matches the start of a line.

The table below describes the significant fields shown in the display.

Table 29: show bgp nsap neighbors paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Refcount	Number of routes using that path.
Metric	The Multiple Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The AS-path for that route, followed by the origin code for that route.

The following sample output from the **show bgp nsap neighbors** command shows the NSAP prefix dampened routes for the neighbor at 10.0.2.2:

```
Router# show bgp nsap neighbors 10.0.2.2 dampened-routes

BGP table version is 10, local router ID is 172.17.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          From          Reuse      Path
*d 49.0101          10.0.2.2          00:25:50 202 101 i
```

The following sample output from the **show bgp nsap neighbors** command shows the NSAP prefix flap statistics for the neighbor at 10.0.2.2:

```
Router# show bgp nsap neighbors 10.0.2.2 flap-statistics

BGP table version is 10, local router ID is 10.1.57.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          From          Flaps Duration Reuse      Path
*d 49.0101          10.0.2.2          3      00:07:00 00:24:50 202 101
```

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast neighbors 10.0.2.3
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a neighboring router.

show bgp nsap paths

To display all the Border Gateway Protocol (BGP) network service access point (NSAP) prefix paths in the database, use the **show bgp nsap paths** command in EXEC mode.

show bgp nsap paths [*AS-path-regexp*]

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast paths [*AS-path-regexp*]

Syntax Description

<i>AS-path-regexp</i>	(Optional) Regular expression that is used to match the received paths in the database.
unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The unicast keyword was added and this command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **show bgp nsap paths** command provides output similar to the **show ip bgp paths** command, except that it is specific to the NSAP address family.

Examples

The following is sample output from the **show bgp nsap paths** command without a specified regular expression:

```
Router# show bgp nsap paths
Address      Hash Refcount Metric Path
0x622803FC   0         1         0 i
0x62280364 1197         1         0 202 101 i
0x62280448 1739         1         0 202 i
0x622803B0 1941         1         0 404 i
```

The table below describes the significant fields shown in the display.

Table 30: show bgp nsap paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Hash	Hash bucket where the path is stored.
RefCount	Number of routes using that path.
Metric	The Multiple Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The AS-path for that route, followed by the origin code for that route.

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast paths
```

show bgp nsap quote-regexp

To display Border Gateway Protocol (BGP) network service access point (NSAP) prefix routes matching the AS-path regular expression as a quoted string of characters, use the **show bgp nsap quote-regexp** command in privileged EXEC mode.

show bgp nsap quote-regexp *as-path-regexp*

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast quote-regexp *as-path-regexp*

Syntax Description

<i>as-path-regexp</i>	Regular expression to match the BGP autonomous system paths. The regular expression is contained within quotes.
unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The unicast keyword was added and this command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **show bgp nsap quote-regexp** command provides output similar to the **show ip bgp quote-regexp** command, except that it is specific to the NSAP address family.

Examples

The following is sample output from the **show bgp nsap quote-regexp** command that shows paths equal to 202:

```
Router# show bgp nsap quote-regexp "202"
BGP table version is 10, local router ID is 10.1.57.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network                Next Hop              Metric LocPrf Weight Path
*d 49.0101                49.0202.2222.2222.2222.00
                                     0 202 101 i
```

```
*> 49.0202          49.0202.2222.2222.2222.2222.00          0 202 i
```

The table below describes the significant fields shown in the display.

Table 31: show bgp nsap quote-regexp Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s--The table entry is suppressed. d--The table entry is dampened. h--The table entry is history. *--The table entry is valid. >--The table entry is the best entry to use for that network. i--The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i--Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e--Entry originated from an Exterior Gateway Protocol (EGP). ?--Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	NSAP prefix of a network entity.
Next Hop	CLNS network entity title (NET) consisting of area address and system ID of the next system that is used when forwarding a packet to the destination network. This entry may cause a line break with the values of the following fields being displayed on the next line under their respective titles.
Metric	If shown, the value of the interautonomous system metric. This field is frequently not used.

Field	Description
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast quote-regexp "202"
```

Related Commands

Command	Description
show bgp nsap regexp	Displays NSAP prefix routes matching the AS-path regular expression.

show bgp nsap regexp

To display Border Gateway Protocol (BGP) network service access point (NSAP) prefix routes matching the AS-path regular expression, use the **show bgp nsap regexp** command in privileged EXEC mode.

show bgp nsap regexp *AS-path-regexp*

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast regexp *AS-path-regexp*

Syntax Description

<i>AS-path-regexp</i>	Regular expression to match the BGP autonomous system paths.
unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The unicast keyword was added and this command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **show bgp nsap regexp** command provides output similar to the **show ip bgp regexp** command, except that it is specific to the NSAP address family.

Examples

The following is sample output from the **show bgp nsap regexp** command that shows paths beginning with 202 or containing 101:

```
Router# show bgp nsap regexp ^202 101
BGP table version is 10, local router ID is 10.1.57.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network                Next Hop                Metric LocPrf Weight Path
*d 49.0101                  49.0202.2222.2222.2222.00
                                     0 202 101 i
```


**Note**

The caret (^) symbol in the example is a regular expression that is entered by simultaneously pressing the Shift and 6 keys on your keyboard. A caret (^) symbol at the beginning of a regular expression matches the start of a line.

The table below describes the significant fields shown in the display.

Table 32: show bgp nsap regexp Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s--The table entry is suppressed. d--The table entry is dampened. h--The table entry is history. *--The table entry is valid. >--The table entry is the best entry to use for that network. i--The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i--Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e--Entry originated from an Exterior Gateway Protocol (EGP). ?--Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	NSAP prefix address of a network entity.
Next Hop	CLNS network entity title (NET) consisting of area address and system ID of the next system that is used when forwarding a packet to the destination network. This entry may cause a line break with the values of the following fields being displayed on the next line under their respective titles.

Field	Description
Metric	If shown, the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast regexp ^202 101
```

Related Commands

Command	Description
show bgp nsap quote-regexp	Displays BGP NSAP prefix routes matching the AS-path regular expression.

show bgp nsap summary

To display the status of all Border Gateway Protocol (BGP) network service access point (NSAP) prefix connections, use the **show bgp nsap summary** command in EXEC mode.

show bgp nsap summary

Syntax in Cisco IOS Release 12.2(33)SRB

show bgp nsap unicast summary

Syntax Description

unicast	Specifies NSAP unicast address prefixes.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRB	The unicast keyword was added and this command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **show bgp nsap summary** command provides output similar to the **show ip bgp summary** command, except that it is specific to the NSAP address family.

Examples

The following is sample output from the **show bgp nsap summary** command:

```
Router# show bgp nsap summary
BGP router identifier 10.2.4.2, local AS number 65202
BGP table version is 26, main routing table version 26
5 network entries and 8 paths using 1141 bytes of memory
6 BGP path attribute entries using 360 bytes of memory
4 BGP AS-PATH entries using 96 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Dampening enabled. 0 history paths, 0 dampened paths
BGP activity 16/261 prefixes, 34/26 paths, scan interval 60 secs
Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ  OutQ Up/Down  State/PfxRcd
10.1.2.1      4  65101   1162   1162     26    0    0 18:17:07      1
10.2.3.3      4  65202   1183   1188     26    0    0 18:23:28      3
10.2.4.4      4  65303   1163   1187     26    0    0 18:23:14      2
```

The table below describes the significant fields shown in the display.

Table 33: show bgp nsap summary Field Descriptions

Field	Description
BGP router identifier	IP address of the networking device.
local AS number	Number of the local autonomous system.
BGP table version	Internal version number of the BGP database.
main routing table version	Last version of the BGP database that was injected into the main routing table.
network entries	Number of network entries and paths in the main routing table including the associated memory usage.
BGP path attribute entries	Number of BGP path attribute entries in the main routing table including the associated memory usage.
BGP route-map cache entries	Number of BGP route map cache entries in the main routing table including the associated memory usage.
BGP filter-list cache entries	Number of BGP filter list cache entries in the main routing table including the associated memory usage.
Dampening	Indicates whether route dampening is enabled, the number of history paths, and number of dampened paths.
BGP activity	Displays the number of BGP prefixes and paths, followed by the BGP scan interval in seconds.
Neighbor	IP address of a neighbor.
V	BGP version number communicated to that neighbor.
AS	Autonomous system.
MsgRcvd	BGP messages received from that neighbor.
MsgSent	BGP messages sent to that neighbor.
TblVer	Last version of the BGP database that was sent to that neighbor.
InQ	Number of messages from that neighbor waiting to be processed.
OutQ	Number of messages waiting to be sent to that neighbor.

Field	Description
Up/Down	The length of time that the BGP session has been in state Established, or the current state if it is not Established.
State/PfxRcd	Current state of the BGP session/the number of prefixes the router has received from a neighbor or peer group. When the maximum number (as set by the neighbor maximum-prefix command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the neighbor shutdown command.

In this example for Cisco IOS Release 12.2(33)SRB there is a new keyword, **unicast**, that is required. The output for the following command is the same as in the first example.

```
Router# show bgp nsap unicast summary
```

Related Commands

Command	Description
clear bgp nsap	Resets an NSAP BGP TCP connection.
neighbor maximum-prefix	Controls how many prefixes can be received from a neighbor.
neighbor shutdown	Disables a neighbor or peer group.

show bgp vpnv6 multicast

To display Virtual Private Network Version 6 (VPNv6) multicast entries in a Border Gateway Protocol (BGP) table, use the **show bgp vpnv6 multicast** command in user EXEC or privileged EXEC mode.

show bgp vpnv6 multicast {**all** | **vrf** *vrf-name* | **rd** *route-distinguisher*}

Syntax Description

all	(Optional) Displays all entries in a BGP table.
vrf <i>vrf-name</i>	(Optional) Specifies VPN routing and forwarding (VRF) instance tables or a specific VRF table for IPv4 or IPv6 address that match the specified VRF table.
rd <i>route-distinguisher</i>	(Optional) Displays routes that match the specified route distinguisher (RD).

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.
15.2(4)S	This command was introduced.

Usage Guidelines

BGP is used for distributing VPN IPv6 routing information in the VPN backbone. The local routes placed in the BGP routing table on an egress provider edge (PE) router are distributed to other PE routers.

Examples

Router# **show bgp vpnv6 multicast all**

```

Network                Next Hop                Metric LocPrf   Weight Path
Route Distinguisher: 100:1
* 2001:0DB8:0:CD30::/56 2001:0DB8:0:CD30::72a    0           0      200 ?
*                          ::                0           32768 ?
* i2001:100:1:2000::/56  ::FFFF:200.10.10.1
Route Distinguisher: 200:1
* 2001:0DB8:2:CD30::/56  ::                0           32768 ?
* 2001:0DB8:2:CD30::/56  ::FFFF:200.10.10.1    0           32768 ?

```

The table below describes the significant fields shown in the displays.

Table 34: show bgp vpnv6 multicast Field Descriptions

Field	Description
Network	IPv6 address of the network that the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
Loc Prf	Local preference value as configured with the set local-preference command.
Weight	Weight of the route as set through autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path. It can be one of the following values: • i—The entry was originated with the IGP and advertised with a network router configuration command. • e—The route originated with the EGP. • ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.
Route Distinguisher	Specifies the VRF instance.

Related Commands

Command	Description
show bgp vpnv6 unicast	Displays VPNv6 unicast entries in a BGP table.

show bgp vpnv6 unicast

To display Virtual Private Network Version 6 (VPNv6) unicast entries in a Border Gateway Protocol (BGP) table, use the **show bgp vpnv6 unicast** command in user EXEC or privileged EXEC mode.

show bgp vpnv6 unicast [**all**| **vrf** [*vrf-name*]]

Syntax Description

all	(Optional) Displays all entries in a BGP table.
vrf	(Optional) Specifies all VPN routing and forwarding (VRF) instance tables or a specific VRF table for IPv4 or IPv6 address.
<i>vrf-name</i>	(Optional) Names a specific VRF table for an IPv4 or IPv6 address.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.2(2)SNI	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

BGP is used for distributing VPN IPv6 routing information in the VPN backbone. The local routes placed in the BGP routing table on an egress provider edge (PE) router are distributed to other PE routers.

Examples

The following examples shows BGP entries from all of the customer-specific IPv6 routing tables:

```
Router# show bgp vpnv6 unicast all
```

```

Network                Next Hop                Metric LocPrf  Weight Path
Route Distinguisher: 100:1
* 2001:100:1:1000::/56  2001:100:1:1000::72a    0           0      200 ?
*                      ::                    0           32768 ?
* i2001:100:1:2000::/56  ::FFFF:200.10.10.1
Route Distinguisher: 200:1
* 2001:100:2:1000::/56  ::                      0           32768 ?
```



```
* 2001:100:2:2000::/56      ::FFFF:200.10.10.1      0      32768 ?
```

The table below describes the significant fields shown in the displays.

Table 35: show bgp vpnv6 unicast Field Descriptions

Field	Description
Network	IPv6 address of the network the entry describes.
Next Hop	IPv6 address of the next system that is used when forwarding a packet to the destination network. An entry of two colons (::) indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
Loc Prf	Local preference value as configured with the set local-preference command.
Weight	Weight of the route as set through autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path. It can be one of the following values: • i—The entry was originated with the IGP and advertised with a network router configuration command. • e—The route originated with EGP. • ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.
Route Distinguisher	Specifies the VRF instance.

Related Commands

Command	Description
show bgp vpnv6 multicast	Displays VPNv6 multicast entries in a BGP table.

 **show bgp vpnv6 unicast**



BGP Commands: show ip through Z

- [show ip as-path-access-list, page 698](#)
- [show ip bgp, page 700](#)
- [show ip bgp bmp, page 713](#)
- [show ip bgp all dampening, page 716](#)
- [show ip bgp cidr-only, page 719](#)
- [show ip bgp cluster-ids, page 722](#)
- [show ip bgp community, page 725](#)
- [show ip bgp community-list, page 729](#)
- [show ip bgp dampened-paths, page 732](#)
- [show ip bgp dampening dampened-paths, page 734](#)
- [show ip bgp dampening flap-statistics, page 736](#)
- [show ip bgp dampening parameters, page 740](#)
- [show ip bgp extcommunity-list, page 742](#)
- [show ip bgp filter-list, page 744](#)
- [show ip bgp flap-statistics, page 747](#)
- [show ip bgp inconsistent-as, page 749](#)
- [show ip bgp injected-paths, page 750](#)
- [show ip bgp ipv4, page 753](#)
- [show ip bgp ipv4 multicast, page 757](#)
- [show ip bgp ipv4 multicast summary, page 760](#)
- [show ip bgp ipv6 multicast, page 762](#)
- [show ip bgp ipv6 unicast, page 763](#)
- [show ip bgp l2vpn, page 766](#)
- [show ip bgp neighbors, page 773](#)

- [show ip bgp path-attribute discard, page 794](#)
- [show ip bgp path-attribute unknown, page 796](#)
- [show ip bgp paths, page 797](#)
- [show ip bgp peer-group, page 799](#)
- [show ip bgp quote-regexp, page 801](#)
- [show ip bgp regexp, page 805](#)
- [show ip bgp replication, page 809](#)
- [show ip bgp rib-failure, page 811](#)
- [show ip bgp rpki servers, page 813](#)
- [show ip bgp rpki table, page 815](#)
- [show ip bgp rtfiler, page 817](#)
- [show ip bgp summary, page 820](#)
- [show ip bgp template peer-policy, page 828](#)
- [show ip bgp template peer-session, page 831](#)
- [show ip bgp unicast route-server, page 834](#)
- [show ip bgp update-group, page 837](#)
- [show ip bgp vpnv4, page 841](#)
- [show ip bgp vpnv4 all dampening, page 855](#)
- [show ip bgp vpnv4 all sso summary, page 857](#)
- [show ip bgp vpnv6 unicast all dampening, page 859](#)
- [show ip community-list, page 861](#)
- [show ip extcommunity-list, page 863](#)
- [show ip policy-list, page 867](#)
- [show ip prefix-list, page 868](#)
- [show ip route, page 870](#)
- [show ip route vrf, page 882](#)
- [show tcp ha connections, page 889](#)
- [slow-peer detection, page 891](#)
- [slow-peer split-update-group dynamic, page 893](#)
- [slow-peer split-update-group static, page 895](#)
- [sso, page 896](#)
- [stats-reporting-period \(bmp\), page 899](#)
- [synchronization, page 901](#)

- [table-map](#), page 903
- [template peer-policy](#), page 906
- [template peer-session](#), page 910
- [timers bgp](#), page 914
- [update-source \(bmp\)](#), page 916
- [ve](#), page 918

show ip as-path-access-list

To display the contents of all current autonomous system (AS) path access lists, use the **show ip as-path-access-list** command in user EXEC or privileged EXEC mode.

show ip as-path-access-list [*number*]

Syntax Description

<i>number</i>	(Optional) Specifies the AS path access list number. The range is from 1 to 500.

Command Default

If the *number* argument is not specified, command output is displayed for all AS path access lists.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
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.

Examples

The following is sample output from the **show ip as-path-access-list** command:

```
Router# show ip as-path-access-list
AS path access list 34
  deny RTR$
AS path access list 100
  permit 100$
```

The table below describes the fields shown in the display.

Table 36: show ip as-path-access-list Field Descriptions

Field	Description
AS path access list	Indicates the AS path access list number.

Field	Description
deny	Indicates the number of packets that are rejected since the regular expression failed to match the representation of the AS path of the route as an ASCII string.
permit	Indicates the number of packets that are forwarded since the regular expression matched the representation of the AS path of the route as an ASCII string.

Related Commands

Command	Description
ip as-path access-list	Configures an autonomous system path filter using a regular expression.

show ip bgp

To display entries in the Border Gateway Protocol (BGP) routing table, use the **show ip bgp** command in user EXEC or privileged EXEC mode.

show ip bgp [*ip-address* [*mask* [**longer-prefixes** [**injected**] | **shorter-prefixes** [*length*] | **bestpath** | **multipaths** | **subnets**] | **bestpath** | **multipaths**] | **all** | **oer-paths** | **prefix-list** *name* | **pending-prefixes** | **route-map** *name* | **version** {*version-number* | **recent** *offset-value*}]

Syntax Description

<i>ip-address</i>	(Optional) IP address entered to filter the output to display only a particular host or network in the BGP routing table.
<i>mask</i>	(Optional) Mask to filter or match hosts that are part of the specified network.
longer-prefixes	(Optional) Displays the specified route and all more-specific routes.
injected	(Optional) Displays more-specific prefixes injected into the BGP routing table.
shorter-prefixes	(Optional) Displays the specified route and all less-specific routes.
<i>length</i>	(Optional) The prefix length. The range is a number from 0 to 32.
bestpath	(Optional) Displays the best path for this prefix.
multipaths	(Optional) Displays multipaths for this prefix.
subnets	(Optional) Displays the subnet routes for the specified prefix.
all	(Optional) Displays all address family information in the BGP routing table.
oer-paths	(Optional) Displays Optimized Edge Routing (OER) controlled prefixes in the BGP routing table.
prefix-list <i>name</i>	(Optional) Filters the output based on the specified prefix list.
pending-prefixes	(Optional) Displays prefixes that are pending deletion from the BGP routing table.

route-map <i>name</i>	(Optional) Filters the output based on the specified route map.
version <i>version-number</i>	(Optional) Displays all prefixes with network versions greater than or equal to the specified version number. The range is from 1 to 4294967295.
recent <i>offset-value</i>	(Optional) Displays the offset from the current routing table version. The range is from 1 to 4294967295.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0	This command was modified. The display of prefix advertisement statistics was added.
12.0(6)T	This command was modified. The display of a message indicating support for route refresh capability was added.
12.0(14)ST	This command was modified. The prefix-list , route-map , and shorter-prefixes keywords were added.
12.2(2)T	This command was modified. The output was modified to display multipaths and the best path to the specified network.
12.0(21)ST	This command was modified. The output was modified to show the number of Multiprotocol Label Switching (MPLS) labels that arrive at and depart from a prefix.
12.0(22)S	This command was modified. A new status code indicating stale routes was added to support BGP graceful restart.
12.2(14)S	This command was modified. A message indicating support for BGP policy accounting was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.2(15)T	This command was modified. A new status code indicating stale routes was added to support BGP graceful restart.
12.3(2)T	This command was modified. The all keyword was added.

Release	Modification
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
12.3(8)T	This command was modified. The oer-paths keyword was added.
12.4(15)T	This command was modified. The pending-prefixes , bestpath , multipaths , and subnets keywords were added.
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.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(22)T	This command was modified. The version <i>version-number</i> and the recent <i>offset-value</i> keyword and argument pairs were added.
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.
Cisco IOS XE Release 2.3	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.
12.2(33)SX11	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format was changed to asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format was changed to asplain.
12.2(33)SRE	This command was modified. The command output was modified to show the backup path and the best external path information. Support for the best external route and backup path was added. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
15.2(1)S	This command was modified to display an Resource Public Key Infrastructure (RPKI) validation code per network, if one applies.
Cisco IOS XE Release 3.5S	This command was modified to display an RPKI validation code per network, if one applies.
15.1(1)SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
15.2(4)S	This command was modified. Output about discarded or unknown path attributes was added for the BGP Attribute Filter feature. Output about additional path selection was added for the BGP Additional Paths feature. Output about paths imported from a virtual routing and forwarding (VRF) table to the global table was added for the BGP Support for IP Prefix Export from a VRF table into the global table.
Cisco IOS XE Release 3.7S	This command was modified. Output about discarded or unknown path attributes was added for the BGP Attribute Filter feature. Output about additional path selection was added for the BGP Additional Paths feature. Output about paths imported from a VRF table to the global table was added for the BGP Support for IP Prefix Export from a VRF table into the global table.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

The **show ip bgp** command is used to display the contents of the BGP routing table. The output can be filtered to display entries for a specific prefix, prefix length, and prefixes injected through a prefix list, route map, or conditional advertisement.

When changes are made to the network address, the network version number is incremented. Use the **version** keyword to view a specific network version.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538, for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2, for example—as the only configuration format, regular expression match, and output display, with no asplain support.

oer-paths Keyword

In Cisco IOS Release 12.3(8)T and later releases, BGP prefixes that are monitored and controlled by OER are displayed by entering the **show ip bgp** command with the **oer-paths** keyword.

Examples

The following sample output displays the BGP routing table:

```
Device# show ip bgp

BGP table version is 6, local router ID is 10.0.96.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f
RT-Filter, a additional-path
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

      Network          Next Hop              Metric LocPrf Weight Path
-----
N*  10.0.0.1           10.0.0.3                  0           0 3 ?
N*>
Nr  10.0.0.0/8          10.0.0.3                  0           0 3 ?
Nr>
Nr> 10.0.0.0/24          10.0.0.3                  0           0 3 ?
V*> 10.0.2.0/24          0.0.0.0                   0          32768 i
Vr> 10.0.3.0/24          10.0.3.5                  0           0 4 ?
```

The table below describes the significant fields shown in the display.

Table 37: show ip bgp Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP (iBGP) session. • r—The table entry is a RIB-failure. • S—The table entry is stale. • m—The table entry has multipath to use for that network. • b—The table entry has a backup path to use for that network. • x—The table entry has a best external route to use for the network.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • a—Path is selected as an additional path. • i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. • e—Entry originated from an Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
RPKI validation codes	If shown, the RPKI validation state for the network prefix, which is downloaded from the RPKI server. The codes are shown only if the bgp rpki server or neighbor announce rpki state command is configured.

Field	Description
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.
(stale)	Indicates that the following path for the specified autonomous system is marked as “stale” during a graceful restart process.

The following sample output shows the BGP routing table with 4-byte autonomous system numbers, 65536 and 65550, shown under the Path field. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or a later release.

Device# **show ip bgp**

```

BGP table version is 4, local router ID is 172.16.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
*> 10.1.1.0/24     192.168.1.2             0         0 65536 i
*> 10.2.2.0/24     192.168.3.2             0         0 65550 i
*> 172.16.1.0/24   0.0.0.0                 0         32768 i

```

The following sample output displays information about the 192.168.1.0 entry in the BGP routing table:

Device# **show ip bgp 192.168.1.0**

```

BGP routing table entry for 192.168.1.0/24, version 22
Paths: (2 available, best #2, table default)
  Additional-path
  Advertised to update-groups:
    3
  10 10
    192.168.3.2 from 172.16.1.2 (10.2.2.2)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
  10 10
    192.168.1.2 from 192.168.1.2 (10.3.3.3)

```

Origin IGP, localpref 100, valid, external, best , recursive-via-connected

The following sample output displays information about the 10.3.3.3 255.255.255.255 entry in the BGP routing table:

```
Device# show ip bgp 10.3.3.3 255.255.255.255

BGP routing table entry for 10.3.3.3/32, version 35
Paths: (3 available, best #2, table default)
Multipath: eBGP
Flag: 0x860
  Advertised to update-groups:
    1
  200
    10.71.8.165 from 10.71.8.165 (192.168.0.102)
      Origin incomplete, localpref 100, valid, external, backup/repair
      Only allowed to recurse through connected route
  200
    10.71.11.165 from 10.71.11.165 (192.168.0.102)
      Origin incomplete, localpref 100, weight 100, valid, external, best
      Only allowed to recurse through connected route
  200
    10.71.10.165 from 10.71.10.165 (192.168.0.104)
      Origin incomplete, localpref 100, valid, external,
      Only allowed to recurse through connected route
```

The table below describes the significant fields shown in the display.

Table 38: show ip bgp ip-address Field Descriptions

Field	Description
BGP routing table entry for	IP address or network number of the routing table entry.
version	Internal version number of the table. This number is incremented whenever the table changes.
Paths	The number of available paths, and the number of installed best paths. This line displays “Default-IP-Routing-Table” when the best path is installed in the IP routing table.
Multipath	This field is displayed when multipath load sharing is enabled. This field will indicate if the multipaths are iBGP or eBGP.
Advertised to update-groups	The number of each update group for which advertisements are processed.
Origin	Origin of the entry. The origin can be IGP, EGP, or incomplete. This line displays the configured metric (0 if no metric is configured), the local preference value (100 is default), and the status and type of route (internal, external, multipath, best).

Field	Description
Extended Community	This field is displayed if the route carries an extended community attribute. The attribute code is displayed on this line. Information about the extended community is displayed on a subsequent line.

The following is sample output from the **show ip bgp** command entered with the **all** keyword. Information about all configured address families is displayed.

Device# **show ip bgp all**

```

For address family: IPv4 Unicast *****
BGP table version is 27, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0                 0         32768 ?
*> 10.13.13.0/24    0.0.0.0                 0         32768 ?
*> 10.15.15.0/24    0.0.0.0                 0         32768 ?
*>i10.18.18.0/24    172.16.14.105          1388     91351    0 100 e
*>i10.100.0.0/16    172.16.14.107          262       272    0 1 2 3 i
*>i10.100.0.0/16    172.16.14.105          1388     91351    0 100 e
*>i10.101.0.0/16    172.16.14.105          1388     91351    0 100 e
*>i10.103.0.0/16    172.16.14.101          1388       173    173 100 e
*>i10.104.0.0/16    172.16.14.101          1388       173    173 100 e
*>i10.100.0.0/16    172.16.14.106          2219    20889    0 53285 33299 51178 47751 e
*>i10.101.0.0/16    172.16.14.106          2219    20889    0 53285 33299 51178 47751 e
* 10.100.0.0/16     172.16.14.109          2309         0 200 300 e
*>                  172.16.14.108          1388         0 100 e
* 10.101.0.0/16     172.16.14.109          2309         0 200 300 e
*>                  172.16.14.108          1388         0 100 e
*> 10.102.0.0/16    172.16.14.108          1388         0 100 e
*> 172.16.14.0/24   0.0.0.0                 0         32768 ?
*> 192.168.5.0      0.0.0.0                 0         32768 ?
*> 10.80.0.0/16     172.16.14.108          1388         0 50 e
*> 10.80.0.0/16     172.16.14.108          1388         0 50 e

For address family: VPNv4 Unicast *****
BGP table version is 21, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf vpn1)
*> 10.1.1.0/24      192.168.4.3           1622         0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.2.0/24      192.168.4.3           1622         0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.3.0/24      192.168.4.3           1622         0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.4.0/24      192.168.4.3           1622         0 100 53285 33299 51178
{27016,57039,16690} e
*> 10.1.5.0/24      192.168.4.3           1622         0 100 53285 33299 51178
{27016,57039,16690} e
*>i172.17.1.0/24    10.3.3.3              10         30    0 53285 33299 51178 47751 ?
*>i172.17.2.0/24    10.3.3.3              10         30    0 53285 33299 51178 47751 ?
*>i172.17.3.0/24    10.3.3.3              10         30    0 53285 33299 51178 47751 ?
*>i172.17.4.0/24    10.3.3.3              10         30    0 53285 33299 51178 47751 ?
*>i172.17.5.0/24    10.3.3.3              10         30    0 53285 33299 51178 47751 ?

For address family: IPv4 Multicast *****
BGP table version is 11, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path

```



```

*> 10.40.40.0/26      172.16.14.110      2219      0 21 22 {51178,47751,27016} e
*                    10.1.1.1          1622      0 15 20 1 {2} e
*> 10.40.40.64/26     172.16.14.110      2219      0 21 22 {51178,47751,27016} e
*                    10.1.1.1          1622      0 15 20 1 {2} e
*> 10.40.40.128/26    172.16.14.110      2219      0 21 22 {51178,47751,27016} e
*                    10.1.1.1          2563      0 15 20 1 {2} e
*> 10.40.40.192/26    10.1.1.1           2563      0 15 20 1 {2} e
*> 10.40.41.0/26      10.1.1.1           1209      0 15 20 1 {2} e
*>i10.102.0.0/16      10.1.1.1            300       500      0 5 4 {101,102} e
*>i10.103.0.0/16      10.1.1.1            300       500      0 5 4 {101,102} e
For address family: NSAP Unicast *****
BGP table version is 1, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network      Next Hop      Metric LocPrf Weight Path
* i45.0000.0002.0001.000c.00  49.0001.0000.0000.0a00      100      0 ?
* i46.0001.0000.0000.0000.0a00  49.0001.0000.0000.0a00      100      0 ?
* i47.0001.0000.0000.000b.00  49.0001.0000.0000.0a00      100      0 ?
* i47.0001.0000.0000.000e.00  49.0001.0000.0000.0a00

```

The following is sample output from the **show ip bgp longer-prefixes** command:

```

Device# show ip bgp 10.92.0.0 255.255.0.0 longer-prefixes

BGP table version is 1738, local router ID is 192.168.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network      Next Hop      Metric LocPrf Weight Path
*> 10.92.0.0      10.92.72.30      8896      32768 ?
*                10.92.72.30      0 109 108 ?
*> 10.92.1.0      10.92.72.30      8796      32768 ?
*                10.92.72.30      0 109 108 ?
*> 10.92.11.0     10.92.72.30      42482     32768 ?
*                10.92.72.30      0 109 108 ?
*> 10.92.14.0     10.92.72.30      8796      32768 ?
*                10.92.72.30      0 109 108 ?
*> 10.92.15.0     10.92.72.30      8696      32768 ?
*                10.92.72.30      0 109 108 ?
*> 10.92.16.0     10.92.72.30      1400      32768 ?
*                10.92.72.30      0 109 108 ?
*> 10.92.17.0     10.92.72.30      1400      32768 ?
*                10.92.72.30      0 109 108 ?
*> 10.92.18.0     10.92.72.30      8876      32768 ?
*                10.92.72.30      0 109 108 ?
*> 10.92.19.0     10.92.72.30      8876      32768 ?
*                10.92.72.30      0 109 108 ?

```

The following is sample output from the **show ip bgp shorter-prefixes** command. An 8-bit prefix length is specified.

```

Device# show ip bgp 172.16.0.0/16 shorter-prefixes 8

*> 172.16.0.0      10.0.0.2          0 ?
*                10.0.0.2          0      0 200 ?

```

The following is sample output from the **show ip bgp prefix-list** command:

```

Device# show ip bgp prefix-list ROUTE

BGP table version is 39, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network      Next Hop      Metric LocPrf Weight Path
*> 192.168.1.0    10.0.0.2          0 ?
*                10.0.0.2          0      0 200 ?

```

The following is sample output from the **show ip bgp route-map** command:

```
Device# show ip bgp route-map LEARNED_PATH
```

```
BGP table version is 40, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network      Next Hop      Metric LocPrf Weight Path
*> 192.168.1.0   10.0.0.2                0 ?
*               10.0.0.2                0 200 ?
```

The following output indicates (for each neighbor) whether any of the additional path tags (group-best, all, best 2 or best 3) are applied to the path. A line of output indicates rx pathid (received from neighbor) and tx pathid (announcing to neighbors). Note that the “Path advertised to update-groups:” is now per-path when the BGP Additional Paths feature is enabled.

```
Device# show ip bgp 10.0.0.1 255.255.255.224
```

```
BGP routing table entry for 10.0.0.1/28, version 82
Paths: (10 available, best #5, table default)
  Path advertised to update-groups:
    21      25
  Refresh Epoch 1
  20 50, (Received from a RR-client)
    192.0.2.1 from 192.0.2.1 (192.0.2.1)
      Origin IGP, metric 200, localpref 100, valid, internal, all
      Originator: 192.0.2.1, Cluster list: 2.2.2.2
      mpls labels in/out 16/nolabel
      rx pathid: 0, tx pathid: 0x9
  Path advertised to update-groups:
    18      21
  Refresh Epoch 1
  30
    192.0.2.2 from 192.0.2.2 (192.0.2.2)
      Origin IGP, metric 200, localpref 100, valid, internal, group-best, all
      Originator: 192.0.2.2, Cluster list: 4.4.4.4
      mpls labels in/out 16/nolabel
      rx pathid: 0x1, tx pathid: 0x8
  Path advertised to update-groups:
    16      18      19      20      21      22      24
    25      27
  Refresh Epoch 1
  10
    192.0.2.3 from 192.0.2.3 (192.0.2.3)
      Origin IGP, metric 200, localpref 100, valid, external, best2, all
      mpls labels in/out 16/nolabel
      rx pathid: 0, tx pathid: 0x7
  Path advertised to update-groups:
    20      21      22      24      25
  Refresh Epoch 1
  10
    192.0.2.4 from 192.0.2.4 (192.0.2.4)
      Origin IGP, metric 300, localpref 100, valid, external, best3, all
      mpls labels in/out 16/nolabel
      rx pathid: 0, tx pathid: 0x6
  Path advertised to update-groups:
    10      13      17      18      19      20      21
    22      23      24      25      26      27      28
  Refresh Epoch 1
  10
    192.0.2.5 from 192.0.2.5 (192.0.2.5)
      Origin IGP, metric 100, localpref 100, valid, external, best
      mpls labels in/out 16/nolabel
      rx pathid: 0, tx pathid: 0x0
  Path advertised to update-groups:
    21
  Refresh Epoch 1
  30
    192.0.2.6 from 192.0.2.6 (192.0.2.6)
```

```

Origin IGP, metric 200, localpref 100, valid, internal, all
Originator: 192.0.2.6, Cluster list: 5.5.5.5
mpls labels in/out 16/nolabel
rx pathid: 0x1, tx pathid: 0x5
Path advertised to update-groups:
 18      23      24      26      28
Refresh Epoch 1
60 40, (Received from a RR-client)
 192.0.2.7 from 192.0.2.7 (192.0.2.7)
Origin IGP, metric 250, localpref 100, valid, internal, group-best
Originator: 192.0.2.7, Cluster list: 3.3.3.3
mpls labels in/out 16/nolabel
rx pathid: 0x2, tx pathid: 0x2
Path advertised to update-groups:
 25
Refresh Epoch 1
30 40, (Received from a RR-client)
 192.0.2.8 from 192.0.2.8 (192.0.2.8)
Origin IGP, metric 200, localpref 100, valid, internal, all
Originator: 192.0.2.8, Cluster list: 2.2.2.2
mpls labels in/out 16/nolabel
rx pathid: 0x1, tx pathid: 0x3
Path advertised to update-groups:
 18      21      23      24      25      26      28
Refresh Epoch 1
20 40, (Received from a RR-client)
 192.0.2.9 from 192.0.2.9 (192.0.2.9)
Origin IGP, metric 200, localpref 100, valid, internal, group-best, all
Originator: 192.0.2.9, Cluster list: 2.2.2.2
mpls labels in/out 16/nolabel
rx pathid: 0x1, tx pathid: 0x4
Path advertised to update-groups:
 21
Refresh Epoch 1
30 40
 192.0.2.9 from 192.0.2.9 (192.0.2.9)
Origin IGP, metric 100, localpref 100, valid, internal, all
Originator: 192.0.2.9, Cluster list: 4.4.4.4
mpls labels in/out 16/nolabel
rx pathid: 0x1, tx pathid: 0x1

```

The following is sample output from the **show ip bgp** command that displays unknown and discarded path attributes:

```

Device# show ip bgp 192.0.2.0/32

BGP routing table entry for 192.0.2.0/32, version 0
Paths: (1 available, no best path)
Refresh Epoch 1
Local
 192.168.101.2 from 192.168.101.2 (192.168.101.2)
Origin IGP, localpref 100, valid, internal
unknown transitive attribute: flag 0xE0 type 0x81 length 0x20
  value 0000 0000 0000 0000 0000 0000 0000 0000
      0000 0000 0000 0000 0000 0000 0000 0000

unknown transitive attribute: flag 0xE0 type 0x83 length 0x20
  value 0000 0000 0000 0000 0000 0000 0000 0000
      0000 0000 0000 0000 0000 0000 0000 0000

discarded unknown attribute: flag 0x40 type 0x63 length 0x64
  value 0000 0000 0000 0000 0000 0000 0000 0000
      0000 0000 0000 0000 0000 0000 0000 0000

```

The following is sample output from the **show ip bgp version** command:

```

Device# show ip bgp version

BGP table version is 5, local router ID is 10.2.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, x best-external

```

```

Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
*> 192.168.34.2/24 10.0.0.1 0 0 1 ?
*> 192.168.35.2/24 10.0.0.1 0 0 1 ?

```

The following example shows how to display the network version:

```
Device# show ip bgp 192.168.34.2 | include version
```

```
BGP routing table entry for 192.168.34.2/24, version 5
```

The following sample output from the **show ip bgp version recent** command displays the prefix changes in the specified version:

```
Device# show ip bgp version recent 2
```

```

BGP table version is 5, local router ID is 10.2.4.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

```

```

      Network          Next Hop      Metric LocPrf  Weight  Path
*> 192.168.134.1/28    10.0.0.1          0           0         1 ?
*> 192.168.134.19/28  10.0.0.1          0           0         1 ?
*> 192.168.134.34/28  10.0.0.1          0           0         1 ?

```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
clear ip bgp	Resets BGP connections using hard or soft reconfiguration.
ip bgp community new-format	Configures BGP to display communities in the format AA:NN.
ip prefix-list	Creates a prefix list or adds a prefix-list entry.
route-map	Defines the conditions for redistributing routes from one routing protocol into another routing protocol.
router bgp	Configures the BGP routing process.

show ip bgp bmp

To display information about the BGP Monitoring Protocol (BMP) servers and neighbors, use the **show ip bgp bmp** command in privileged EXEC mode.

show ip bgp bmp {**neighbors** | **server** {*server-number* | **details** | **summary**}}

Syntax Description

neighbors	Displays information about the BGP neighbors configured for BMP.
server	Displays information about the BMP servers.
<i>server-number</i>	Displays information about a particular BMP server. The range of BMP servers you can display is from 1 to 4.
details	Displays detailed information about BMP servers.
summary	Displays a summary of the BMP server status.

Command Default

No information about the BGP BMP servers or the BGP BMP neighbors is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S

Usage Guidelines

Use the **neighbor bmp-activate** and the **bmp** commands to configure the BMP servers, clients, and BGP neighbors. Once configured, use the **show ip bgp bmp** command to display the following information:

- Number of BMP servers configured.
- Number of BGP neighbors configured for BMP.
- Current state of the BMP servers.
- Duration of the initial refresh delay and buffer size for BMP.
- Various queues, such as TransitionQ, MonitoringQ, ConfigQ, and StatsQ, configured for the BGP BMP neighbors and BMP servers.
- The IP address or network address, port number, status, uptime, number of messages sent, and the number of active and configured BMP servers for a BGP BMP neighbor.

Examples

The following is sample output from the **show ip bgp bmp server** command for server number 1. The attributes displayed are configured in the BMP server configuration mode:

```
Device# show ip bgp bmp server 1

Print detailed info for 1 server number 1.

bmp server 1
address: 10.1.1.1    port 8000
description SERVER1
up time 00:06:22
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
activated
```

The following is sample output from the **show ip bgp bmp server** command for server number 2. The attributes displayed are configured in the BMP server configuration mode:

```
Device# show ip bgp bmp server 2

Print detailed info for 1 server number 2.

bmp server 2
address: 20.1.1.1    port 9000
description SERVER2
up time 00:06:23
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
activated
```

The following is sample output from the **show ip bgp bmp server summary** command after deactivating the BMP server 1 and 2 connections:

```
Device# show ip bgp bmp server summary

Number of BMP servers configured: 2
Number of BMP neighbors configured: 10
Number of neighbors on TransitionQ: 0, MonitoringQ: 0, ConfigQ: 0
Number of BMP servers on StatsQ: 0
BMP Refresh not in progress, refresh not scheduled
Initial Refresh Delay configured, refresh value 3s
BMP buffer size configured, buffer size 2048 MB, buffer size bytes used 0 MB
```

ID	Host/Net	Port	TCB	Status	Uptime	MsgSent	LastStat
1	10.1.1.1	8000	0x0	Down		0	
2	20.1.1.1	9000	0x0	Down		0	

The following is sample output from the **show ip bgp bmp neighbors** command, which shows the status of the BGP BMP neighbors after reactivating the BMP server 1 and 2 connections:

```
Device# show ip bgp bmp server neighbors

Number of BMP neighbors configured: 10
BMP Refresh not in progress, refresh not scheduled
Initial Refresh Delay configured, refresh value 3s
BMP buffer size configured, buffer size 2048 MB, buffer size bytes used 0 MB
```

Neighbor	PriQ	MsgQ	CfgSvr#	ActSvr#	RM Sent
30.1.1.1	0	0	1 2	1 2	16
2001:DB8::2001	0	0	1 2	1 2	15
40.1.1.1	0	0	1 2	1 2	26
2001:DB8::2002	0	0	1 2	1 2	15

```

50.1.1.1      0      0      1 2      1 2      16
60.1.1.1      0      0      1 2      1 2      26
2001:DB8::2002 0      0      1        1        9
70.1.1.1      0      0      2        2        12
Neighbor      PriQ    MsgQ    CfgSvr#    ActSvr#    RM Sent
80.1.1.1      0      0      1        1        10
2001:DB8::2002 0      0      1 2      1 2      16

```

Related Commands

Command	Description
bmp	Configures BMP parameters on BGP BMP servers.
neighbor bmp-activate	Activates monitoring of BMP servers.

show ip bgp all dampening

To display BGP dampening information, use the **show ip bgp all dampening** command in user EXEC or privileged EXEC mode.

show ip bgp all dampening {**dampened-paths**| **flap-statistics** [**filter-list** *filter-list*| **quote-regexp** *regexp*| **regexp** *regexp*]} **parameters**}

Syntax Description

dampened-paths	Display routes suppressed due to dampening.
flap-statistics	Displays flap statistics of routes.
filter-list <i>filter-list</i>	(Optional) Used with the flap-statistics keyword, displays routes that conform to the specified filter list in the range 1-500.
quote-regexp <i>regexp</i>	(Optional) Used with the flap-statistics keyword, displays routes matching the AS path “regular expression”.
regexp <i>regexp</i>	(Optional) Used with the flap-statistics keyword, displays routes matching the AS path regular expression.
parameters	Display details of configured dampening parameters.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use this command to display BGP dampening information.

Examples

The following example show how to display the BGP dampening parameters.

```
Router# show ip bgp all dampening parameters
```

```
For address family: IPv4 Unicast
% dampening not enabled for base
For address family: VPNv4 Unicast
```



```

% dampening not enabled for base
For vrf: Cust_A
dampening 15 750 2000 60 (DEFAULT)
  Half-life time      : 15 mins      Decay Time          : 2320 secs
  Max suppress penalty: 12000        Max suppress time: 60 mins
  Suppress penalty    : 2000         Reuse penalty       : 750
For vrf: Cust_B
dampening 15 750 2000 60 (DEFAULT)
  Half-life time      : 15 mins      Decay Time          : 2320 secs
  Max suppress penalty: 12000        Max suppress time: 60 mins
  Suppress penalty    : 2000         Reuse penalty       : 750
For address family: IPv4 Multicast
% dampening not enabled for base

Router#

```

The table below describes the significant fields shown in the display.

Table 39: show ip bgp all dampening Field Descriptions

Field	Description
Half-life time	Time after which a penalty is decreased, in minutes. Once the interface has been assigned a penalty, the penalty is decreased by half after the half-life period. The process of reducing the penalty happens every 5 seconds. The range of the half-life is 1 to 45 minutes. The default is 1 minute.
Decay Time	Penalty value below which an unstable interface is unsuppressed, in seconds. The process of unsuppressing routers occurs at 10-second increments. The range of the reuse value is 1 to 20000 seconds. The default value is 750 seconds.
Max suppress penalty	Limit at which an interface is suppressed when its penalty exceeds that limit, in seconds. The default value is 2000 seconds.
Max suppress time	Maximum time that an interface can be suppressed, in minutes. This value effectively acts as a ceiling that the penalty value cannot exceed. The default value is four times the half-life period.

The following is sample output for the **show ip bgp all dampening dampened-paths** command. The output includes dampened paths for individual VRFs.

```

Router# show ip bgp all dampening dampened-paths

For address family: IPv4 Unicast
% dampening not enabled for base
For address family: VPNv4 Unicast
% dampening not enabled for base
For vrf: Cust_A
BGP table version is 42, local router ID is 144.124.23.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

```

show ip bgp all dampening

```

      Network          From          Reuse      Path
Route Distinguisher: 1:100 (Cust_A)
*d 10.10.10.10/32      172.16.1.2      00:04:49  65001 ?
*d 20.20.20.20/32      172.16.1.2      00:04:59  65001 ?
For address family: IPv4 Multicast
% dampening not enabled for base

```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
show dampening interface	Displays a summary of the dampening parameters and status.

show ip bgp cidr-only

To display routes with classless interdomain routing (CIDR), use the **show ip bgp cidr-only** command in user EXEC or privileged EXEC mode.

show ip bgp cidr-only

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC (>)
Privileged EXEC (#)

Command History	Release	Modification
	10.0	This command was introduced.
	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)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.

Examples The following is sample output from the **show ip bgp cidr-only** command in privileged EXEC mode:

```
Router# show ip bgp cidr-only
BGP table version is 220, local router ID is 172.16.73.131
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
*> 192.168.0.0/8   172.16.72.24             0 1878 ?
*> 172.16.0.0/16   172.16.72.30             0 108 ?
```

The table below describes the significant fields shown in the display.

Table 40: show ip bgp cidr-only Field Descriptions

Field	Description
BGP table version is 220	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.

Field	Description
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

show ip bgp cluster-ids

To display the cluster IDs applied to any neighbor and other cluster information, use the **show ip bgp cluster-ids** command in user EXEC or privileged EXEC mode.

show ip bgp cluster-ids

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC (>)
Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines Use this command to display cluster IDs, including the number of neighbors using each cluster ID, and those cluster IDs for which intracluster client-to-client route reflection has been disabled.

Examples The following is sample output for the **show ip bgp cluster-ids** command:

```
Device# show ip bgp cluster-id

Global cluster-id: 1.1.1.10 (configured: 0.0.0.0)
BGP client-to-client reflection: Configured Used
  all (inter-cluster and intra-cluster): ENABLED
  intra-cluster: ENABLED ENABLED

List of cluster-ids:
Cluster-id    #-neighbors C2C-rfl-CFG C2C-rfl-USE
0.0.0.1       1 ENABLED   ENABLED
0.0.0.2       1 DISABLED  DISABLED
0.0.0.3       1 DISABLED  DISABLED
0.0.0.4       0 DISABLED  DISABLED
```

The table below describes the significant fields shown in the display.

Table 41: show ip bgp cluster-ids Field Descriptions

Field	Description
Global cluster-id	Global cluster ID, which is either configured by the bgp cluster-id command or, in the absence of such configuration, the router ID of the local route reflector.

Field	Description
configured:	Global cluster ID configured by the bgp cluster-id command. The cluster ID 0.0.0.0 means no cluster ID was configured, so the router ID is used as the default cluster ID.
BGP client-to-client reflection:	Configured and Used are column headings for the data below them. Because of the order in which the software processes the commands, what is configured might not be what is used. See the bgp client-to-client reflection intra-cluster command for the rules that determine whether reflection is enabled or not.
all (inter-cluster and intra-cluster):	Intracluster and intercluster client-to-client reflection is ENABLED (which is the default) or DISABLED by the bgp client-to-client reflection command.
intra-cluster:	Intracluster client-to-client reflection is ENABLED (which is the default) or DISABLED by the bgp client-to-client reflection intra-cluster command. Values are displayed for what is Configured and what is Used because they could be different values. See the bgp client-to-client reflection intra-cluster command for the rules that determine whether reflection is enabled or not.
List of cluster-ids: Cluster-id	Cluster IDs configured on the device.
#-neighbors	Number of neighbors that are using each cluster ID (regardless of whether the cluster ID is configured directly or by a template).
C2C-rfl-CFG	Client-to-client reflection configured displays ENABLED (the default) or DISABLED, based on what is configured.
C2C-rfl-USE	Client-to-client reflection used displays ENABLED (the default) or DISABLED, based on what command value is used. See the bgp client-to-client reflection intra-cluster command for the rules that determine whether reflection is enabled or not.

Related Commands

Command	Description
bgp client-to-client reflection	Enables route reflection from a BGP route reflector to clients.

Command	Description
bgp client-to-client reflection intra-cluster	Enables intracluster client-to-client route reflection to clients for the specified clusters.
bgp cluster-id	Sets the global cluster ID on a route reflector.
neighbor cluster-id	Sets a cluster ID for a neighbor.

show ip bgp community

To display routes that belong to specified BGP communities, use the **show ip bgp community** command in user EXEC or privileged EXEC mode.

show ip bgp community [*community-number*] [**gshut**] [**local-as**] [**no-advertise**] [**no-export**] [**exact**]

Syntax Description

<i>community-number</i>	(Optional) Displays routes that have a community number in the range from 1 to 4294967200, or AA:NN (autonomous system-community number/2-byte number).
gshut	(Optional) Displays routes that have the well-known Graceful Shutdown (GSHUT) community.
local-as	(Optional) Displays routes that have the well-known local-AS community, which means do not send outside the local autonomous system.
no-advertise	(Optional) Displays routes that have the well-known no-advertise community, which means do not advertise to any peer.
no-export	(Optional) Displays routes that have the well-known no-export community, which means do not export to the next autonomous system.
exact	(Optional) Displays only routes that have the same communities as the communities specified in this command.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.3	This command was introduced.
12.0	This command was modified. The local-as community was added.
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.
15.2(2)S	This command was modified. The gshut keyword was added.
Cisco IOS XE Release 3.6S	This command was modified. The gshut keyword was added.
Cisco IOS XE Release 3.7S	This command was implemented on the Cisco ASR 903 router.
15.2(4)M	This command was integrated into Cisco IOS Release 15.2(4)M.
15.2(4)S	This command was implemented on the Cisco 7200 series router.

Examples

The following is sample output from the **show ip bgp community** command:

```
Router# show ip bgp community 111:12345 local-as

BGP table version is 10, local router ID is 224.0.0.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop           Metric LocPrf Weight Path
*> 172.16.2.2/32    10.43.222.2         0             0 222 ?
*> 10.0.0.0         10.43.222.2         0             0 222 ?
*> 10.43.0.0        10.43.222.2         0             0 222 ?
*> 10.43.44.44/32   10.43.222.2         0             0 222 ?
* 10.43.222.0/24    10.43.222.2         0             0 222 i
*> 172.17.240.0/21  10.43.222.2         0             0 222 ?
*> 192.168.212.0    10.43.222.2         0             0 222 i
*> 172.31.1.0       10.43.222.2         0             0 222 ?
```

The table below describes the significant fields shown in the display.

Table 42: show ip bgp community Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show ip bgp community gshut** command:

Router# **show ip bgp community gshut**

BGP table version is 44, local router ID is 87.87.87.87

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,

Origin codes: i - IGP, e - EGP, ? - incomplete

RPKI validation codes: V valid, I invalid, N Not found

Network	Next Hop	Metric	LocPrf	Weight	Path
*> 1.1.1.1/32	192.168.10.1	0	65546	14	i
*> 1.1.1.2/32	192.168.10.1	0	65546	14	i
*> 1.1.1.3/32	192.168.10.1	0	65546	14	i
*> 1.1.1.4/32	192.168.10.1	0	65546	14	i
*> 1.1.1.5/32	192.168.10.1	0	65546	14	i
*> 1.1.1.6/32	192.168.10.1	0	65546	14	i
*> 1.1.1.7/32	192.168.10.1	0	65546	14	i
*> 1.1.1.8/32	192.168.10.1	0	65546	14	i
*> 1.1.1.9/32	192.168.10.1	0	65546	14	i
*> 1.1.1.10/32	192.168.10.1	0	65546	14	i
*> 2.2.2.2/32	192.168.10.1	0	65546	4260036618	i
*> 2.2.2.3/32	192.168.10.1	0	65546	4260036618	i
*> 2.2.2.4/32	192.168.10.1	0	65546	4260036618	i
*> 2.2.2.5/32	192.168.10.1	0	65546	4260036618	i

show ip bgp community-list

To display routes that are permitted by the Border Gateway Protocol (BGP) community list, use the **show ip bgp community-list** command in user EXEC or privileged EXEC mode.

show ip bgp community-list {*community-list-number*| *community-list-name* [**exact-match**]}

Syntax Description

<i>community-list-number</i>	A standard or expanded community list number in the range from 1 to 500.
<i>community-list-name</i>	Community list name. The community list name can be standard or expanded.
exact-match	(Optional) Displays only routes that have an exact match.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.3	This command was introduced.
12.0(10)S	Named community list support was added.
12.0(16)ST	Named community lists support was integrated into Cisco IOS Release 12.0(16)ST.
12.1(9)E	Named community lists support was integrated into Cisco IOS Release 12.1(9)E.
12.2(8)T	Named community lists support was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB to support the Cisco 10000 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

This command requires you to specify an argument when used. The **exact-match** keyword is optional.

Examples

The following is sample output of the **show ip bgp community-list** command in privileged EXEC mode:

```
Router# show ip bgp community-list 20

BGP table version is 716977, local router ID is 192.168.32.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
* i10.3.0.0       10.0.22.1          0      100      0 1800 1239 ?
*>i              10.0.16.1          0      100      0 1800 1239 ?
* i10.6.0.0       10.0.22.1          0      100      0 1800 690 568 ?
*>i              10.0.16.1          0      100      0 1800 690 568 ?
* i10.7.0.0       10.0.22.1          0      100      0 1800 701 35 ?
*>i              10.0.16.1          0      100      0 1800 701 35 ?
*                  10.92.72.24          0      100      0 1878 704 701 35 ?
* i10.8.0.0       10.0.22.1          0      100      0 1800 690 560 ?
*>i              10.0.16.1          0      100      0 1800 690 560 ?
*                  10.92.72.24          0      100      0 1878 704 701 560 ?
* i10.13.0.0      10.0.22.1          0      100      0 1800 690 200 ?
*>i              10.0.16.1          0      100      0 1800 690 200 ?
*                  10.92.72.24          0      100      0 1878 704 701 200 ?
* i10.15.0.0      10.0.22.1          0      100      0 1800 174 ?
*>i              10.0.16.1          0      100      0 1800 174 ?
* i10.16.0.0      10.0.22.1          0      100      0 1800 701 i
*>i              10.0.16.1          0      100      0 1800 701 i
*                  10.92.72.24          0      100      0 1878 704 701 i
```

The table below describes the significant fields shown in the display.

Table 43: show ip bgp community-list Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.

Field	Description
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show ip bgp dampened-paths

To display BGP dampened routes, use the **show ip bgp dampened-paths** command in user EXEC or privileged EXEC mode.

show ip bgp dampened-paths

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

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

On the Cisco 10000 series router, use the **show ip bgp dampening dampened-paths** command to display BGP dampened routes.

Examples

The following is sample output from the **show ip bgp dampened-paths** command in privileged EXEC mode:

```
Router# show ip bgp dampened-paths

BGP table version is 10, local router ID is 172.29.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        From        Reuse    Path
*d 10.0.0.0        172.16.232.177  00:18:4 100 ?
*d 10.2.0.0        172.16.232.177  00:28:5 100 ?
```

The table below describes the significant fields shown in the display.

Table 44: show ip bgp dampened-paths Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.

Field	Description
local router	IP address of the router where route dampening is enabled.
*d	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear ip bgp dampening	Clears BGP route dampening information and unsuppresses the suppressed routes.

show ip bgp dampening dampened-paths

To display Border Gateway Protocol (BGP) dampened routes on the Cisco 10000 series router, use the **show ip bgp dampening dampened-paths** command in user EXEC or privileged EXEC mode.

show ip bgp dampening dampened-paths [*community-list-number*| *community-list-name* [**exact-match**]]

Syntax Description

<i>community-list-number</i>	(Optional) Community list number. The range is from 1 to 500.
<i>community-list-name</i>	(Optional) Community list name.
exact-match	(Optional) Displays only routes that have an exact match.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2S	This command was introduced.

Usage Guidelines

For router platforms other than the Cisco 10000 series router, use the **show ip bgp dampened-paths** command to display BGP dampened routes.

Examples

The following example show how to display BGP dampened routes information:

```
Router# show ip bgp dampening dampened-paths

BGP table version is 10, local router ID is 172.29.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        From        Reuse    Path
*d 10.0.0.0       172.16.232.177  00:18:4  100 ?
*d 10.2.0.0       172.16.232.177  00:28:5  100 ?
```

The table below describes the significant fields shown in the display.

Table 45: show ip bgp dampening dampened-paths Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router where route dampening is enabled.
*d	Route to the network is dampened.
From	IP address of the peer that advertised this path.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system (AS) path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear ip bgp dampening	Clears BGP route dampening information and unsuppresses the suppressed routes.
show dampening interface	Displays a summary of the dampening parameters and status.
show ip bgp dampened-paths	Displays IPv6 Border Gateway Protocol (BGP) dampened routes.

show ip bgp dampening flap-statistics

To display Border Gateway Protocol (BGP) flap statistics for all paths on the Cisco 10000 series router, use the **show ip bgp dampening flap-statistics** command in privileged EXEC mode.

show ip bgp dampening flap-statistics [*ip-address* [*mask*]] **cidr-only** **filter-list** *access-list-number* | **injected-paths** | **labels** | **prefix-list** *prefix-list* | **quote-regexp** *regexp* | **regexp** *regexp* | **route-map** *route-map-name* | **template** {**peer-policy** *template-name* | **peer-session** *template-name*}

Syntax Description

<i>ip-address</i>	(Optional) IP address for the flap statistics that you want to display.
mask	(Optional) Mask to filter or match hosts that are part of the specified network.
cidr-only	(Optional) Displays flap statistics for routes with classless interdomain routing (CIDR).
filter-list <i>access-list-number</i>	(Optional) Displays flap statistics for routes that conform to the specified autonomous system (AS) path access list number.
injected-paths	(Optional) Displays flap statistics for all injected paths.
labels	(Optional) Displays flap statistics for IPv4 Network Layer Reachability Information (NLRI) labels.
prefix-list <i>prefix-list</i>	(Optional) Filters output based on the specified prefix list.
quote-regexp <i>regexp</i>	(Optional) Filters output based on the specified quoted expression.
regexp <i>regexp</i>	(Optional) Filters output based on the specified regular expression.
route-map <i>route-map-name</i>	(Optional) Filters output based on the specified route map.
template	(Optional) Displays peer-policy or peer-session template information.
peer-policy <i>template-name</i>	(Optional) Used with the template keyword, displays peer-policy template information for the specified template name.

peer-session <i>template-name</i>	(Optional) Used with the template keyword, displays peer-session template information for the specified template name.

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	12.2S	This command was introduced.

Usage Guidelines For router platforms other than the Cisco 10000 series router, use the **show ip bgp flap-statistics** command to display BGP flap statistics.

Examples The following example show how to display the BGP flap statistics for routes with non-natural network masks (CIDR):

```
Router# show ip bgp dampening flap-statistics cidr-only

BGP table version is 56, local router ID is 100.10.7.11
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
*>i205.0.5.0/30    100.10.5.11             0      100      0 i
*>i205.0.5.4/30    205.0.5.1               0      100      0 105 ?
*>i205.10.5.9/32   205.0.5.1               2      100      0 105 ?
*>i205.10.5.13/32  205.0.5.1               2      100      0 105 ?
*>i206.0.6.0/30    100.10.5.11             0      100      0 i
*>i206.0.6.4/30    206.0.6.1               0      100      0 106 ?
*>i206.10.6.9/32   206.0.6.1               2      100      0 106 ?
*>i206.10.6.13/32  206.0.6.1               2      100      0 106 ?
*> 207.0.7.0/30    0.0.0.0                 0             32768 i
*> 207.0.7.4/30    207.0.7.1               0             0 107 ?
*> 207.10.7.9/32   207.0.7.1               2             0 107 ?
*> 207.10.7.13/32  207.0.7.1               2             0 107 ?
*> 208.0.8.0/30    0.0.0.0                 0             32768 i
*> 208.0.8.4/30    208.0.8.1               0             0 108 ?
*> 208.10.8.9/32   208.0.8.1               2             0 108 ?
*> 208.10.8.13/32  208.0.8.1               2             0 108 ?
```

The table below describes the significant fields shown in the display.

Table 46: show ip bgp dampening flap-statistics cidr-only Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router where route dampening is enabled.

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Network	Internet address of the network that the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.

Command	Description
clear ip bgp flap-statistics	Clears BGP flap statistics.
show dampening interface	Displays a summary of the dampening parameters and status.
show ip bgpflap-statistics	Displays BGP flap statistics.

show ip bgp dampening parameters

To display detailed Border Gateway Protocol (BGP) dampening information on the Cisco 10000 series router, use the **show ip bgp dampening parameters** command in privileged EXEC mode.

show ip bgp dampening parameters

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2S	This command was introduced.

Examples The following example shows how to display detailed BGP dampening information:

```
Router# show ip bgp dampening parameters
dampening 15 750 2000 60 (DEFAULT)
  Half-life time      : 15 mins      Decay Time           : 2320 secs
  Max suppress penalty: 12000       Max suppress time: 60 mins
```

The table below describes the significant fields shown in the display.

Table 47: show ip bgp dampening parameters Field Descriptions

Field	Description
Half-life time	Time after which a penalty is decreased, in minutes. Once the interface has been assigned a penalty, the penalty is decreased by half after the half-life period. The process of reducing the penalty happens every 5 seconds. The range of the half-life period is 1 to 45 minutes. The default is 1 minute.
Decay Time	Penalty value below which an unstable interface is unsuppressed, in seconds. The process of unsuppressing routers occurs at 10 second increments. The range of the reuse value is 1 to 20000 seconds. The default value is 750 seconds.
Max suppress penalty	Limit at which an interface is suppressed when its penalty exceeds that limit, in seconds. The default value is 2000 seconds.

Field	Description
Max suppress time	Maximum time that an interface can be suppressed, in minutes. This value effectively acts as a ceiling that the penalty value cannot exceed. The default value is four times the half-life period.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear ip bgp dampening	Clears BGP dampening information.
show dampening interface	Displays a summary of the dampening parameters and status.

show ip bgp extcommunity-list

To display routes that match the extended community list in the Border Gateway Protocol (BGP) routing table, use the **show ip bgp extcommunity-list** command in user EXEC or privileged EXEC mode.

show ip bgp extcommunity-list [*list-name*]

Syntax Description

<i>list-name</i>	(Optional) Specifies an extended community list name.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(27)SBC	This command was integrated into the Cisco IOS Release 12.2(27)SBC.
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 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

You need to configure the extended community lists by using the **ip extcommunity-list** command for the **show ip bgp extcommunity-list** command to display the output.

Examples

The following is sample output from the **show ip bgp extcommunity-list** command:

```
Router# show ip bgp extcommunity-list 1
Standard extended community-list list1
 9 permit RT:1:100 RT:2:100
19 deny RT:5:100 RT:6:200
29 permit RT:4:100
39 permit RT:5:900
49 permit RT:4:100 RT:6:200
```

The table below describes the significant fields shown in the display.

Table 48: show ip bgp extcommunity-list Field Descriptions

Field	Description
Standard extended community-list	The standard named extended community list.
permit	Permits access for a matching condition. Once a permit value has been configured to match a given set of extended communities, the extended community list defaults to an implicit deny for all other values.
RT	The route target (RT) extended community attribute.
deny	Denies access for a matching condition.

Related Commands

Command	Description
ip extcommunity-list	Creates an extended community list to configure VPN route filtering.
router bgp	Configures the BGP routing process.
show route-map	Displays configured route maps.

show ip bgp filter-list

To display routes that conform to a specified filter list, use the **show ip bgp filter-list** command in EXEC mode.

show ip bgp filter-list *access-list-number*

Syntax Description

<i>access-list-number</i>	Number of an autonomous system path access list. It can be a number from 1 to 199, or on the Cisco 10000 series router this is a number from 1 to 500.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)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.

Examples

The following is sample output from the **show ip bgp filter-list** command in privileged EXEC mode:

```
Router# show ip bgp filter-list 2

BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
* 172.16.0.0      172.16.72.30              0 109 108 ?
* 172.16.1.0      172.16.72.30              0 109 108 ?
* 172.16.11.0     172.16.72.30              0 109 108 ?
* 172.16.14.0     172.16.72.30              0 109 108 ?
* 172.16.15.0     172.16.72.30              0 109 108 ?
* 172.16.16.0     172.16.72.30              0 109 108 ?
* 172.16.17.0     172.16.72.30              0 109 108 ?
* 172.16.18.0     172.16.72.30              0 109 108 ?
* 172.16.19.0     172.16.72.30              0 109 108 ?
* 172.16.24.0     172.16.72.30              0 109 108 ?
* 172.16.29.0     172.16.72.30              0 109 108 ?
* 172.16.30.0     172.16.72.30              0 109 108 ?
* 172.16.33.0     172.16.72.30              0 109 108 ?
* 172.16.35.0     172.16.72.30              0 109 108 ?
* 172.16.36.0     172.16.72.30              0 109 108 ?
* 172.16.37.0     172.16.72.30              0 109 108 ?
```

```
* 172.16.38.0      172.16.72.30      0 109 108 ?
* 172.16.39.0      172.16.72.30      0 109 108 ?
```

The table below describes the significant fields shown in the display.

Table 49: show ip bgp filter-list Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP route to this network.
Metric	If shown, this is the value of the interautonomous system metric. This field is frequently not used.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.

Field	Description
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

show ip bgp flap-statistics

To display BGP flap statistics, use the **show ip bgp flap-statistics** command in EXEC mode.

show ip bgp flap-statistics[*regexp regexp*| **filter-list** *access-list*| *ip-address mask*[**longer-prefix**]]

Syntax Description

regexp <i>regexp</i>	(Optional) Clears flap statistics for all the paths that match the regular expression.
filter-list <i>access-list</i>	(Optional) Clears flap statistics for all the paths that pass the access list.
<i>ip-address</i>	(Optional) Clears flap statistics for a single entry at this IP address.
<i>mask</i>	(Optional) Network mask applied to the value.
longer-prefix	(Optional) Displays flap statistics for more specific entries.

Command Modes

EXEC

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

If no arguments or keywords are specified, the router displays flap statistics for all routes.

Examples

The following is sample output from the **show ip bgp flap-statistics** command in privileged EXEC mode:

```
Router# show ip bgp flap-statistics

BGP table version is 10, local router ID is 172.29.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          From          Flaps Duration Reuse      Path
```

```
*d 10.0.0.0          172.29.232.177  4      00:13:31 00:18:10 100
*d 10.2.0.0          172.29.232.177  4      00:02:45 00:28:20 100
```

The table below describes the significant fields shown in the display.

Table 50: show ip bgp flap-statistics Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router where route dampening is enabled.
Network	Route to the network indicated is dampened.
From	IP address of the peer that advertised this path.
Flaps	Number of times the route has flapped.
Duration	Time (in hours:minutes:seconds) since the router noticed the first flap.
Reuse	Time (in hours:minutes:seconds) after which the path will be made available.
Path	Autonomous system path of the route that is being dampened.

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes various BGP route dampening factors.
clear ip bgp flap-statistics	Clears BGP flap statistics.

show ip bgp inconsistent-as

To display routes with inconsistent originating autonomous systems, use the **show ip bgp inconsistent-as** command in EXEC mode.

show ip bgp inconsistent-as

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	11.0	This command was introduced.
	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)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.

Examples The following is sample output from the **show ip bgp inconsistent-as** command in privileged EXEC mode:

```
Router# show ip bgp inconsistent-as

BGP table version is 87, local router ID is 172.19.82.53
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop        Metric LocPrf Weight Path
*   10.1.0.0      172.29.232.55      0           0 300 88 90 99 ?
*>                172.29.232.52     2222          0 400 ?
*  172.29.0.0     172.29.232.55      0           0 300 90 99 88 200 ?
*>                172.29.232.52     2222          0 400 ?
*  10.200.199.0   172.29.232.55      0           0 300 88 90 99 ?
*>                172.29.232.52     2222          0 400 ?
```

show ip bgp injected-paths

To display all the injected paths in the Border Gateway Protocol (BGP) routing table, use the **show ip bgp injected-paths** command in user or privileged EXEC mode.

show ip bgp injected-paths

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC (>)
Privileged EXEC (#)

Command History	Release	Modification
	12.0(14)ST	This command was introduced.
	12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.

Examples The following is sample output from the **show ip bgp injected-paths** command in EXEC mode:

```
Router# show ip bgp injected-paths

BGP table version is 11, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
*> 172.16.0.0      10.0.0.2                0 ?
*> 172.17.0.0/16   10.0.0.2                0 ?
```

The table below describes the significant fields shown in the display.

Table 51: show ip bgp injected-paths Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

 show ip bgp injected-paths

show ip bgp ipv4

To display entries in the IP version 4 (IPv4) Border Gateway Protocol (BGP) routing table, use the **show ip bgp ipv4** command in privileged EXEC mode.

show ip bgp ipv4 {**mdt** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} | **mvpn** {**all** | **rd** *route-distinguisher* | **vrf** *vrf-name*} | **unicast** *prefix* | **multicast** *prefix* | **tunnel**}

Syntax Description

mdt	Displays entries for multicast distribution tree (MDT) sessions.
all	Displays all the entries in the routing table.
rd <i>route-distinguisher</i>	Displays information about the specified VPN route distinguisher.
vrf <i>vrf-name</i>	Displays information about the specified VRF.
mvpn	Displays entries for multicast VPN (MVPN) sessions.
unicast	Displays entries for unicast sessions.
<i>prefix</i>	Displays entries for the specified prefix.
multicast	Displays entries for multicast sessions.
tunnel	Displays entries for tunnel sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(29)S	This command was modified. The mdt keyword was added.
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.

Release	Modification
12.4(20)T	This command was modified. The mdt keyword was added.
15.2(1)S	This command was modified. An RPKI validation code is displayed per network, if one applies.
Cisco IOS XE 3.5S	This command was modified. An RPKI validation code is displayed per network, if one applies.
Cisco IOS XE 3.7S	This command was modified. Imported paths from a VRF table to the global routing table are displayed, if any.
15.2(4)S	This command was implemented on the Cisco 7200 series routers.
Cisco IOS XE 3.8S	This command was modified. The mvpn keyword was added.

Examples

The following is sample output from the **show ip bgp ipv4 unicast** command:

```
Router# show ip bgp ipv4 unicast

BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1             0           0 300 i
*> 10.10.20.0/24   172.16.10.1             0           0 300 i
* 10.20.10.0/24    172.16.10.1             0           0 300 i
```

The following is sample output from the **show ip bgp ipv4 multicast** command:

```
Router# show ip bgp ipv4 multicast

BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1             0           0 300 i
*> 10.10.20.0/24   172.16.10.1             0           0 300 i
* 10.20.10.0/24    172.16.10.1             0           0 300 i
```

The table below describes the significant fields shown in the display.

Table 52: show ip bgp ipv4 unicast Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is damped. • h—The table entry history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an Internal Border Gateway Protocol (IBGP) session.
Origin codes	Origin of the entry. The origin code is displayed at the end of each line in the table. It can be one of the following values: • i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. • e—Entry originated from an Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.

Field	Description
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show ip bgp ipv4 unicast *prefix*** command. The output indicates the imported path information from a VRF named vpn1.

Device# **show ip bgp ipv4 unicast 150.1.1.0**

```
BGP routing table entry for 150.1.1.0/24, version 2
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1
  65002, imported path from 1:1:150.1.1.0/24 (vpn1)
    4.4.4.4 (metric 11) from 4.4.4.4 (4.4.4.4)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:1:1
      mpls labels in/out nolabel/16
```

Related Commands

Command	Description
clear ip bgp ipv4 mdt	Resets MDT IPv4 BGP address-family sessions.
export map	Exports IP prefixes from a VRF table into the global table.
show ip bgp	Displays entries in the BGP routing table.

show ip bgp ipv4 multicast

To display IP Version 4 multicast database-related information, use the **show ip bgp ipv4 multicast** command in EXEC mode.

show ip bgp ipv4 multicast [*command*]

Syntax Description

<i>command</i>	(Optional) Any multiprotocol BGP command supported by the show ip bgp ipv4 multicast <i>command</i> .

Command Modes

EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)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.

Usage Guidelines

Use this command in conjunction with the **show ip rpf** command to determine if IP multicast routing is using multiprotocol BGP routes.

To determine which multiprotocol BGP commands are supported by the **show ip bgp ipv4 multicast** *command*, enter the following command while in EXEC mode:

```
Router# show ip bgp ipv4 multicast ?
```

The **show ip bgp ipv4 multicast** command replaces the **show ip mbgp** command.

Examples

The following is sample output from the **show ip bgp ipv4 multicast** command:

```
Router# show ip bgp ipv4 multicast
```

```
MBGP table version is 6, local router ID is 192.168.200.66
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
*> 10.0.20.16/28   0.0.0.0             0         0 32768 i
*> 10.0.35.16/28   0.0.0.0             0         0 32768 i
```

```

*> 10.0.36.0/28      0.0.0.0      0      0 32768 i
*> 10.0.48.16/28     0.0.0.0      0      0 32768 i
*> 10.2.0.0/16       0.0.0.0      0      0 32768 i
*> 10.2.1.0/24       0.0.0.0      0      0 32768 i
*> 10.2.2.0/24       0.0.0.0      0      0 32768 i
*> 10.2.3.0/24       0.0.0.0      0      0 32768 i
*> 10.2.7.0/24       0.0.0.0      0      0 32768 i
*> 10.2.8.0/24       0.0.0.0      0      0 32768 i
*> 10.2.10.0/24      0.0.0.0      0      0 32768 i
*> 10.2.11.0/24      0.0.0.0      0      0 32768 i
*> 10.2.12.0/24      0.0.0.0      0      0 32768 i
*> 10.2.13.0/24      0.0.0.0      0      0 32768 i

```

The table below describes the significant fields shown in the display.

Table 53: show ip bgp ipv4 multicast Field Descriptions

Field	Description
MBGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h--The table entry is historical. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration or address family configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.

Field	Description
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

Related Commands

Command	Description
show ip rpf	Displays how IP multicast routing does RPF.

show ip bgp ipv4 multicast summary

To display a summary of IP Version 4 multicast database-related information, use the **show ip bgp ipv4 multicast summary** command in EXEC mode.

show ip bgp ipv4 multicast summary

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	12.0(7)T	This command was introduced.
	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)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.

Usage Guidelines The **show ip bgp ipv4 multicast summary** command replaces the **show ip mbgp summary** command.

Examples The following is sample output from the **show ip bgp ipv4 multicast summary** command:

```
Router# show ip bgp ipv4 multicast summary

BGP router identifier 10.0.33.34, local AS number 34
BGP table version is 5, main routing table version 1
4 network entries and 6 paths using 604 bytes of memory
5 BGP path attribute entries using 260 bytes of memory
1 BGP AS-PATH entries using 24 bytes of memory
2 BGP community entries using 48 bytes of memory
2 BGP route-map cache entries using 32 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP activity 8/28 prefixes, 12/0 paths, scan interval 15 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.0.33.35      4     35     624     624       5     0     0 10:13:46         3
```

The table below describes the significant fields shown in the display.

Table 54: show ip bgp ipv4 multicast summary Field Descriptions

Field	Description
Neighbor	IP address of configured neighbor in the multicast routing table.
V	Version of multiprotocol BGP used.
AS	Autonomous system to which the neighbor belongs.
MsgRcvd	Number of messages received from the neighbor.
MsgSent	Number of messages sent to the neighbor.
TblVer	Number of the table version, which is incremented each time the table changes.
InQ	Number of messages received in the input queue.
OutQ	Number of messages ready to go in the output queue.
Up/Down	Days and hours that the neighbor has been up or down (no information in the State column means the connection is up).
State/PfxRcd	State of the neighbor/number of routes received. If no state is indicated, the state is up.

Related Commands

Command	Description
show ip rpf	Displays how IP multicast routing does RPF.

show ip bgp ipv6 multicast

To display multicast entries in the IPv6 BGP routing table, use the **show ip bgp ipv6 multicast** command in user EXEC or privileged EXEC mode.

show ip bgp ipv6 multicast [*prefix/length*]

Syntax Description

<i>prefix/length</i>	(Optional) IPv6 network number (entered to display a particular network in the IPv6 BGP routing table) and length of the IPv6 prefix. For the length, a decimal value indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was modified. It displays information about imported paths from a VRF, if any.

Usage Guidelines

The **show ip bgp ipv6 multicast** command provides output similar to the **show ip bgp** command, except that it is IPv6 multicast-specific.

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection or session.

show ip bgp ipv6 unicast

To display entries in the Internet Protocol version 6 (IPv6) Border Gateway Protocol (BGP) routing table, use the **show ip bgp ipv6 unicast** command in user EXEC or privileged EXEC mode.

show ip bgp ipv6 unicast [*prefix/length*]

Syntax Description

<i>prefix/length</i>	(Optional) IPv6 network number and length of the IPv6 prefix, entered to display a particular network in the IPv6 BGP routing table. The <i>length</i> is a decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was modified. The command displays the RPKI validation state, if present, as part of the path description.
15.2(1)S	This command was modified. The command displays the RPKI validation state, if present, as part of the path description.
Cisco IOS XE Release 3.7S	This command was modified. It displays information about imported paths from a VRF, if any.
15.2(4)S	This command was implemented on the Cisco 7200 series routers.

Usage Guidelines

The **show ip bgp ipv6 unicast** command provides output similar to the **show ip bgp** command, except that it is IPv6 specific.

Examples

The following is sample output from the **show bgp ipv6 unicast prefix/length** command, showing the RPKI state of the path:

```
Router# show bgp ipv6 unicast 2010::1/128
```

```

BGP routing table entry for 2010::1/128, version 5
Paths: (1 available, best #1, table default)
  Advertised to update-groups:
    1          2
  Refresh Epoch 1
    3
    2002::1 (FE80::A8BB:CCFF:FE00:300) from 2002::1 (10.0.0.3)
      Origin IGP, metric 0, localpref 100, valid, external, best
      path 079ECBD0 RPKI State not found

```

The table below describes the significant fields shown in the display.

Table 55: show ip bgp ipv6 Field Descriptions

Field	Description
BGP routing table entry for	IPv6 prefix and prefix length, internal version number of the table. This number is incremented whenever the table changes.
Paths:	Number of routes available to destination.
Advertised to update-groups:	Update group numbers.
3	Autonomous system number.
2002::1 (FE80::A8BB:CCFF:FE00:300) from 2002::1 (10.0.0.3)	Address of the neighbor from which the path was received, link local address of the neighbor, from address of the neighbor, BGP router ID of the neighbor.
Origin	Indicates the origin of the entry.
metric	If shown, the value of the interautonomous system metric.
localpref	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
valid	Path is legitimate.
external	Path is an External Border Gateway Protocol (EBGP) path.
best path	Path is flagged as the best path; number indicates which path in memory.
RPKI State	RPKI state of the network prefix shown at the beginning of the output. The state could be valid, invalid, or not found.

Related Commands

Command	Description
clear bgp ipv6	Resets an IPv6 BGP connection or session.

show ip bgp l2vpn

To display Layer 2 Virtual Private Network (L2VPN) address family information from the Border Gateway Protocol (BGP) table, use the **show ip bgp l2vpn** command in user EXEC or privileged EXEC mode.

With BGP show Command Argument

```
show ip bgp l2vpn vpls {all | [summary | [slow] ve-id id-value] {block-offset | [value]} | rd
{route-distinguisher | [ve-id | {block-offset | [value]}]} [bgp-keyword]
```

With IP Prefix and Mask Length Syntax

```
show ip bgp l2vpn vpls {all | rd route-distinguisher} [ip-prefix/length [[bestpath]] [longer-prefixes
[[injected]]] [[multipaths]] [shorter-prefixes [[ mask-length ]]] [[subnets]]]
```

With Network Address Syntax

```
show ip bgp l2vpn vpls {all | rd route-distinguisher} [network-address [mask| bestpath| multipaths] [bestpath]
[longer-prefixes [injected]] [multipaths] [shorter-prefixes [ mask-length ]]] [subnets]]
```

Syntax Description

vpls	Displays L2VPN address family database information for the Virtual Private LAN Service (VPLS) subsequent address family identifier (SAFI).
all	Displays the complete L2VPN database.
rd <i>route-distinguisher</i>	Displays prefixes that match the specified route distinguisher.
ve-id <i>id-value</i>	(Optional) Displays the target VPLS Endpoint (VE) ID and ID value.
summary	(Optional) Displays a summary of BGP neighbor status.
slow	(Optional) Displays a summary of slow-peer status.
block-offset <i>value</i>	Displays the target block-offset value.
<i>bgp-keyword</i>	(Optional) Argument representing a show ip bgp command keyword that can be added to this command. See the table below.
<i>ip-prefix/length</i>	(Optional) The IP prefix address (in dotted decimal format) and the length of the mask (0 to 32). The slash mark must be included.
bestpath	(Optional) Displays the best path for the specified prefix.

longer-prefixes	(Optional) Displays the route and more specific routes.
injected	(Optional) Displays more specific routes that were injected because of the specified prefix.
multipaths	(Optional) Displays the multipaths for the specified prefix.
shorter-prefixes	(Optional) Displays the less specific routes.
<i>mask-length</i>	(Optional) The length of the mask as a number in the range from 0 to 32. Prefixes longer than the specified mask length are displayed.
subnets	(Optional) Displays the subnet routes for the specified prefix.
<i>network-address</i>	(Optional) The IP address of a network in the BGP routing table.
<i>mask</i>	(Optional) The mask of the network address, in dotted decimal format.

Command Default If no arguments or keywords are specified, this command displays the complete L2VPN database.

Command Modes User EXEC (>)
Privileged EXEC (#)

Command History	Release	Modification
	12.2(33)SRB	This command was introduced.
	Cisco IOS XE2.6	This command was integrated into Cisco IOS XE Release 2.6.
	Cisco IOS XE3.8S	This command was modified. RFC4761 is fully supported in Cisco IOS XE Release 3.8S.

Usage Guidelines The table below displays optional **show ip bgp** command keywords that can be configured with the **show ip bgp l2vpn** command. Replace the *bgp-keyword* argument with the appropriate keyword from the table. For more details about each command in its **show ip bgp *bgp-keyword*** form, see the *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols*, Release 12.2.

Table 56: Optional show ip bgp Command Keywords and Descriptions

Keyword	Description
community	Displays routes that match a specified community.
community-list	Displays routes that match a specified community list.
dampening	Displays paths suppressed because of dampening (BGP route from peer is up and down).
extcommunity-list	Displays routes that match a specified extcommunity list.
filter-list	Displays routes that conform to the filter list.
inconsistent-as	Displays only routes that have inconsistent autonomous systems of origin.
neighbors	Displays details about TCP and BGP neighbor connections.
oer-paths	Displays all OER-managed path information.
paths [<i>regex</i>]	Displays autonomous system path information. If the optional <i>regex</i> argument is entered, the autonomous system paths that are displayed match the autonomous system path regular expression.
peer-group	Displays information about peer groups.
pending-prefixes	Displays prefixes that are pending deletion.
prefix-list	Displays routes that match a specified prefix list.
quote-regex	Displays routes that match the quoted autonomous system path regular expression.
regex	Displays routes that match the autonomous system path regular expression.
replication	Displays the replication status update groups.
route-map	Displays routes that match the specified route map.
rt-filter-list	Displays the specified inbound route target filter list.
summary	Displays a summary of BGP neighbor status.
update-group	Displays information on update groups.

Examples

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **all** keywords are used to display the complete L2VPN database:

```
Device# show ip bgp l2vpn vpls all

BGP table version is 5, local router ID is 192.168.3.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network        Next Hop           Metric LocPrf Weight Path
Route Distinguisher: 45000:100
*> 45000:100:172.17.1.1/96
      0.0.0.0                                32768 ?
*>i45000:100:172.18.2.2/96
      172.16.1.2                            0      100      0 ?
Route Distinguisher: 45000:200
*> 45000:200:172.17.1.1/96
      0.0.0.0                                32768 ?
*>i45000:200:172.18.2.2/96
      172.16.1.2                            0      100      0 ?
```

The table below describes the significant fields shown in the display.

Table 57: show ip bgp l2vpn vpls all Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is a historical entry. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP (iBGP) session. • r—The table entry failed to install in the routing information base (RIB) table. • S—The table entry is Stale (old). This entry is useful in BGP graceful restart situations.

Field	Description
Origin codes	Origin of the entry. The origin code is displayed at the end of each line in the table. It can be one of the following values: • i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. • e—Entry originated from an Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the set local-preference command in route-map configuration mode. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.
Route Distinguisher	Route distinguisher that identifies a set of routing and forwarding tables used in virtual private networks.

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **all** keywords are used to display information about all VPLS BGP signaling prefixes (including local generated and received from remote):

```
Device#show ip bgp l2vpn vpls all
```

```
BGP table version is 14743, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found
```

Network	Next Hop	Metric	LocPrf	Weight	Path
Route Distinguisher: 65000:1					
*>i 65000:1:VEID-3:Blk-1/136	3.3.3.3	0	100	0	?
*> 65000:1:VEID-4:Blk-1/136	0.0.0.0			32768	?
*>i 65000:1:VEID-5:Blk-1/136	2.2.2.2	0	100	0	?
*>i 65000:1:VEID-6:Blk-1/136	4.4.4.4	0	100	0	?
Route Distinguisher: 65000:2					
*> 65000:2:VEID-20:Blk-20/136	0.0.0.0			32768	?
*>i 65000:2:VEID-21:Blk-20/136	2.2.2.2	0	100	0	?
*>i 65000:2:VEID-22:Blk-20/136	3.3.3.3	0	100	0	?
*>i 65000:2:VEID-23:Blk-20/136	4.4.4.4	0	100	0	?

The following example shows output for the **show ip bgp l2vpn** command when the **vpls**, **all** and **summary** keywords are used to display information about the L2VPN VPLS address family:

Device# **show ip bgp l2vpn vpls all summary**

```

BGP router identifier 10.1.1.1, local AS number 65000
BGP table version is 14743, main routing table version 14743
6552 network entries using 1677312 bytes of memory
6552 path entries using 838656 bytes of memory
3276/3276 BGP path/bestpath attribute entries using 760032 bytes of memory
1638 BGP extended community entries using 65520 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 3341520 total bytes of memory
BGP activity 9828/3276 prefixes, 9828/3276 paths, scan interval 60 secs
Neighbor      V      AS  MsgRcvd  MsgSent  TblVer  InQ  OutQ  Up/Down
State/PfxRcd
10.2.2.2      4      65000   90518    90507    14743    0     0  8w0d   1638
10.3.3.3      4      65000    4901     4895    14743    0     0  2d01h  1638
10.4.4.4      4      65000    4903     4895    14743    0     0  2d01h  1638

```

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **rd rd** keywords are used to display information about all VPLS BGP signaling prefixes with the specified rd, i.e. the same VPLS instance:

Device# **show ip bgp l2vpn vpls rd 65000:3**

```

BGP table version is 14743, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
               x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network      Next Hop      Metric LocPrf Weight Path
Route Distinguisher: 65000:3
*> 65000:3:VEID-30:Blk-30/136
    0.0.0.0                                32768 ?
*>i 65000:3:VEID-31:Blk-30/136
    2.2.2.2                                0 100 0 ?
*>i 65000:3:VEID-32:Blk-30/136
    3.3.3.3                                0 100 0 ?
*>i 65000:3:VEID-33:Blk-30/136
    4.4.4.4                                0 100 0 ?

```

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **rd** keywords are used to display the L2VPN information that matches the route distinguisher 45000:100. Note that the information displayed is a subset of the information displayed using the **all** keyword.

```
Device# show ip bgp l2vpn vpls rd 45000:100

BGP table version is 5, local router ID is 192.168.3.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network        Next Hop           Metric LocPrf Weight Path
Route Distinguisher: 45000:100
*> 45000:100:172.17.1.1/96
                        0.0.0.0                 32768 ?
*>i45000:100:172.18.2.2/96
                        172.16.1.2                 0   100       0 ?
```

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **all** keywords are used to display information about an individual prefix:

```
Device# show ip bgp l2vpn vpls all ve-id 31 block 30

BGP routing table entry for 65000:3:VEID-31:Blk-30/136, version 11
Paths: (1 available, best #1, table L2VPN-VPLS-BGP-Table)
  Not advertised to any peer
  Refresh Epoch 2
  Local
    2.2.2.2 (metric 2) from 2.2.2.2 (2.2.2.2)
    Origin incomplete, metric 0, localpref 100, valid, internal, best
    AGI version(0), VE Block Size(10) Label Base(16596)
    Extended Community: RT:65000:3 L2VPN L2:0x0:MTU-1500
    rx pathid: 0, tx pathid: 0x0
      0      100      0 ?
```

Related Commands

Command	Description
address-family l2vpn	Enters address family configuration mode to configure a routing session using L2VPN endpoint provisioning information.
show bgp l2vpn vpls	Displays L2VPN VPLS address family information from the BGP table.

show ip bgp neighbors

To display information about Border Gateway Protocol (BGP) and TCP connections to neighbors, use the **show ip bgp neighbors** command in user or privileged EXEC mode.

```
show ip bgp [ipv4 {multicast|unicast}| vpnv4 all| vpnv6 unicast all] neighbors [slow| ip-address|  
ipv6-address [advertised-routes| dampened-routes| flap-statistics| paths [reg-exp ]| policy [detail]| received  
prefix-filter| received-routes| routes]]
```

Syntax Description

ipv4	(Optional) Displays peers in the IPv4 address family.
multicast	(Optional) Specifies IPv4 multicast address prefixes.
unicast	(Optional) Specifies IPv4 unicast address prefixes.
vpnv4 all	(Optional) Displays peers in the VPNv4 address family.
vpnv6 unicast all	(Optional) Displays peers in the VPNv6 address family.
slow	(Optional) Displays information about dynamically configured slow peers.
<i>ip-address</i>	(Optional) IP address of the IPv4 neighbor. If this argument is omitted, information about all neighbors is displayed.
<i>ipv6-address</i>	(Optional) IP address of the IPv6 neighbor.
advertised-routes	(Optional) Displays all routes that have been advertised to neighbors.
dampened-routes	(Optional) Displays the dampened routes received from the specified neighbor.
flap-statistics	(Optional) Displays the flap statistics of the routes learned from the specified neighbor (for external BGP peers only).
paths <i>reg-exp</i>	(Optional) Displays autonomous system paths learned from the specified neighbor. An optional regular expression can be used to filter the output.
policy	(Optional) Displays the policies applied to this neighbor per address family.

detail	(Optional) Displays detailed policy information such as route maps, prefix lists, community lists, access control lists (ACLs), and autonomous system path filter lists.
received prefix-filter	(Optional) Displays the prefix list (outbound route filter [ORF]) sent from the specified neighbor.
received-routes	(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
routes	(Optional) Displays all routes that are received and accepted. The output displayed when this keyword is entered is a subset of the output displayed by the received-routes keyword.

Command Default

The output of this command displays information for all neighbors.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Mainline and T Release	Modification
10.0	This command was introduced.
11.2	This command was modified. The received-routes keyword was added.
12.2(4)T	This command was modified. The received and prefix-filter keywords were added.
12.2(15)T	This command was modified. Support for the display of BGP graceful restart capability information was added.
12.3(7)T	This command was modified. The command output was modified to support the BGP TTL Security Check feature and to display explicit-null label information.
12.4(4)T	This command was modified. Support for the display of Bidirectional Forwarding Detection (BFD) information was added.
12.4(11)T	This command was modified. Support for the policy and detail keywords was added.
12.4(20)T	This command was modified. The output was modified to support BGP TCP path MTU discovery.

Mainline and T Release	Modification
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.

Command History

S Release	Modification
12.0(18)S	This command was modified. The output was modified to display the no-prepend configuration option.
12.0(21)ST	This command was modified. The output was modified to display Multiprotocol Label Switching (MPLS) label information.
12.0(22)S	This command was modified. Support for the display of BGP graceful restart capability information was added. Support for the Cisco 12000 series routers (Engine 0 and Engine 2) was also added.
12.0(25)S	This command was modified. The policy and detail keywords were added.
12.0(27)S	This command was modified. The command output was modified to support the BGP TTL Security Check feature and to display explicit-null label information.
12.0(31)S	This command was modified. Support for the display of BFD information was added.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17b)SXA	This command was integrated into Cisco IOS Release 12.2(17b)SXA.
12.2(18)SXE	This command was modified. Support for the display of BFD information was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was modified. The output was modified to support BGP TCP path Maximum Transmission Unit (MTU) discovery.
12.2(33)SRB	This command was modified. Support for the policy and detail keywords was added.

S Release	Modification
12.2(33)SXH	This command was modified. Support for displaying BGP dynamic neighbor information was added.
12.2(33)SRC	This command was modified. Support for displaying BGP graceful restart information was added.
12.2(33)SB	This command was modified. Support for displaying BFD and the BGP graceful restart per peer information was added, and support for the policy and detail keywords was integrated into Cisco IOS Release 12.2(33)SB.
12.2(33)SXII	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)SRE	This command was modified. Support for displaying BGP best external and BGP additional path features information was added. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)S	This command was modified. The slow keyword was added.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)S	This command was modified. The Layer 2 VPN address family is displayed if graceful restart or nonstop forwarding (NSF) is enabled.
15.1(1)SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
15.2(4)S	This command was modified and implemented on the Cisco 7200 series router. The configured discard and treat-as-withdraw attributes are displayed, along with counts of incoming Updates with a matching discard attribute or treat-as-withdraw attribute, and number of times a malformed Update is treat-as-withdraw. The capabilities of the neighbor to send and receive additional paths that are advertised or received are added.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Command History

Cisco IOS XE	Modification
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Cisco IOS XE	Modification
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
Cisco IOS XE Release 3.1S	This command was modified. The slow keyword was added.
Cisco IOS XE Release 3.6S	This command was modified. Support for displaying BGP BFD multihop and C-bit information was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format became asplain.
Cisco IOS XE Release 3.7S	This command was implemented on the Cisco ASR 903 router and the output modified. The configured discard and treat-as-withdraw attributes are displayed, along with counts of incoming Updates with a matching discard attribute or treat-as-withdraw attribute, and number of times a malformed Update is treat-as-withdraw. The capabilities of the neighbor to send and receive additional paths that are advertised or received are added.
Cisco IOS XE Release 3.8S	This command was modified. In support of the BGP Multi-Cluster ID feature, the cluster ID of a neighbor is displayed if the neighbor is assigned a cluster.

Usage Guidelines

Use the **show ip bgp neighbors** command to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance.

Prefix activity is displayed based on the number of prefixes that are advertised and withdrawn. Policy denials display the number of routes that were advertised but then ignored based on the function or attribute that is displayed in the output.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538, for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Cisco IOS Releases 12.0(25)S, 12.4(11)T, 12.2(33)SRB, 12.2(33)SB, and Later Releases

When BGP neighbors use multiple levels of peer templates, determining which policies are applied to the neighbor can be difficult.

In Cisco IOS Release 12.0(25)S, 12.4(11)T, 12.2(33)SRB, 12.2(33)SB, and later releases, the **policy** and **detail** keywords were added to display the inherited policies and the policies configured directly on the specified neighbor. Inherited policies are policies that the neighbor inherits from a peer group or a peer policy template.

Examples

Example output is different for the various keywords available for the **show ip bgp neighbors** command. Examples using the various keywords appear in the following sections.

Examples

The following example shows output for the BGP neighbor at 10.108.50.2. This neighbor is an internal BGP (iBGP) peer. This neighbor supports the route refresh and graceful restart capabilities.

Device# **show ip bgp neighbors 10.108.50.2**

```
BGP neighbor is 10.108.50.2, remote AS 1, internal link
BGP version 4, remote router ID 192.168.252.252
BGP state = Established, up for 00:24:25
Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is
60 seconds
Neighbor capabilities:
  Route refresh: advertised and received(old & new)
  MPLS Label capability: advertised and received
  Graceful Restart Capability: advertised
  Address family IPv4 Unicast: advertised and received
Message statistics:
  InQ depth is 0
  OutQ depth is 0

          Sent          Rcvd
Opens:           3           3
Notifications:    0           0
Updates:          0           0
Keepalives:      113        112
Route Refresh:    0           0
Total:           116        115
Default minimum time between advertisement runs is 5 seconds
For address family: IPv4 Unicast
BGP additional-paths computation is enabled
BGP advertise-best-external is enabled
BGP table version 1, neighbor version 1/0
Output queue size : 0
Index 1, Offset 0, Mask 0x2
1 update-group member

          Sent          Rcvd
Prefix activity:  ----  ----
Prefixes Current:      0           0
Prefixes Total:        0           0
Implicit Withdraw:      0           0
Explicit Withdraw:      0           0
Used as bestpath:      n/a           0
Used as multipath:      n/a           0
                   Outbound  Inbound
Local Policy Denied Prefixes:  -----
Total:                        0           0
Number of NLRI in the update sent: max 0, min 0
Connections established 3; dropped 2
Last reset 00:24:26, due to Peer closed the session
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 10.108.50.1, Local port: 179
Foreign host: 10.108.50.2, Foreign port: 42698
Enqueued packets for retransmit: 0, input: 0 mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x68B944):
Timer           Starts    Wakeups          Next
Retrans           27         0           0x0
TimeWait          0         0           0x0
```

```

AckHold          27          18          0x0
SendWnd          0           0          0x0
KeepAlive        0           0          0x0
GiveUp           0           0          0x0
PmtuAger         0           0          0x0
DeadWait         0           0          0x0
iss: 3915509457  snduna: 3915510016  sndnxt: 3915510016  sndwnd: 15826
irs: 233567076  rcvnxt: 233567616  rcvwnd: 15845  delrcvwnd: 539
SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6
Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08
The table below describes the significant fields shown in the display. Fields that are preceded by the asterisk
character (*) are displayed only when the counter has a nonzero value.

```

Table 58: show ip bgp neighbors Field Descriptions

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number.
remote AS	Autonomous system number of the neighbor.
local AS 300 no-prepend (not shown in display)	Verifies that the local autonomous system number is not prepended to received external routes. This output supports the hiding of the local autonomous systems when a network administrator is migrating autonomous systems.
internal link	“internal link” is displayed for iBGP neighbors; “external link” is displayed for external BGP (eBGP) neighbors.
BGP version	BGP version being used to communicate with the remote router.
remote router ID	IP address of the neighbor.
BGP state	Finite state machine (FSM) stage of session negotiation.
up for	Time, in hh:mm:ss, that the underlying TCP connection has been in existence.
Last read	Time, in hh:mm:ss, since BGP last received a message from this neighbor.
last write	Time, in hh:mm:ss, since BGP last sent a message to this neighbor.

Field	Description
hold time	Time, in seconds, that BGP will maintain the session with this neighbor without receiving messages.
keepalive interval	Time interval, in seconds, at which keepalive messages are transmitted to this neighbor.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor. "advertised and received" is displayed when a capability is successfully exchanged between two routers.
Route refresh	Status of the route refresh capability.
MPLS Label capability	Indicates that MPLS labels are both sent and received by the eBGP peer.
Graceful Restart Capability	Status of the graceful restart capability.
Address family IPv4 Unicast	IP Version 4 unicast-specific properties of this neighbor.
Message statistics	Statistics organized by message type.
InQ depth is	Number of messages in the input queue.
OutQ depth is	Number of messages in the output queue.
Sent	Total number of transmitted messages.
Revd	Total number of received messages.
Opens	Number of open messages sent and received.
Notifications	Number of notification (error) messages sent and received.
Updates	Number of update messages sent and received.
Keepalives	Number of keepalive messages sent and received.
Route Refresh	Number of route refresh request messages sent and received.
Total	Total number of messages sent and received.
Default minimum time between...	Time, in seconds, between advertisement transmissions.
For address family:	Address family to which the following fields refer.

Field	Description
BGP table version	Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.
neighbor version	Number used by the software to track prefixes that have been sent and those that need to be sent.
1 update-group member	Number of the update-group member for this address family.
Prefix activity	Prefix statistics for this address family.
Prefixes Current	Number of prefixes accepted for this address family.
Prefixes Total	Total number of received prefixes.
Implicit Withdraw	Number of times that a prefix has been withdrawn and readvertised.
Explicit Withdraw	Number of times that a prefix has been withdrawn because it is no longer feasible.
Used as bestpath	Number of received prefixes installed as best paths.
Used as multipath	Number of received prefixes installed as multipaths.
* Saved (soft-reconfig)	Number of soft resets performed with a neighbor that supports soft reconfiguration. This field is displayed only if the counter has a nonzero value.
* History paths	This field is displayed only if the counter has a nonzero value.
* Invalid paths	Number of invalid paths. This field is displayed only if the counter has a nonzero value.
Local Policy Denied Prefixes	Prefixes denied due to local policy configuration. Counters are updated for inbound and outbound policy denials. The fields under this heading are displayed only if the counter has a nonzero value.
* route-map	Displays inbound and outbound route-map policy denials.
* filter-list	Displays inbound and outbound filter-list policy denials.

Field	Description
* prefix-list	Displays inbound and outbound prefix-list policy denials.
* Ext Community	Displays only outbound extended community policy denials.
* AS_PATH too long	Displays outbound AS_PATH length policy denials.
* AS_PATH loop	Displays outbound AS_PATH loop policy denials.
* AS_PATH confed info	Displays outbound confederation policy denials.
* AS_PATH contains AS 0	Displays outbound denials of autonomous system 0.
* NEXT_HOP Martian	Displays outbound martian denials.
* NEXT_HOP non-local	Displays outbound nonlocal next-hop denials.
* NEXT_HOP is us	Displays outbound next-hop-self denials.
* CLUSTER_LIST loop	Displays outbound cluster-list loop denials.
* ORIGINATOR loop	Displays outbound denials of local originated routes.
* unsuppress-map	Displays inbound denials due to an unsuppress map.
* advertise-map	Displays inbound denials due to an advertise map.
* VPN Imported prefix	Displays inbound denials of VPN prefixes.
* Well-known Community	Displays inbound denials of well-known communities.
* SOO loop	Displays inbound denials due to site-of-origin.
* Bestpath from this peer	Displays inbound denials because the best path came from the local router.
* Suppressed due to dampening	Displays inbound denials because the neighbor or link is in a dampening state.
* Bestpath from iBGP peer	Displays inbound denials because the best path came from an iBGP neighbor.
* Incorrect RIB for CE	Displays inbound denials due to RIB errors for a customer edge (CE) router.
* BGP distribute-list	Displays inbound denials due to a distribute list.

Field	Description
Number of NLRIs...	Number of network layer reachability attributes in updates.
Connections established	Number of times a TCP and BGP connection has been successfully established.
dropped	Number of times that a valid session has failed or been taken down.
Last reset	Time, in hh:mm:ss, since this peering session was last reset. The reason for the reset is displayed on this line.
External BGP neighbor may be...	Indicates that the BGP time to live (TTL) security check is enabled. The maximum number of hops that can separate the local and remote peer is displayed on this line.
Connection state	Connection status of the BGP peer.
unread input bytes	Number of bytes of packets still to be processed.
Connection is ECN Disabled	Explicit congestion notification status (enabled or disabled).
Local host: 10.108.50.1, Local port: 179	IP address of the local BGP speaker. BGP port number 179.
Foreign host: 10.108.50.2, Foreign port: 42698	Neighbor address and BGP destination port number.
Enqueued packets for retransmit:	Packets queued for retransmission by TCP.
Event Timers	TCP event timers. Counters are provided for starts and wakeups (expired timers).
Retrans	Number of times a packet has been retransmitted.
TimeWait	Time waiting for the retransmission timers to expire.
AckHold	Acknowledgment hold timer.
SendWnd	Transmission (send) window.
KeepAlive	Number of keepalive packets.
GiveUp	Number of times a packet is dropped due to no acknowledgment.
PmtuAger	Path MTU discovery timer.

Field	Description
DeadWait	Expiration timer for dead segments.
iss:	Initial packet transmission sequence number.
snduna:	Last transmission sequence number that has not been acknowledged.
sndnxt:	Next packet sequence number to be transmitted.
sndwnd:	TCP window size of the remote neighbor.
irs:	Initial packet receive sequence number.
rcvnxt:	Last receive sequence number that has been locally acknowledged.
rcvwnd:	TCP window size of the local host.
delrcvwnd:	Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is higher than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT:	A calculated smoothed round-trip timeout.
RTTO:	Round-trip timeout.
RTV:	Variance of the round-trip time.
KRTT:	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.
minRTT:	Shortest recorded round-trip timeout (hard-wired value used for calculation).
maxRTT:	Longest recorded round-trip timeout.
ACK hold:	Length of time the local host will delay an acknowledgment to carry (piggyback) additional data.
IP Precedence value:	IP precedence of the BGP packets.
Datagrams	Number of update packets received from a neighbor.
Rcvd:	Number of received packets.

Field	Description
out of order:	Number of packets received out of sequence.
with data	Number of update packets sent with data.
total data bytes	Total amount of data received, in bytes.
Sent	Number of update packets sent.
Second Congestion	Number of update packets with data sent.
Datagrams: Rcvd	Number of update packets received from a neighbor.
retransmit	Number of packets retransmitted.
fastretransmit	Number of duplicate acknowledgments retransmitted for an out of order segment before the retransmission timer expires.
partialack	Number of retransmissions for partial acknowledgments (transmissions before or without subsequent acknowledgments).
Second Congestion	Number of second retransmissions sent due to congestion.

Examples

The following partial example shows output for several external BGP neighbors in autonomous systems with 4-byte autonomous system numbers, 65536 and 65550. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or a later release.

```
Router# show ip bgp neighbors
```

```
BGP neighbor is 192.168.1.2, remote AS 65536, external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read 02:03:38, last write 02:03:38, hold time is 120, keepalive interval is 70
seconds
  Configured hold time is 120, keepalive interval is 70 seconds
  Minimum holdtime from neighbor is 0 seconds
.
.
.
BGP neighbor is 192.168.3.2, remote AS 65550, external link
  Description: finance
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read 02:03:48, last write 02:03:48, hold time is 120, keepalive interval is 70
seconds
  Configured hold time is 120, keepalive interval is 70 seconds
  Minimum holdtime from neighbor is 0 seconds
```

Examples

The following example displays routes advertised for only the 172.16.232.178 neighbor:

```
Device# show ip bgp neighbors 172.16.232.178 advertised-routes

BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network        Next Hop           Metric LocPrf Weight Path
*>i10.0.0.0      172.16.232.179         0    100      0 ?
*> 10.20.2.0     10.0.0.0                0          32768 i
The table below describes the significant fields shown in the display.
```

Table 59: show ip bgp neighbors advertised-routes Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This is the primary routing table with which the neighbor has been updated. The number increments when the table changes.
local router ID	IP address of the local BGP speaker.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened and will not be advertised to BGP neighbors. • h—The table entry does not contain the best path based on historical information. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP (iBGP) session.

Field	Description
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. • e—Entry originated from Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system used to forward a packet to the destination network. An entry of 0.0.0.0 indicates that there are non-BGP routes in the path to the destination network.
Metric	If shown, this is the value of the interautonomous system metric. This field is not used frequently.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

Examples

The following is sample output from the **show ip bgp neighbors** command entered with the **check-control-plane-failure** option configured:

```
Device# show ip bgp neighbors 10.10.10.1
```

```
BGP neighbor is 10.10.10.1, remote AS 10, internal link
  Fall over configured for session
  BFD is configured. BFD peer is Up. Using BFD to detect fast fallover (single-hop) with
c-bit check-control-plane-failure.
Inherits from template cbit-tps for session parameters
  BGP version 4, remote router ID 10.7.7.7
  BGP state = Established, up for 00:03:55
  Last read 00:00:02, last write 00:00:21, hold time is 180, keepalive interval is 60 seconds
```

```
Neighbor sessions:
  1 active, is not multisession capable (disabled)
```

```

Neighbor capabilities:
  Route refresh: advertised and received(new)
  Four-octets ASN Capability: advertised and received
  Address family IPv4 Unicast: advertised and received
  Enhanced Refresh Capability: advertised and received
  Multisession Capability:
  Stateful switchover support enabled: NO for session 1

```

Examples

The following is sample output from the **show ip bgp neighbors** command entered with the **paths** keyword:

```
Device# show ip bgp neighbors 172.29.232.178 paths 10
```

```

Address      Refcount Metric Path
0x60E577B0      2      40 10 ?

```

The table below describes the significant fields shown in the display.

Table 60: show ip bgp neighbors paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Refcount	Number of routes using that path.
Metric	Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	Autonomous system path for that route, followed by the origin code for that route.

Examples

The following example shows that a prefix list that filters all routes in the 10.0.0.0 network has been received from the 192.168.20.72 neighbor:

```
Device# show ip bgp neighbors 192.168.20.72 received prefix-filter
```

```

Address family:IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
  seq 5 deny 10.0.0.0/8 le 32

```

The table below describes the significant fields shown in the display.

Table 61: show ip bgp neighbors received prefix-filter Field Descriptions

Field	Description
Address family	Address family mode in which the prefix filter is received.
ip prefix-list	Prefix list sent from the specified neighbor.

Examples

The following sample output shows the policies applied to the neighbor at 192.168.1.2. The output displays both inherited policies and policies configured on the neighbor device. Inherited policies are policies that the neighbor inherits from a peer group or a peer-policy template.

```
Device# show ip bgp neighbors 192.168.1.2 policy
Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
  route-map ROUTE in
Inherited policies:
  prefix-list NO-MARKETING in
  route-map ROUTE in
  weight 300
  maximum-prefix 10000
```

Examples

The following is sample output from the **show ip bgp neighbors** command that verifies that Bidirectional Forwarding Detection (BFD) is being used to detect fast fallover for the BGP neighbor that is a BFD peer:

```
Device# show ip bgp neighbors
BGP neighbor is 172.16.10.2, remote AS 45000, external link
.
.
.
Using BFD to detect fast fallover
```

Examples

The following is sample output from the **show ip bgp neighbors** command that verifies that BGP TCP path maximum transmission unit (MTU) discovery is enabled for the BGP neighbor at 172.16.1.2:

```
Device# show ip bgp neighbors 172.16.1.2
BGP neighbor is 172.16.1.2, remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
.
.
.
Address tracking is enabled, the RIB does have a route to 172.16.1.2
Address tracking requires at least a /24 route to the peer
Connections established 3; dropped 2
Last reset 00:00:35, due to Router ID changed
Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

Examples

The following is sample output from the **show ip bgp neighbors** command that verifies that the neighbor 192.168.3.2 is a member of the peer group group192 and belongs to the subnet range group 192.168.0.0/16, which shows that this BGP neighbor was dynamically created:

```
Device# show ip bgp neighbors 192.168.3.2
```

show ip bgp neighbors

```

BGP neighbor is *192.168.3.2, remote AS 50000, external link
Member of peer-group group192 for session parameters
Belongs to the subnet range group: 192.168.0.0/16
BGP version 4, remote router ID 192.168.3.2
BGP state = Established, up for 00:06:35
Last read 00:00:33, last write 00:00:25, hold time is 180, keepalive intervals
Neighbor capabilities:
  Route refresh: advertised and received(new)
  Address family IPv4 Unicast: advertised and received
Message statistics:
  InQ depth is 0
  OutQ depth is 0

              Sent          Rcvd
Opens:          1            1
Notifications:  0            0
Updates:        0            0
Keepalives:     7            7
Route Refresh:  0            0
Total:          8            8
Default minimum time between advertisement runs is 30 seconds
For address family: IPv4 Unicast
BGP table version 1, neighbor version 1/0
Output queue size : 0
Index 1, Offset 0, Mask 0x2
1 update-group member
group192 peer-group member
.
.
.

```

Examples

The following is partial output from the **show ip bgp neighbors** command that verifies the status of the BGP graceful restart capability for the external BGP peer at 192.168.3.2. Graceful restart is shown as disabled for this BGP peer.

```

Device# show ip bgp neighbors 192.168.3.2

BGP neighbor is 192.168.3.2, remote AS 50000, external link
Inherits from template S2 for session parameters
BGP version 4, remote router ID 192.168.3.2
BGP state = Established, up for 00:01:41
Last read 00:00:45, last write 00:00:45, hold time is 180, keepalive intervals
Neighbor sessions:
  1 active, is multisession capable
Neighbor capabilities:
  Route refresh: advertised and received(new)
  Address family IPv4 Unicast: advertised and received
.
.
.
Address tracking is enabled, the RIB does have a route to 192.168.3.2
Connections established 1; dropped 0
Last reset never
Transport(tcp) path-mtu-discovery is enabled
Graceful-Restart is disabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0

```

Examples

The following is partial output from the **show ip bgp neighbors** command. For this release, the display includes the Layer 2 VFN address family information if graceful restart or NSF is enabled.

```

Device# show ip bgp neighbors

Load for five secs: 2%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:49:17.034 GMT Wed Sep 22 2010
BGP neighbor is 10.1.1.3, remote AS 2, internal link

```

BGP version 4, remote router ID 10.1.1.3
 BGP state = Established, up for 00:14:32
 Last read 00:00:30, last write 00:00:43, hold time is 180, keepalive interval is 60 seconds

Neighbor sessions:

1 active, is not multisession capable (disabled)

Neighbor capabilities:

Route refresh: advertised and received(new)

Four-octets ASN Capability: advertised and received

Address family IPv4 Unicast: advertised and received

Address family L2VPN Vpls: advertised and received

Graceful Restart Capability: advertised and received

Remote Restart timer is 120 seconds

Address families advertised by peer:

IPv4 Unicast (was not preserved), L2VPN Vpls (was not preserved)

Multisession Capability:

Message statistics:

InQ depth is 0

OutQ depth is 0

	Sent	Rcvd
Opens:	1	1
Notifications:	0	0
Updates:	4	16
Keepalives:	16	16
Route Refresh:	0	0
Total:	21	33

Default minimum time between advertisement runs is 0 seconds

For address family: IPv4 Unicast

Session: 10.1.1.3

BGP table version 34, neighbor version 34/0

Output queue size : 0

Index 1, Advertise bit 0

1 update-group member

Slow-peer detection is disabled

Slow-peer split-update-group dynamic is disabled

	Sent	Rcvd
Prefix activity:	----	----
Prefixes Current:	2	11 (Consumes 572 bytes)
Prefixes Total:	4	19
Implicit Withdraw:	2	6
Explicit Withdraw:	0	2
Used as bestpath:	n/a	7
Used as multipath:	n/a	0

	Outbound	Inbound
Local Policy Denied Prefixes:	-----	-----
NEXT_HOP is us:	n/a	1
Bestpath from this peer:	20	n/a
Bestpath from iBGP peer:	8	n/a
Invalid Path:	10	n/a
Total:	38	1

Number of NLRI in the update sent: max 2, min 0

Last detected as dynamic slow peer: never

Dynamic slow peer recovered: never

For address family: L2VPN Vpls

Session: 10.1.1.3

BGP table version 8, neighbor version 8/0

Output queue size : 0

Index 1, Advertise bit 0

1 update-group member

Slow-peer detection is disabled

Slow-peer split-update-group dynamic is disabled

	Sent	Rcvd
Prefix activity:	----	----
Prefixes Current:	1	1 (Consumes 68 bytes)
Prefixes Total:	2	1
Implicit Withdraw:	1	0
Explicit Withdraw:	0	0
Used as bestpath:	n/a	1
Used as multipath:	n/a	0

	Outbound	Inbound
Local Policy Denied Prefixes:	-----	-----
Bestpath from this peer:	4	n/a

show ip bgp neighbors

```

      Bestpath from iBGP peer:          1          n/a
      Invalid Path:                    2          n/a
      Total:                            7          0
Number of NLRI in the update sent: max 1, min 0
Last detected as dynamic slow peer: never
Dynamic slow peer recovered: never
Address tracking is enabled, the RIB does have a route to 10.1.1.3
Connections established 1; dropped 0
Last reset never
Transport(tcp) path-mtu-discovery is enabled
Graceful-Restart is enabled, restart-time 120 seconds, stalepath-time 360 seconds
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Minimum incoming TTL 0, Outgoing TTL 255
Local host: 10.1.1.1, Local port: 179
Foreign host: 10.1.1.3, Foreign port: 48485
Connection tableid (VRF): 0
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0xE750C):
Timer           Starts      Wakeups          Next
Retrans         18          0             0x0
TimeWait        0           0             0x0
AckHold         22          20            0x0
SendWnd         0           0             0x0
KeepAlive       0           0             0x0
GiveUp          0           0             0x0
PmtuAger        0           0             0x0
DeadWait        0           0             0x0
Linger          0           0             0x0
iss: 3196633674  snduna: 3196634254  sndnxt: 3196634254  sndwnd: 15805
irs: 1633793063  rcvnxt: 1633794411  rcvwnd: 15037  delrcvwnd: 1347
SRTT: 273 ms, RTTO: 490 ms, RTV: 217 ms, KRTT: 0 ms
minRTT: 2 ms, maxRTT: 300 ms, ACK hold: 200 ms
Status Flags: passive open, gen tcbs
Option Flags: nagle, path mtu capable
Datagrams (max data segment is 1436 bytes):
Rcvd: 42 (out of order: 0), with data: 24, total data bytes: 1347
Sent: 40 (retransmit: 0 fastretransmit: 0),with data: 19, total data bytes: 579

```

Examples

The following is sample output from the **show ip bgp neighbors** command that indicates the discard attribute values and treat-as-withdraw attribute values configured. It also provides a count of received Updates matching a treat-as-withdraw attribute, a count of received Updates matching a discard attribute, and a count of received malformed Updates that are treat-as-withdraw.

```

Device# show ip bgp vpnv4 all neighbors 10.0.103.1

BGP neighbor is 10.0.103.1, remote AS 100, internal link
  Path-attribute treat-as-withdraw inbound
  Path-attribute treat-as-withdraw value 128
  Path-attribute treat-as-withdraw 128 in: count 2
  Path-attribute discard 128 inbound
  Path-attribute discard 128 in: count 2

      Outbound      Inbound
Local Policy Denied Prefixes:  -----
MALFORM treat as withdraw:      0          1
Total:                          0          1

```

Examples

The following output indicates that the neighbor is capable of advertising additional paths and sending additional paths it receives. It is also capable of receiving additional paths and advertised paths.

```

Device# show ip bgp neighbors 10.108.50.2

BGP neighbor is 10.108.50.2, remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 00:24:25

```

Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is 60 seconds

Neighbor capabilities:
 Additional paths Send: advertised and received
 Additional paths Receive: advertised and received
 Route refresh: advertised and received(old & new)
 Graceful Restart Capabilty: advertised and received
 Address family IPv4 Unicast: advertised and received

Examples

In the following output, the cluster ID of the neighbor is displayed. (The vertical bar and letter “i” for “include” cause the device to display only lines that include the user's input after the “i”, in this case, “cluster-id.”) The cluster ID displayed is the one directly configured through a neighbor or a template.

Device# **show ip bgp neighbors 192.168.2.2 | i cluster-id**

Configured with the cluster-id 192.168.15.6

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
bgp enhanced-error	Restores the default behavior of treating Update messages that have a malformed attribute as withdrawn, or includes iBGP peers in the Enhanced Attribute Error Handling feature.
neighbor path-attribute discard	Configures the device to discard unwanted Update messages from the specified neighbor that contain a specified path attribute.
neighbor path-attribute treat-as-withdraw	Configures the device to withdraw from the specified neighbor unwanted Update messages that contain a specified attribute.
neighbor send-label	Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.
neighbor send-label explicit-null	Enables a BGP router to send MPLS labels with explicit-null information for a CSC-CE router and BGP routes to a neighboring CSC-PE router.
router bgp	Configures the BGP routing process.

show ip bgp path-attribute discard

To display all prefixes for which an attribute has been discarded, use the **show ip bgp path-attribute discard** command in user EXEC or privileged EXEC mode.

show ip bgp path-attribute discard

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Examples

The following is sample output from the **show ip bgp path-attribute discard** command:

```
Device# show ip bgp path-attribute discard
```

```
Network      Next Hop
2.1.1.1/32    192.168.101.2
```

The table below describes the significant fields shown in the display.

Table 62: show ip bgp path-attribute discard Field Descriptions

Field	Description
Network	Network address and prefix length of the prefix that had a path attribute discarded.
Next Hop	Address of the next hop toward that network.

Related Commands

Command	Description
neighbor path-attribute discard	Configures the device to discard specific path attributes from Update messages from the specified neighbor.

show ip bgp path-attribute unknown

To display all prefixes that have an unknown attribute, use the **show ip bgp path-attribute unknown** command in user EXEC or privileged EXEC mode.

show ip bgp path-attribute unknown

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC (>)
Privileged EXEC (#)

Command History	Release	Modification
	15.2(4)S	This command was introduced.
	Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
	15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Examples The following is sample output from the **show ip bgp path-attribute unknown** command:

```
Device# show ip bgp path-attribute unknown
```

```
Network      Next Hop
2.1.1.1/32    192.168.101.2
```

The table below describes the significant fields shown in the display.

Table 63: show ip bgp path-attribute unknown Field Descriptions

Field	Description
Network	Network address and prefix length of the prefix that had an unknown path attribute.
Next Hop	Address of the next hop toward that network.

show ip bgp paths

To display all the BGP paths in the database, use the **show ip bgp paths** command in EXEC mode.

show ip bgp paths

Cisco 10000 Series Router

show ip bgp paths *regex*

Syntax Description

<i>regex</i>	Regular expression to match the BGP autonomous system paths.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)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.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
12.2(33)SRE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.

Examples

The following is sample output from the **show ip bgp paths** command in privileged EXEC mode:

```
Router# show ip bgp paths

Address      Hash Refcount Metric Path
0x60E5742C   0      1      0 i
0x60E3D7AC   2      1      0 ?
0x60E5C6C0  11      3      0 10 ?
0x60E577B0  35      2      40 10 ?
```

The table below describes the significant fields shown in the display.

Table 64: show ip bgp paths Field Descriptions

Field	Description
Address	Internal address where the path is stored.
Hash	Hash bucket where path is stored.
Refcount	Number of routes using that path.
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The autonomous system path for that route, followed by the origin code for that route.

show ip bgp peer-group

To display information about BGP peer groups, use the **show ip bgp peer-group** command in user EXEC or privileged EXEC mode.

show ip bgp peer-group [*peer-group-name*] [summary]

Syntax Description

<i>peer-group-name</i>	(Optional) Displays information about a specific peer group.
summary	(Optional) Displays a summary of the status of all the members of a peer group.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)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, and the output was modified to support BGP dynamic neighbors.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S, with the modified output to support BGP dynamic neighbors.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S, with the modified output to support BGP dynamic neighbors.
15.2.(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Examples

The following is sample output from the **show ip bgp peer-group** command for a peer group named internal in privileged EXEC mode:

```
Router# show ip bgp peer-group internal
BGP peer-group is internal, remote AS 100
BGP version 4
Minimum time between advertisement runs is 5 seconds
```

```

For address family:IPv4 Unicast
BGP neighbor is internal, peer-group internal, members:
    10.1.1.1      10.1.1.2
Index 3, Offset 0, Mask 0x8
Incoming update AS path filter list is 53
Outgoing update AS path filter list is 54
Route map for incoming advertisements is MAP193
Route map for outgoing advertisements is MAP194
Update messages formatted 0, replicated 0

```

The following output from the **show ip bgp peer-group** command shows information about a configured listen range group, group192. In Cisco IOS Release 12.2(33)SXH, 15.0(1)S, and XE Release 3.1S and later releases, the BGP dynamic neighbor feature introduced the ability to support the dynamic creation of BGP neighbor peers using a subnet range associated with a peer group (listen range group).

```
Router# show ip bgp peer-group group192
```

```

BGP peer-group is group192, remote AS 40000
BGP peergroup group192 listen range group members:
  192.168.0.0/16
BGP version 4
Default minimum time between advertisement runs is 30 seconds
For address family: IPv4 Unicast
BGP neighbor is group192, peer-group external, members:
  *192.168.3.2
Index 0, Offset 0, Mask 0x0
Update messages formatted 0, replicated 0
Number of NLRIs in the update sent: max 0, min 0

```

show ip bgp quote-regexp

To display routes matching the autonomous system path regular expression, use the **show ip bgp quote-regexp** command in privileged EXEC mode.

show ip bgp quote-regexp *regexp*

Syntax Description

<i>regexp</i>	The regular expression to match the Border Gateway Protocol (BGP) autonomous system paths. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the router bgp command. Note The regular expression has to be an exact match.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
12.2(33)SRE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(1)SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain--65538 for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot--1.2 for example--as the only configuration format, regular expression match, and output display, with no asplain support.

Examples

The following is sample output from the **show ip bgp quote-regex** command in EXEC mode:

```
Router# show ip bgp quote-regex "^10_" | begin 10.40
*> 10.40.0.0/20      10.10.10.10      0 10 2548 1239 10643 i
*> 10.40.16.0/20     10.10.10.10      0 10 2548 6172 i
*> 10.40.32.0/19     10.10.10.10      0 10 2548 6172 i
*> 10.41.0.0/19      10.10.10.10      0 10 2548 3356 3703 ?
```

```
*> 10.42.0.0/17      10.10.10.10                0 10 2548 6172 i
```

**Note**

Although the columns in the above display are not labeled, see the Field Descriptions table below for detailed information.

The table below describes the significant fields shown in the display from left to right.

Table 65: show ip bgp quote-regexp Field Descriptions

Field	Description
Status codes	Status of the table entry; for example, * in the above display. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened. h—The table entry history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session. r—The table entry failed to install in the routing table. S—The table entry is a stale route.
Network	IP address of a network entity; for example, 24.40.0.0/20 in the above display.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network; for example, 10.10.10.10. in the above display. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.; for example, 0 in the above display.
LocPrf	Local preference value as set with the set local-preference route-map configuration command; for example, 10 in the above display. The default value is 100.
Weight	Weight of the route as set via autonomous system filters; for example, 2548 in the above display.

Field	Description
Path	Autonomous system paths to the destination network; for example, 1239 in the above display. There can be one entry in this field for each autonomous system in the path.
Origin codes	Origin of the entry; for example, ? in the above display. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.

The following output from the **show ip bgp quote-regexp** command shows routes that match the quoted regular expression for the 4-byte autonomous system number 65550. The 4-byte autonomous system number is displayed in the default asplain format. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.0(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or a later release.

```
Router# show ip bgp quote-regexp "^65550$"
```

```
BGP table version is 4, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
*> 10.2.2.0/24    192.168.3.2             0         0 65550 i
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
router bgp	Configures the BGP routing process.
show ip bgp regexp	Displays routes matching the autonomous system path regular expression.

show ip bgp regexp

To display routes matching the autonomous system path regular expression, use the **show ip bgp regexp** command in EXEC mode.

show ip bgp regexp *regexp*

Syntax Description

<i>regexp</i>	Regular expression to match the BGP autonomous system paths. • In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. • In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. For more details about autonomous system number formats, see the router bgp command.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
12.2(33)SRE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(1)SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain--65538 for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot--1.2 for example--as the only configuration format, regular expression match, and output display, with no asplain support.

To ensure a smooth transition we recommend that all BGP speakers within an autonomous system that is identified using a 4-byte autonomous system number, are upgraded to support 4-byte autonomous system numbers.

Examples

The following is sample output from the **show ip bgp regexp** command in privileged EXEC mode:

```
Router# show ip bgp regexp 108$
```

```

BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
  Network          Next Hop          Metric LocPrf Weight Path
* 172.16.0.0        172.16.72.30              0 109 108 ?
* 172.16.1.0        172.16.72.30              0 109 108 ?
* 172.16.11.0       172.16.72.30              0 109 108 ?
* 172.16.14.0       172.16.72.30              0 109 108 ?
* 172.16.15.0       172.16.72.30              0 109 108 ?
* 172.16.16.0       172.16.72.30              0 109 108 ?
* 172.16.17.0       172.16.72.30              0 109 108 ?
* 172.16.18.0       172.16.72.30              0 109 108 ?
* 172.16.19.0       172.16.72.30              0 109 108 ?
* 172.16.24.0       172.16.72.30              0 109 108 ?
* 172.16.29.0       172.16.72.30              0 109 108 ?
* 172.16.30.0       172.16.72.30              0 109 108 ?
* 172.16.33.0       172.16.72.30              0 109 108 ?
* 172.16.35.0       172.16.72.30              0 109 108 ?
* 172.16.36.0       172.16.72.30              0 109 108 ?
* 172.16.37.0       172.16.72.30              0 109 108 ?
* 172.16.38.0       172.16.72.30              0 109 108 ?
* 172.16.39.0       172.16.72.30              0 109 108 ?

```

The following example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or a later release. After the **bgp asnotation dot** command is configured, the regular expression match format for 4-byte autonomous system paths is changed to asdot notation format. Although a 4-byte autonomous system number can be configured in a regular expression using either asplain or asdot format, only 4-byte autonomous system numbers configured using the current default format are matched. In the first example, the **show ip bgp regexp** command is configured with a 4-byte autonomous system number in asplain format. The match fails because the default format is currently asdot format and there is no output. In the second example using asdot format, the match passes and the information about the 4-byte autonomous system path is shown using the asdot notation.

**Note**

The asdot notation uses a period which is a special character in Cisco regular expressions. to remove the special meaning, use a backslash before the period.

```

Router# show ip bgp regexp ^65536$

Router# show ip bgp regexp ^1\.0$

BGP table version is 2, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
  Network          Next Hop          Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.0 i

```

The following is sample output from the **show ip bgp regexp** command after the **bgp asnotation dot** command has been entered to display 4-byte autonomous system numbers in dot notation in Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or later release. The dot notation is the only format for 4-byte autonomous system numbers in Cisco IOS Release 12.0(32)S12, 12.4(24)T, or Cisco IOS XE Release 2.3.

**Note**

The asdot notation uses a period which is a special character in Cisco regular expressions. to remove the special meaning, use a backslash before the period.

```

Router# show ip bgp regexp ^1\.14$

```

```

BGP table version is 4, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network        Next Hop           Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2             0             0 1.14   i

```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
router bgp	Configures the BGP routing process.
show ip bgp quote-regexp	Displays routes matching the autonomous system path regular expression.

show ip bgp replication

To display update replication statistics for Border Gateway Protocol (BGP) update groups, use the **show ip bgp replication** command in EXEC mode.

show ip bgp replication [*index-group*| *ip-address*]

Syntax Description

<i>index-group</i>	(Optional) Displays update replication statistics for the update group with the corresponding index number. The range of update-group index numbers is from 1 to 4294967295.
<i>ip-address</i>	(Optional) Displays update replication statistics for this neighbor.

Command Modes

EXEC

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
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.
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 output of this command displays BGP update-group replication statistics.

When a change to outbound policy occurs, the router automatically recalculates update-group memberships and applies the changes by triggering an outbound soft reset after a 3-minute timer expires. This behavior is designed to provide the network operator with time to change the configuration if a mistake is made. You can manually enable an outbound soft reset before the timer expires by entering the **clear ip bgp ip-address soft out** command.

Examples

The following sample output from the **show ip bgp replication** command shows update-group replication information for all neighbors:

```
Router# show ip bgp replication
```

```
BGP Total Messages Formatted/Enqueued : 0/0
  Index      Type  Members      Leader    MsgFmt  MsgRepl  Csize  Qsize
    1 internal      1    10.4.9.21      0        0      0      0
    2 internal      2    10.4.9.5       0        0      0      0
```

The following sample output from the **show ip bgp replication** command shows update-group statistics for the 10.4.9.5 neighbor:

```
Router# show ip bgp replication 10.4.9.5
```

```
  Index      Type  Members      Leader    MsgFmt  MsgRepl  Csize  Qsize
    2 internal      2    10.4.9.5       0        0      0      0
```

The table below describes the significant fields shown in the display.

Table 66: show ip bgp replication Field Descriptions

Field	Description
Index	Index number of the update group.
Type	Type of peer (internal or external).
Members	Number of members in the dynamic update peer group.
Leader	First member of the dynamic update peer group.

Related Commands

Command	Description
clear ip bgp	Resets a BGP connection or session.
clear ip bgp update-group	Clears BGP update-group member sessions.
debug ip bgp groups	Displays information related to the processing of BGP update groups.
show ip bgp peer-group	Displays information about BGP update groups.

show ip bgp rib-failure

To display Border Gateway Protocol (BGP) routes that failed to install in the Routing Information Base (RIB) table, use the **show ip bgp rib-failure** command in privileged EXEC mode.

show ip bgp rib-failure

Syntax Description This command has no keywords or arguments.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.3	This command was introduced.
	12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
	12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
	12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples The following is sample output from the **show ip bgp rib-failure** command:

Router# **show ip bgp rib-failure**

Network	Next Hop	RIB-failure	RIB-NH	Matches
10.1.15.0/24	10.1.35.5	Higher admin distance		n/a
10.1.16.0/24	10.1.15.1	Higher admin distance		n/a

The table below describes the significant fields shown in the display.

Table 67: show ip bgp rib-failure Field Descriptions

Field	Description
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.

Field	Description
RIB-failure	Cause of RIB failure. Higher admin distance means that a route with a better (lower) administrative distance such as a static route already exists in the IP routing table.
RIB-NH Matches	Route status that applies only when Higher admin distance appears in the RIB-failure column and bgp suppress-inactive is configured for the address family being used. There are three choices: • Yes—Means that the route in the RIB has the same next hop as the BGP route or next hop recurses down to the same adjacency as the BGP nexthop. • No—Means that the next hop in the RIB recurses down differently from the next hop of the BGP route. • n/a—Means that bgp suppress-inactive is not configured for the address family being used.

Related Commands

Command	Description
bgp suppress-inactive	Configures a router to suppress the advertisement of BGP routes that are not installed in the RIB and FIB tables.
clear ip bgp	Resets a BGP connection or session.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

show ip bgp rpki servers

To display the current state of communication with the Resource Public Key Infrastructure (RPKI) cache servers, use the **show ip bgp rpki servers** command in user EXEC or privileged EXEC mode.

show ip bgp rpki servers

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC (>)
Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Release 3.5S	This command was introduced.
	15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.
	15.2(4)S	This command was implemented on the Cisco 7200 series routers.

Usage Guidelines This command is useful after configuring the **bgp rpki server** command.

Examples The following is sample output from the **show ip bgp rpki servers** command:

```
Router# show ip bgp rpki servers

BGP SOVC neighbor is 10.0.96.254 connected to port 32000
Flags 0, Refresh time is 5, Serial number is 1
InQ has 0 messages, OutQ has 0 messages, formatted msg 9
Session IO flags 0, Session flags 10000008
Neighbor Statistics:
  Nets Processed 13

Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Minimum incoming TTL 0, Outgoing TTL 255
Local host: 10.0.96.2, Local port: 56238
Foreign host: 10.0.96.254, Foreign port: 32000
Connection tableid (VRF): 0

Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0xCD931):
Timer           Starts      Wakeups      Next
Retrans         10          0           0x0
TimeWait        0           0           0x0
AckHold         9           9           0x0
SendWnd         0           0           0x0
KeepAlive       0           0           0x0
GiveUp          0           0           0x0
PmtuAger        1           0           0x1554E6
```

show ip bgp rpki servers

```

DeadWait          0          0          0x0
Linger            0          0          0x0

iss: 1144343423  snduna: 1144343528  sndnxt: 1144343528  sndwnd: 5840
irs: 2151800169  rcvnxt: 2151800610  rcvwnd: 15944  delrcvwnd: 440

SRTT: 221 ms, RTTO: 832 ms, RTV: 611 ms, KRTT: 0 ms
minRTT: 3 ms, maxRTT: 300 ms, ACK hold: 200 ms
Status Flags: none
Option Flags: higher precedence, nagle, path mtu capable

Datagrams (max data segment is 1460 bytes):
Rcvd: 11 (out of order: 0), with data: 9, total data bytes: 440
Sent: 20 (retransmit: 0 fastretransmit: 0),with data: 9, total data bytes: 104

```

Related Commands

Command	Description
bgp rpki server	Connects to an RPKI server and enables the validation of BGP prefixes based on the AS from which the prefix originates.
neighbor announce rpki state	Sends and receives the RPKI status and prefix/AS pairs to and from an IBGP neighbor.

show ip bgp rpki table

To display the currently cached list of networks and associated autonomous system (AS) numbers received from the Resource Public Key Infrastructure (RPKI) server, use the **show ip bgp rpki table** command in user EXEC or privileged EXEC mode.

show ip bgp [ipv6 unicast] rpki table

Syntax Description

ipv6 unicast	(Optional) Displays only the IPv6 prefixes.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(1)S	This command was integrated into Cisco IOS Release 15.2(1)S.
15.2(4)S	This command was implemented on the Cisco 7200 series routers.

Usage Guidelines

This command is useful after configuring the **bgp rpki server** command to see the list of networks and corresponding AS numbers received from the RPKI server.

Examples

The following is sample output from the **show ip bgp rpki table** command:

```
Router# show ip bgp rpki table
12 BGP sovc network entries using 1056 bytes of memory
13 BGP sovc record entries using 260 bytes of memory

Network          Maxlen  Origin-AS  Source  Neighbor
1.1.0.0/16       24      1          0       10.0.96.254
3.0.0.0/24       24      2          0       10.0.96.254
4.0.0.0/24       24      3          0       10.0.96.254
4.0.0.0/8        8       3          0       10.0.96.254
5.0.0.0/24       24      4          0       10.0.96.254
8.0.0.0/4        6       200        0       10.0.96.254
8.2.0.0/8        24      36394      0       10.0.96.254
9.2.0.0/16       24      34000      0       10.0.96.254
10.0.0.0/6       8       100        0       10.0.96.254
```

The table below describes the significant fields shown in the display.

Table 68: show ip bgp rpki table Field Descriptions

Field	Description
Network	Prefix and mask length received from RPKI server.
Maxlen	Limit on the prefix length of the corresponding network (the value is provided by the server).
Origin-AS	Number of the AS from which the prefix originated.
Source	Value is always 0.
Neighbor	IP address of the RPKI cache server from which the record came.

Related Commands

Command	Description
bgp rpki server	Connects to an RPKI server and enables the validation of BGP prefixes based on the AS from which the prefix originates.
neighbor announce rpki state	Sends and receives the RPKI status and prefix/AS pairs to and from an IBGP neighbor.

show ip bgp rtfilter

To display information about BGP route target (RT) filtering, use the **show ip bgp rtfilter** command in user EXEC or privileged EXEC mode.

```
show ip bgp rtfilter {all | default | rt {ASN| ip-address} :nn}
```

Syntax Description

all	Displays RT information for all VPNs.
default	Displays the default RT filter.
rt	Displays a specific RT filter prefix.
<i>ASN:nn</i>	Autonomous system number, followed by a colon and number.
<i>ip-address:nn</i>	IP address, followed by a colon and a number.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(1)S	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use this command if you have configured the BGP: RT Constrained Route Distribution feature and you want to display RT filter information.



Note

If you enter the **all** keyword, many more optional keywords are available that are not shown here.

Examples

The following is sample output from the **show ip bgp rtfilter all** command:

```
Router# show ip bgp rtfilter all

BGP table version is 14, local router ID is 192.168.7.7
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f RT-Filter
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network Next Hop Metric LocPrf Weight Path
*>i0:0:0:0 192.168.2.2 0 100 0 i
*>i1:2:1:100 192.168.6.6 0 100 0 i
* i1:2:3:3 192.168.2.2 0 100 0 i
*> 0.0.0.0 32768 i
*>i1:2:150:1 192.168.6.6 0 100 0 i
* i1:2:200:200 192.168.2.2 0 100 0 i
*> 0.0.0.0 32768 i
```

The table below describes the fields shown in the display.

Table 69: show ip bgp rtfilter Field Descriptions

Field	Description
Network	RT filter prefix.
Next Hop	Next hop in the RT filter prefix.
Metric	BGP metric associated with the RT filter prefix.
LocPrf	BGP local preference.
Weight	BGP weight.
Path	Path information associated with the RT prefix.

The following is sample output from the **show ip bgp rtfilter all summary** command:

```
Router# show ip bgp rtfilter all summary

BGP router identifier 192.168.7.7, local AS number 1
BGP table version is 14, main routing table version 14
5 network entries using 820 bytes of memory
7 path entries using 336 bytes of memory
2/2 BGP path/bestpath attribute entries using 256 bytes of memory
1 BGP rrinfo entries using 24 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1484 total bytes of memory
BGP activity 7/0 prefixes, 14/5 paths, scan interval 60 secs
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
192.168.2.2 4 1 13 12 14 0 0 00:03:21 5
```

Related Commands

Command	Description
address-family rtfilter unicast	Enters address family configuration mode and enables Automated Route Target Filtering with a BGP peer.
neighbor default-originate	Allows a BGP speaker (the local router) to send the default route 0:0:0:0 to a neighbor for use as a default route.
show ip bgp rtfilter all summary	Displays summary information about RT filtering.

show ip bgp summary

To display the status of all Border Gateway Protocol (BGP) connections, use the **show ip bgp summary** command in user EXEC or privileged EXEC mode.

show ip bgp [**ipv4** {**multicast**|**unicast**}|**vpn4 all**|**vpn6 unicast all**|**topology** {*****|*routing-topology-instance-name*}] [**update-group**] **summary** [**slow**]

Syntax Description

ipv4 { multicast unicast }	(Optional) Displays peers in the IPv4 address family.
vpn4 all	(Optional) Displays peers in the VPNv4 address family.
vpn6 unicast all	(Optional) Displays peers in the VPNv6 address family.
topology	(Optional) Displays routing topology information.
*	(Optional) Displays all routing topology instances.
<i>routing-topology-instance-name</i>	(Optional) Displays routing topology information for that instance.
update-group	(Optional) Includes information about the update group of the peers.
slow	(Optional) Displays only information about dynamically configured slow peers.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0	Support for the neighbor maximum-prefix command was added to the output.
12.2	This command was modified. - The number of networks and paths displayed in the output was split out to two separate lines. - A field was added to display multipath entries in the routing table.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was modified. A line was added to the output to display the advertised bitfield cache entries and associated memory usage.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH, and the output was modified to support BGP dynamic neighbors.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
Cisco IOS XE Release 2.3	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
12.2(33)SRE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)S	This command was modified. The slow keyword was added.
Cisco IOS XE Release 3.1S	This command was modified. The slow keyword was added.
15.2(1)S	This command was modified. It will show information about how many paths are in each RPKI state.
Cisco IOS XE Release 3.5S	This command was modified. It will show information about how many paths are in each RPKI state.
15.1(1)SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.

Release	Modification
Cisco IOS XE Release 3.3SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
15.2(4)S	This command was implemented on the Cisco 7200 series routers.

Usage Guidelines

The **show ip bgp summary** command is used to display BGP path, prefix, and attribute information for all connections to BGP neighbors.

A prefix is an IP address and network mask. It can represent an entire network, a subset of a network, or a single host route. A path is a route to a given destination. By default, BGP will install only a single path for each destination. If multipath routes are configured, BGP will install a path entry for each multipath route, and only one multipath route will be marked as the bestpath.

BGP attribute and cache entries are displayed individually and in combinations that affect the bestpath selection process. The fields for this output are displayed when the related BGP feature is configured or attribute is received. Memory usage is displayed in bytes.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot—1.2 for example—as the only configuration format, regular expression match, and output display, with no asplain support.

Examples

The following is sample output from the **show ip bgp summary** command in privileged EXEC mode:

```
Router# show ip bgp summary

BGP router identifier 172.16.1.1, local AS number 100
BGP table version is 199, main routing table version 199
37 network entries using 2850 bytes of memory
59 path entries using 5713 bytes of memory
18 BGP path attribute entries using 936 bytes of memory
2 multipath network entries and 4 multipath paths
10 BGP AS-PATH entries using 240 bytes of memory
7 BGP community entries using 168 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
90 BGP advertise-bit cache entries using 1784 bytes of memory
36 received paths for inbound soft reconfiguration
BGP using 34249 total bytes of memory
Dampening enabled. 4 history paths, 0 dampened paths
BGP activity 37/2849 prefixes, 60/1 paths, scan interval 15 secs

Neighbor      V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
10.100.1.1    4    200     26      22      199   0    0 00:14:23 23
10.200.1.1    4    300     21      51      199   0    0 00:13:40 0
```

The table below describes the significant fields shown in the display. Fields that are preceded by the asterisk (*) are not shown in the above output.

Table 70: show ip bgp summary Field Descriptions

Field	Description
BGP router identifier	In order of precedence and availability, the router identifier specified by the bgp router-id command, a loopback address, or the highest IP address.
BGP table version	Internal version number of BGP database.
main routing table version	Last version of BGP database that was injected into the main routing table.
...network entries	Number of unique prefix entries in the BGP database.
...using ... bytes of memory	Amount of memory, in bytes, that is consumed for the path, prefix, or attribute entry displayed on the same line.
...path entries using	Number of path entries in the BGP database. Only a single path entry will be installed for a given destination. If multipath routes are configured, a path entry will be installed for each multipath route.
...multipath network entries using	Number of multipath entries installed for a given destination.
* ...BGP path/bestpath attribute entries using	Number of unique BGP attribute combinations for which a path is selected as the bestpath.
* ...BGP rrinfo entries using	Number of unique ORIGINATOR and CLUSTER_LIST attribute combinations.
...BGP AS-PATH entries using	Number of unique AS_PATH entries.
...BGP community entries using	Number of unique BGP community attribute combinations.
*...BGP extended community entries using	Number of unique extended community attribute combinations.
BGP route-map cache entries using	Number of BGP route-map match and set clause combinations. A value of 0 indicates that the route cache is empty.
...BGP filter-list cache entries using	Number of filter-list entries that match an AS-path access list permit or deny statements. A value of 0 indicates that the filter-list cache is empty.

Field	Description
BGP advertise-bit cache entries using	(Cisco IOS Release 12.4(11)T and later releases only) Number of advertised bitfield entries and the associated memory usage. A bitfield entry represents a piece of information (one bit) that is generated when a prefix is advertised to a peer. The advertised bit cache is built dynamically when required.
...received paths for inbound soft reconfiguration	Number paths received and stored for inbound soft reconfiguration.
BGP using...	Total amount of memory, in bytes, used by the BGP process.
Dampening enabled...	Indicates that BGP dampening is enabled. The number of paths that carry an accumulated penalty and the number of dampened paths are displayed on this line.
BGP activity...	Displays the number of times that memory has been allocated or released for a path or prefix.
Neighbor	IP address of the neighbor.
V	BGP version number spoken to the neighbor.
AS	Autonomous system number.
MsgRcvd	Number of messages received from the neighbor.
MsgSent	Number of messages sent to the neighbor.
TblVer	Last version of the BGP database that was sent to the neighbor.
InQ	Number of messages queued to be processed from the neighbor.
OutQ	Number of messages queued to be sent to the neighbor.
Up/Down	The length of time that the BGP session has been in the Established state, or the current status if not in the Established state.

Field	Description
State/PfxRcd	Current state of the BGP session, and the number of prefixes that have been received from a neighbor or peer group. When the maximum number (as set by the neighbor maximum-prefix command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is set to Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the neighbor shutdown command.

The following output from the **show ip bgp summary** command shows that the BGP neighbor 192.168.3.2 was dynamically created and is a member of the listen range group, group192. The output also shows that the IP prefix range of 192.168.0.0/16 is defined for the listen range group named group192. In Cisco IOS Release 12.2(33)SXH and later releases, the BGP dynamic neighbor feature introduced the ability to support the dynamic creation of BGP neighbor peers using a subnet range associated with a peer group (listen range group).

Router# **show ip bgp summary**

```

BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1
Neighbor      V      AS MsgRcvd MsgSent   TblVer  InQ  OutQ Up/Down  State/PfxRcd
*192.168.3.2  4 50000      2        2        0    0    0 00:00:37      0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1
BGP peer group group192 listen range group members:
  192.168.0.0/16

```

The following output from the **show ip bgp summary** command shows two BGP neighbors, 192.168.1.2 and 192.168.3.2, in different 4-byte autonomous system numbers, 65536 and 65550. The local autonomous system 65538 is also a 4-byte autonomous system number and the numbers are displayed in the default asplain format. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or a later release.

Router# **show ip bgp summary**

```

BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1
Neighbor      V      AS MsgRcvd MsgSent   TblVer  InQ  OutQ Up/Down  Statd
192.168.1.2    4      65536      7        7        1    0    0 00:03:04      0
192.168.3.2    4      65550      4        4        1    0    0 00:00:15      0

```

The following output from the **show ip bgp summary** command shows the same two BGP neighbors, but the 4-byte autonomous system numbers are displayed in asdot notation format. To change the display format the **bgp asnotation dot** command must be configured in router configuration mode. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(32)S12, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, 12.4(24)T, or Cisco IOS XE Release 2.3 or later releases.

Router# **show ip bgp summary**

```

BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1
Neighbor      V      AS MsgRcvd MsgSent   TblVer  InQ  OutQ Up/Down  Statd
192.168.1.2    4        1.0      9        9        1    0    0 00:04:13      0
192.168.3.2    4        1.14      6        6        1    0    0 00:01:24      0

```

The following example displays sample output of the **show ip bgp summary slow** command:

```
Router# show ip bgp summary slow
```

```
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 37, main routing table version 37
36 network entries using 4608 bytes of memory
36 path entries using 1872 bytes of memory
1/1 BGP path/bestpath attribute entries using 124 bytes of memory
1 BGP rrinfo entries using 24 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 6700 total bytes of memory
BGP activity 46/0 prefixes, 48/0 paths, scan interval 60 secs
Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
6.6.6.6 4 100 11 10 1 0 0 00:44:20 0
```

The following example displays counts of prefix/AS pairs for each RPKI state. The fourth line of output indicates "Path RPKI states: x valid, x not found, x invalid." Of course the line of output indicating RPKI states can be displayed only if the **bgp rpki server** command or the **neighbor announce rpki state** command is configured.

```
Router> show ip bgp summary
```

```
For address family: IPv4 Unicast
BGP router identifier 10.0.96.2, local AS number 2
BGP table version is 8, main routing table version 8
Path RPKI states: 0 valid, 7 not found, 0 invalid
6 network entries using 888 bytes of memory
7 path entries using 448 bytes of memory
3/3 BGP path/bestpath attribute entries using 384 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1768 total bytes of memory
BGP activity 12/0 prefixes, 14/0 paths, scan interval 60 secs

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State
/PfxRcd
10.0.0.3      4        3      6      9        8    0    0 00:01:04
3
10.0.2.4      4        2      5      8        8    0    0 00:01:15
0
10.0.3.5      4        4      6      7        8    0    0 00:01:14
3
10.0.96.254   4        1      0      0        1    0    0 never    Idle
```

```
For address family: IPv6 Unicast
BGP router identifier 10.0.96.2, local AS number 2
BGP table version is 9, main routing table version 9
Path RPKI states: 3 valid, 4 not found, 0 invalid
6 network entries using 1032 bytes of memory
7 path entries using 616 bytes of memory
5/5 BGP path/bestpath attribute entries using 640 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2336 total bytes of memory
BGP activity 12/0 prefixes, 14/0 paths, scan interval 60 secs

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ OutQ Up/Down  State
/PfxRcd
2001::2       4        2      6      9        6    0    0 00:01:08
2
2002::1       4        3      7     11        9    0    0 00:01:07
2
2003::2       4        4      6      8        9    0    0 00:01:08
```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
bgp router-id	Configures a fixed router ID for the local BGP routing process.
neighbor maximum-prefix	Controls how many prefixes can be received from a BGP neighbor.
neighbor shutdown	Disables a BGP neighbor or peer group.
neighbor slow-peer split-update-group dynamic	Causes a dynamically detected slow peer to be moved to a slow update group.
router bgp	Configures the BGP routing process.

show ip bgp template peer-policy

To display locally configured peer policy templates, use the **show ip bgp template peer-policy** command in user EXEC or privileged EXEC mode.

show ip bgp template peer-policy [*policy-template-name* [**detail**]]

Syntax Description

<i>policy-template-name</i>	(Optional) Name of a locally configured peer policy template.
detail	(Optional) Displays detailed policy information such as route maps, prefix lists, community lists, access control lists (ACLs), and AS-path filter lists.

Command Default

If a peer policy template is not specified using the *policy-template-name* argument, all peer policy templates will be displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.0(25)S	The detail keyword was added.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.4(11)T	Support for the detail keyword was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SRB	This command and support for the detail keyword were 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.

Release	Modification
12.2(33)SB	Support for the detail keyword was integrated into Cisco IOS Release 12.2(33)SB.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

This command is used to display locally configured peer policy templates. The output can be filtered to display a single peer policy template using the *policy-template-name* argument. This command also supports all standard output modifiers.

When BGP neighbors use multiple levels of peer templates it can be difficult to determine which policies are associated with a specific template. In Cisco IOS Release 12.0(25)S, 12.4(11)T, 12.2(33)SRB, 12.2(33)SB, and later releases, the **detail** keyword was added to display the detailed configuration of local and inherited policies associated with a specific template. Inherited policies are policies that the template inherits from other peer-policy templates.

Examples

The **show ip bgp template peer-policy** command is used to verify the configuration of local peer policy templates. The following sample output shows the peer policy templates named GLOBAL and NETWORK1. The output also shows that the GLOBAL template was inherited by the NETWORK1 template.

```
Device# show ip bgp template peer-policy

Template:GLOBAL, index:1.
Local policies:0x80840, Inherited polices:0x0
  *Inherited by Template NETWORK1, index:2
Locally configured policies:
  prefix-list NO-MARKETING in
  weight 300
  maximum-prefix 10000
Inherited policies:
Template:NETWORK1, index:2.
Local policies:0x1, Inherited polices:0x80840
This template inherits:
  GLOBAL, index:1, seq_no:10, flags:0x1
Locally configured policies:
  route-map ROUTE in
Inherited policies:
  prefix-list NO-MARKETING in
  weight 300
  maximum-prefix 10000
```

The table below describes the significant fields shown in the display.

Table 71: show ip bgp template peer-policy Field Descriptions

Field	Description
Template	Name of the peer template.
index	The sequence number in which the displayed template is processed.
Local policies	Displays the hexadecimal value of locally configured policies.

Field	Description
Inherited polices	Displays the hexadecimal value of inherited policies. The 0x0 value is displayed when no templates are inherited.
Locally configured policies	Displays a list of commands that are locally configured in a peer policy template.
Inherited policies	Displays a list of commands that are inherited from a peer template.

The following sample output of the **show ip bgp template peer-policy** command with the **detail** keyword displays details of the template named NETWORK1, which includes the inherited template named GLOBAL. The output in this example displays the configuration commands of the locally configured route map and prefix list and the inherited prefix list.

```
Device# show ip bgp template peer-policy NETWORK1 detail
```

```
Template:NETWORK1, index:2.
Local policies:0x1, Inherited policies:0x80840
This template inherits:
  GLOBAL, index:1, seq_no:10, flags:0x1
Locally configured policies:
  route-map ROUTE in
Inherited policies:
  prefix-list NO-MARKETING in
  weight 300
  maximum-prefix 10000
Template:NETWORK1 <detail>
Locally configured policies:
  route-map ROUTE in
route-map ROUTE, permit, sequence 10
  Match clauses:
    ip address prefix-lists: DEFAULT
ip prefix-list DEFAULT: 1 entries
  seq 5 permit 10.1.1.0/24
  Set clauses:
    Policy routing matches: 0 packets, 0 bytes
Inherited policies:
  prefix-list NO-MARKETING in
ip prefix-list NO-MARKETING: 1 entries
  seq 5 deny 10.2.2.0/24
```

Related Commands

Command	Description
inherit peer-policy	Configures a peer policy template to inherit the configuration from another peer policy template.
template peer-policy	Creates a peer policy template and enters policy-template configuration mode.

show ip bgp template peer-session

To display peer policy template configurations, use the **show ip bgp template peer-session** command in user EXEC or privileged EXEC mode.

show ip bgp template peer-session [*session-template-name*]

Syntax Description

<i>session-template-name</i>	(Optional) Name of a locally configured peer session template.

Command Default

If a peer session template is not specified with the *session-template-name* argument, all peer session templates will be displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
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.
Cisco IOS XE Release 3.8S	This command was modified. The cluster ID for the template is displayed.

Usage Guidelines

This command is used to display locally configured peer session templates. The output can be filtered to display a single peer session template with the *peer-session-name* argument. This command also supports all standard output modifiers.

Examples

The **show ip bgp template peer-session** command is used to verify the configuration of local peer session templates. The following example shows the peer session templates named INTERNAL-BGP and CORE1. The output also shows that INTERNAL-BGP is inherited by CORE1.

```
Device# show ip bgp template peer-session

Template:INTERNAL-BGP, index:1
Local policies:0x21, Inherited policies:0x0
  *Inherited by Template CORE1, index= 2
Locally configured session commands:
  remote-as 202
  timers 30 300
Inherited session commands:
Template:CORE1, index:2
Local policies:0x180, Inherited policies:0x21
This template inherits:
  INTERNAL-BGP index:1 flags:0x0
Locally configured session commands:
  update-source loopback 1
  description CORE-123
Inherited session commands:
  remote-as 202
  timers 30 300
```

The table below describes the significant fields shown in the display.

Table 72: show ip bgp template peer-session Field Descriptions

Field	Description
Template:	Name of the peer template.
index:	The sequence number in which the displayed template is processed.
Local policies:	Displays the hexadecimal value of locally configured policies.
Inherited policies:	Displays the hexadecimal value of inherited policies. The 0x0 value is displayed when no templates are inherited.
Locally configured session commands:	Displays a list of commands that are locally configured in a peer template.
Inherited session commands:	Displays a list of commands that are inherited from a peer session template.

The following sample output displays the cluster ID assigned to the template:

```
Device# show ip bgp template peer-session TS1

Template:TS1, index:1
Local policies:0x10000000, Inherited policies:0x0
Locally configured session commands:
```

```
cluster-id 192.168.0.115
Inherited session commands:
```

Related Commands

Command	Description
bgp cluster-id	Sets the global cluster ID on a route reflector.
inherit peer-session	Configures a peer session template to inherit the configuration from another peer session template.
neighbor cluster-id	Sets the cluster ID for a neighbor.
template peer-session	Creates a peer session template and enters session-template configuration mode.

show ip bgp unicast route-server

To display on a BGP route server which paths are chosen for a route server context, in particular if the normal bestpath was overridden or suppressed, use the **show ip bgp unicast route-server** command in privileged EXEC mode.

show ip bgp {ipv4|ipv6} unicast route-server {all|context *context-name*} [summary]

Syntax Description

ipv4	Displays only IPv4 prefixes.
ipv6	Displays only IPv6 prefixes.
all	Displays information for all route server contexts.
context <i>context-name</i>	Displays information for the specified route server context only.
summary	(Optional) Displays the neighbor state for route server clients.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE 3.3S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

Use this command on a BGP route server to see the next hop to network prefixes and additional information about the path.

Examples

The following output displays all the routes chosen by the policy for the context named example-context:

```
Route-Server# show ip bgp ipv4 unicast route-server context example-context
```

```
Networks for route server context example-context:
  Network      Next Hop      Metric LocPrf Weight Path
*  1.1.1.1/32   10.10.10.22    123             0 22 ?
*  1.1.2.0/24   10.10.10.22    123             0 22 ?
*  1.3.0.0/16   10.10.10.22    123             0 22 ?
*  8.8.0.0/16   10.10.10.22    123             0 22 ?
    100.100.100.21/32 (suppressed)
*> 100.100.100.22/32 10.10.10.22    123             0 22 ?
*  100.100.100.23/32 10.10.10.23    123             0 23 ?
```

```
*> 100.100.100.24/32 10.10.10.24      123      0 24 ?
*> 100.100.100.25/32 10.10.10.25      123      0 25 ?
*> 100.100.100.26/32 10.10.10.26      123      0 26 ?
```

Three types of routes can be in a context, as shown in the preceding output. They are:

- Those where the policy for the context chooses the same path as the regular BGP best path algorithm (for example, 100.100.100.25/32, denoted by ">").
- Those where the policy for the context excluded the regular best path, but found a suitable alternative path to advertise to the client (for example, 1.1.1.1/32, not denoted with ">", but still valid "*").
- Those where the policy for the context excluded all available paths and therefore those routes will not be sent to the client; for example, 100.100.100.21/32, denoted by "(suppressed)".

In the following example, specifying **all** instead of a specific context reveals that different contexts may have differing routes due to the configured policy:

```
Route-Server# show ip bgp ipv4 unicast route-server all

Networks for route server context all-base:
  Network      Next Hop      Metric LocPrf Weight Path
*> 1.1.1.1/32   10.10.10.21    23      0 21 ?
*> 1.1.2.0/24   10.10.10.21    23      0 21 ?
*> 1.3.0.0/16   10.10.10.21    23      0 21 ?
*> 8.8.0.0/16   10.10.10.21    23      0 21 ?
*> 100.100.100.21/32 10.10.10.21    23      0 21 ?
*> 100.100.100.22/32 10.10.10.22    123     0 22 ?
*> 100.100.100.23/32 10.10.10.21    23      0 21 ?
* 100.100.100.24/32 10.10.10.24    123     0 24 ?
*> 100.100.100.25/32 10.10.10.25    123     0 25 ?
*> 100.100.100.26/32 10.10.10.26    123     0 26 ?

Networks for route server context all-policy-deny:
  Network      Next Hop      Metric LocPrf Weight Path
1.1.1.1/32     (suppressed)
1.1.2.0/24     (suppressed)
1.3.0.0/16     (suppressed)
8.8.0.0/16     (suppressed)
100.100.100.21/32 (suppressed)
100.100.100.22/32 (suppressed)
100.100.100.23/32 (suppressed)
100.100.100.24/32 (suppressed)
100.100.100.25/32 (suppressed)
100.100.100.26/32 (suppressed)

Networks for route server context all-policy:
  Network      Next Hop      Metric LocPrf Weight Path
* 1.1.1.1/32   10.10.10.27    878     0 27 ?
* 1.1.2.0/24   10.10.10.27    878     0 27 ?
* 1.3.0.0/16   10.10.10.27    878     0 27 ?
* 8.8.0.0/16   10.10.10.27    878     0 27 ?
* 100.100.100.21/32 10.10.10.27    878     0 27 ?
* 100.100.100.22/32 10.10.10.27    878     0 27 ?
* 100.100.100.23/32 10.10.10.27    878     0 27 ?
* 100.100.100.24/32 10.10.10.27    878     0 27 ?
* 100.100.100.25/32 10.10.10.27    878     0 27 ?
* 100.100.100.26/32 10.10.10.27    878     0 27 ?

Networks for route server context example-context:
  Network      Next Hop      Metric LocPrf Weight Path
* 1.1.1.1/32   10.10.10.23    123     0 23 ?
* 1.1.2.0/24   10.10.10.23    123     0 23 ?
* 1.3.0.0/16   10.10.10.23    123     0 23 ?
* 8.8.0.0/16   10.10.10.23    123     0 23 ?
100.100.100.21/32 (suppressed)
*> 100.100.100.22/32 10.10.10.22    123     0 22 ?
* 100.100.100.23/32 10.10.10.23    123     0 23 ?
* 100.100.100.24/32 10.10.10.24    123     0 24 ?
*> 100.100.100.25/32 10.10.10.25    123     0 25 ?
*> 100.100.100.26/32 10.10.10.26    123     0 26 ?
```

In the following example, the **summary** keyword displays output similar to the **show ip bgp summary** command in that it shows the neighbor state for route server clients in the specified context (or all contexts):

```
Route-Server# show ip bgp ipv4 unicast route-server context example-context summary
```

```
Route server clients assigned to context example-context:
Neighbor      V   AS MsgRcvd MsgSent   TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.10.10.18    4   18     283     291     13    0    0  04:13:21      0
```

In the following example, the **all** keyword and the **summary** keyword display summary output for all contexts:

```
Route-Server# show ip bgp ipv4 unicast route-server all summary
```

```
Route server clients without assigned contexts:
Neighbor      V   AS MsgRcvd MsgSent   TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.10.10.12    4   12      12      17     12    0    0  00:08:29      0
Route server clients assigned to context all-base:
Neighbor      V   AS MsgRcvd MsgSent   TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.10.10.14    4   14      12      17     12    0    0  00:08:25      0
Route server clients assigned to context all-policy-deny:
Neighbor      V   AS MsgRcvd MsgSent   TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.10.10.16    4   16      12      13     12    0    0  00:08:24      0
Route server clients assigned to context all-policy:
Neighbor      V   AS MsgRcvd MsgSent   TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.10.10.13    4   13      11      14     12    0    0  00:08:22      0
Route server clients assigned to context example-context:
Neighbor      V   AS MsgRcvd MsgSent   TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.10.10.18    4   18      12      17     12    0    0  00:08:30      0
```

Related Commands

Command	Description
neighbor route-server-client	Specifies on a BGP route server that a neighbor is a route server client.

show ip bgp update-group

To display information about the Border Gateway Protocol (BGP) update groups, use the **show ip bgp update-group** command in user EXEC or privileged EXEC mode.

show ip bgp update-group [*index-group*| *ip-address*| *ipv6-address*] [**summary**]

Syntax Description

<i>index-group</i>	(Optional) Update group type with its corresponding index number. The range of update-group index numbers is from 1 to 4294967295.
<i>ip-address</i>	(Optional) IP address of a single neighbor that is a member of an update group.
<i>ipv6-address</i>	(Optional) IPv6 address of a single neighbor that is member of an update group.
summary	(Optional) Displays a summary of update-group member information. The output can be filtered to show information for a single index group or peer with the <i>index-group</i> , <i>ip-address</i> , or <i>ipv6-address</i> argument.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S. The <i>ipv6-address</i> argument was added.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
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 3.8S	This command was modified. The cluster ID for the update group is displayed.

Usage Guidelines

Use this command to display information about BGP update groups. When a change to BGP outbound policy occurs, the router automatically recalculates update group memberships and applies the changes by triggering an outbound soft reset after a 1-minute timer expires. This behavior is designed to provide the network operator with time to change the configuration if a mistake is made. You can manually enable an outbound soft reset before the timer expires by entering the **clear ip bgp ip-address soft out** command.

**Note**

In Cisco IOS Release 12.0(25)S, 12.3(2)T, and earlier releases, the update group recalculation delay timer is set to 3 minutes.

Neighbors with different cluster IDs are assigned to different update groups.

Examples

The following sample output from the **show ip bgp update-group** command shows update group information for all neighbors:

```
Device# show ip bgp update-group
```

```
BGP version 4 update-group 1, internal, Address Family: IPv4 Unicast
BGP Update version : 0, messages 0/0
Route map for outgoing advertisements is COST1
Update messages formatted 0, replicated 0
Number of NLRIs in the update sent: max 0, min 0
Minimum time between advertisement runs is 5 seconds
Has 1 member:
10.4.9.21
BGP version 4 update-group 2, internal, Address Family: IPv4 Unicast
BGP Update version : 0, messages 0/0
Update messages formatted 0, replicated 0
Number of NLRIs in the update sent: max 0, min 0
Minimum time between advertisement runs is 5 seconds
Has 2 members:
10.4.9.5 10.4.9.8
```

The table below describes the significant fields shown in the display.

Table 73: show ip bgp update-group Field Descriptions

Field	Description
BGP version	BGP version.
update-group	Update-group number and type (internal or external).
Update messages formatted 0, replicated 0	Number of update messages that have been formatted and replicated.
Number of NLRIs...	NLRI sent in an update.
Minimum time between advertisement runs	Minimum time, in seconds, between update advertisements.
Has 2 members	Number of members listed by IP address in the update group.

The following sample output from the **show ip bgp update-group** command shows a summary of update-group information for the 10.4.9.8 neighbor:

```
Device# show ip bgp update-group 10.4.9.8 summary
```

```
Summary for Update-group 2 :
```

```
-----
BGP router identifier 10.4.9.4, local AS number 101
BGP table version is 1, main routing table version 1
Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ  OutQ Up/Down  State/PfxRcd
10.4.9.5      4      101      35      35        1    0    0 00:26:22      0
10.4.9.8      4      101      39      39        1    0    0 00:26:21      0
```

The table below describes the significant fields shown in the display.

Table 74: show ip bgp update-group summary Field Descriptions

Field	Description
Summary for Update-group 2	Update-group number.
BGP router identifier 10.4.9.4	IP address and AS number for the specified peer.
BGP table version...	Displays incremental changes in the BGP routing table.
Neighbor...	Specific peer information and statistics, including IP address and AS number.

The following sample output displays the cluster ID assigned to the update group:

```
Device# show ip bgp update-group 1.1.1.1
```

```
BGP version 4 update-group 60, internal, Address Family: IPv4 Unicast
BGP Update version : 391/0, messages 0
Route-Reflector Client
Configured with the cluster-id 4.0.0.115
Topology: global, highest version: 391, tail marker: 391
Format state: Current working (OK, last not in list)
Refresh blocked (not in list, last not in list)
Update messages formatted 0, replicated 0, current 0, refresh 0, limit 1000
Number of NLRI in the update sent: max 0, min 0
Minimum time between advertisement runs is 0 seconds
Has 1 member:
1.1.1.1
```

Related Commands

Command	Description
bgp cluster-id	Sets the global cluster ID on a route reflector.
clear ip bgp	Resets a BGP connection or session.
clear ip bgp update-group	Clears BGP update-group member sessions.

Command	Description
debug ip bgp groups	Displays information related to the processing of BGP update groups.
neighbor cluster-id	Sets the cluster ID for a neighbor.
show ip bgp replication	Displays BGP update-group replication statistics.

show ip bgp vpnv4

To display VPN Version 4 (VPNv4) address information from the Border Gateway Protocol (BGP) table, use the **show ip bgp vpnv4** command in user EXEC or privileged EXEC mode.

```
show ip bgp vpnv4 {all|rd route-distinguisher|vrf vrf-name} [[ip-prefix/length [mask|bestpath|multipaths]]|  
network-address [mask|bestpath|longer-prefixes|multipaths|shorter-prefixes|subnets]]|cidr-only|  
cluster-ids|community|community-list|dampening|extcommunity-list extcommunity-list-name|filter-list|  
inconsistency nexthop-label|inconsistent-as|labels|neighbors [ {ip-address|ipv6-address}  
[advertised-routes|dampened-routes|flap-statistics|paths|policy [detail]|received|received-routes|  
routes]| slow]| nexthops|oer-paths|path-attribute {discard|unknown}| paths [ line ]]| peer-group|  
pending-prefixes|prefix-list prefix-list-name| quote-regexp|regexp|replication [ update-group-index ]  
[ update-group-member-address ]]| rib-failure|route-map route-map-name| summary| update-group|  
update-source| version {version-number|recent offset-value}]
```

Syntax Description

all	Displays the complete VPNv4 database.
rd <i>route-distinguisher</i>	Displays Network Layer Reachability Information (NLRI) prefixes that match the named route distinguisher.
vrf <i>vrf-name</i>	Displays NLRI prefixes associated with the named VPN routing and forwarding (VRF) instance.
<i>ip-prefix/length</i>	(Optional) IP prefix address (in dotted decimal format) and the length of the mask (0 to 32). The slash mark must be included.
longer-prefixes	(Optional) Displays the entry, if any, that exactly matches the specified prefix parameter and all entries that match the prefix in a “longest-match” sense. That is, prefixes for which the specified prefix is an initial substring.
<i>network-address</i>	(Optional) IP address of a network in the BGP routing table.
<i>mask</i>	(Optional) Mask of the network address, in dotted decimal format.
cidr-only	(Optional) Displays only routes that have nonclassful netmasks.
cluster-ids	(Optional) Displays configured cluster IDs.
community	(Optional) Displays routes that match this community.

community-list	(Optional) Displays routes that match this community list.
dampening	(Optional) Displays paths suppressed because of dampening (BGP route from peer is up and down).
extcommunity-list <i>extended-community-list-name</i>	(Optional) Displays routes that match the extended community list.
filter-list	(Optional) Displays routes that conform to the filter list.
inconsistency nexthop-label	(Optional) Displays all inconsistent paths.
inconsistent-as	(Optional) Displays only routes that have inconsistent autonomous systems of origin.
labels	(Optional) Displays incoming and outgoing BGP labels for each NLRI prefix.
neighbors	(Optional) Displays details about TCP and BGP neighbor connections.
<i>ip-address</i>	(Optional) Displays information about the neighbor at this IPv4 address.
<i>ipv6-address</i>	(Optional) Displays information about the neighbor at this IPv6 address.
advertised-routes	(Optional) Displays advertised routes from the specified neighbor.
dampened-routes	(Optional) Displays dampened routes from the specified neighbor.
flap-statistics	(Optional) Displays flap statistics about the specified neighbor.
paths	(Optional) Displays path information.
<i>line</i>	(Optional) A regular expression to match the BGP autonomous system paths.
policy [detail]	(Optional) Displays configured policies for the specified neighbor.
slow	(Optional) Displays BGP slow peer information.
nexthops	(Optional) Displays nexthop address table.

oer-paths	(Optional) Displays all OER-controlled paths.
path-attribute	(Optional) Displays path-attribute-specific information.
discard	(Optional) Displays prefixes with discarded path attribute.
unknown	(Optional) Displays prefixes with unknown path attribute.
paths	(Optional) Displays path information.
<i>line</i>	(Optional) A regular expression to match the BGP autonomous system paths.
peer-group	(Optional) Displays information about peer groups.
pending-prefixes	(Optional) Displays prefixes that are pending deletion.
prefix-list <i>prefix-list</i>	(Optional) Displays routes that match the prefix list.
quote-regexp	(Optional) Displays routes that match the autonomous system path regular expression.
regexp	(Optional) Displays routes that match the autonomous system path regular expression.
replication	(Optional) Displays replication status of update group(s).
rib-failure	(Optional) Displays BGP routes that failed to install in the VRF table.
route-map	(Optional) Displays routes that match the route map.
summary	(Optional) Displays BGP neighbor status.
update-group	(Optional) Displays information on update groups.
update-source	(Optional) Displays update source interface table.
version	(Optional) Displays prefixes with matching version numbers.
<i>version-number</i>	(Optional) If the version keyword is specified, either a <i>version-number</i> or the recent keyword and an <i>offset-value</i> are required.

recent <i>offset-value</i>	(Optional) Displays prefixes with matching version numbers.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(2)T	This command was modified. The output of the show ip bgp vpnv4 all ip-prefix command was enhanced to display attributes including multipaths and a best path to the specified network.
12.0(21)ST	This command was modified. The tags keyword was replaced by the labels keyword to conform to the MPLS guidelines.
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(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.0(27)S	This command was modified. The output of the show ip bgp vpnv4 all labels command was enhanced to display explicit-null label information.
12.3	This command was modified. The rib-failure keyword was added for VRFs.
12.2(22)S	This command was modified. The output of the show ip bgp vpnv4 vrf vrf-name labels command was modified so that directly connected VRF networks no longer display as aggregate; no label appears instead.
12.2(25)S	This command was updated to display MPLS VPN nonstop forwarding information.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router. The display output was modified to indicate whether BGP nonstop routing (NSR) with stateful switchover (SSO) is enabled and the reason the last BGP lost SSO capability.
12.2(33)SRA	This command was modified. The output was modified to support per-VRF assignment of the BGP router ID.
12.2(31)SB2	This command was modified. The output was modified to support per-VRF assignment of the BGP router ID.

Release	Modification
12.2(33)SXH	This command was modified. The output was modified to support per-VRF assignment of the BGP router ID. Note In Cisco IOS Release 12.2(33)SXH, the command output does not display on the standby Route Processor in NSF/SSO mode.
12.4(20)T	This command was modified. The output was modified to support per-VRF assignment of the BGP router ID.
15.0(1)M	This command was modified. The output was modified to support the BGP Event-Based VPN Import feature.
12.2(33)SRE	This command was modified. The command output was modified to support the BGP Event-Based VPN Import, BGP best external, and BGP additional path features.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.
15.2(4)S	This command was implemented on the Cisco 7200 series router and the output was modified to display unknown attributes and discarded attributes associated with a prefix.
Cisco IOS XE Release 3.7S	This command was implemented on the Cisco ASR 903 router and the output modified to display unknown attributes and discarded attributes associated with a prefix.
15.2(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command to display VPNv4 information from the BGP database. The **show ip bgp vpnv4 all** command displays all available VPNv4 information. The **show ip bgp vpnv4 all summary** command displays BGP neighbor status. The **show ip bgp vpnv4 all labels** command displays explicit-null label information.

Examples

The following example shows all available VPNv4 information in a BGP routing table:

```
Router# show ip bgp vpnv4 all
```

```
BGP table version is 18, local router ID is 10.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network          Next Hop              Metric LocPrf Weight Path
```

```

Route Distinguisher: 1:101 (default for vrf vpn1)
*>i10.6.6.6/32      10.0.0.21      11      100      0      ?
*> 10.7.7.7/32      10.150.0.2      11      32768    ?
*>i10.69.0.0/30     10.0.0.21      0       100      0      ?
*> 10.150.0.0/24    0.0.0.0        0       32768    ?

```

The table below describes the significant fields shown in the display.

Table 75: show ip bgp vpnv4 all Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows how to display a table of labels for NLRI prefixes that have a route distinguisher value of 100:1.

```

Router# show ip bgp vpnv4 rd 100:1 labels

Network          Next Hop          In label/Out label
Route Distinguisher: 100:1 (vrf1)
 10.0.0.0         10.20.0.60        34/nolabel
 10.0.0.0         10.20.0.60        35/nolabel
 10.0.0.0         10.20.0.60        26/nolabel
                  10.20.0.60        26/nolabel
 10.0.0.0         10.15.0.15        nolabel/26

```

The table below describes the significant fields shown in the display.

Table 76: show ip bgp vpnv4 rd labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Specifies the BGP next hop address.
In label	Displays the label (if any) assigned by this router.
Out label	Displays the label assigned by the BGP next-hop router.

The following example shows VPNv4 routing entries for the VRF named vpn1:

```
Router# show ip bgp vpnv4 vrf vpn1

BGP table version is 18, local router ID is 10.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop          Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf test1)
*> 10.1.1.1/32      192.168.1.1              0             0 100 i
*bi                 10.4.4.4                  0            100    0 100 i
*> 10.2.2.2/32      192.168.1.1              0             0 100 i
*bi                 10.4.4.4                  0            100    0 100 i
*> 172.16.1.0/24    192.168.1.1              0             0 100 i
* i                 10.4.4.4                  0            100    0 100 i
r> 192.168.1.0      192.168.1.1              0             0 100 i
rbi                 10.4.4.4                  0            100    0 100 i
*> 192.168.3.0      192.168.1.1              0             0 100 i
*bi                 10.4.4.4                  0            100    0 100 i
```

The table below describes the significant fields shown in the display.

Table 77: show ip bgp vpnv4 vrf Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows attributes for network 192.168.9.0 that include multipaths, best path, and a recursive-via-host flag:

```
Router# show ip bgp vpnv4 vrf vpn1 192.168.9.0 255.255.255.0

BGP routing table entry for 100:1:192.168.9.0/24, version 44
Paths: (2 available, best #2, table test1)
  Additional-path
    Advertised to update-groups:
      2
  100, imported path from 400:1:192.168.9.0/24
    10.8.8.8 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.8.8.8, Cluster list: 10.5.5.5 , recursive-via-host
      mpls labels in/out nlabel/17
  100, imported path from 300:1:192.168.9.0/24
    10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
      Originator: 10.7.7.7, Cluster list: 10.5.5.5 , recursive-via-host
```

```
mpls labels in/out nolabel/17
```

The table below describes the significant fields shown in the display.

Table 78: show ip bgp vpnv4 all network-address Field Descriptions

Field	Description
BGP routing table entry for ... version	Internal version number of the table. This number is incremented whenever the table changes.
Paths	Number of autonomous system paths to the specified network. If multiple paths exist, one of the multipaths is designated the best path.
Multipath	Indicates the maximum paths configured (iBGP or eBGP).
Advertised to non peer-group peers	IP address of the BGP peers to which the specified route is advertised.
10.22.7.8 (metric 11) from 10.11.3.4 (10.0.0.8)	Indicates the next hop address and the address of the gateway that sent the update.
Origin	Indicates the origin of the entry. It can be one of the following values: • IGP—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. • incomplete—Entry originated from other than an IGP or Exterior Gateway Protocol (EGP) and was advertised with the redistribute router configuration command. • EGP—Entry originated from an EGP.
metric	If shown, the value of the interautonomous system metric.
localpref	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
valid	Indicates that the route is usable and has a valid set of attributes.
internal/external	The field is internal if the path is learned via iBGP. The field is external if the path is learned via eBGP.
multipath	One of multiple paths to the specified network.

Field	Description
best	If multiple paths exist, one of the multipaths is designated the best path and this path is advertised to neighbors.
Extended Community	Route Target value associated with the specified route.
Originator	The router ID of the router from which the route originated when route reflector is used.
Cluster list	The router ID of all the route reflectors that the specified route has passed through.

The following example shows routes that BGP could not install in the VRF table:

```
Router# show ip bgp vpnv4 vrf xyz rib-failure
```

```

Network          Next Hop          RIB-failure    RIB-NH Matches
Route Distinguisher: 2:2 (default for vrf bar)
10.1.1.2/32      10.100.100.100    Higher admin distance    No
10.111.111.112/32 10.9.9.9          Higher admin distance    Yes

```

The table below describes the significant fields shown in the display.

Table 79: show ip bgp vpnv4 vrf rib-failure Field Descriptions

Field	Description
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
RIB-failure	Cause of the Routing Information Base (RIB) failure. Higher admin distance means that a route with a better (lower) administrative distance, such as a static route, already exists in the IP routing table.

Field	Description
RIB-NH Matches	Route status that applies only when Higher admin distance appears in the RIB-failure column and the bgp suppress-inactive command is configured for the address family being used. There are three choices: • Yes—Means that the route in the RIB has the same next hop as the BGP route or that the next hop recurses down to the same adjacency as the BGP next hop. • No—Means that the next hop in the RIB recurses down differently from the next hop of the BGP route. • n/a—Means that the bgp suppress-inactive command is not configured for the address family being used.

The following example shows the information displayed on the active and standby Route Processors when they are configured for NSF/SSO: MPLS VPN.



Note

In Cisco IOS Release 12.2(33)SXH, the Cisco IOS Software Modularity: MPLS Layer 3 VPNs feature incurred various infrastructure changes. The result of those changes affects the output of this command on the standby Route Processor (RP). In Cisco IOS Release 12.2(33)SXH, the standby RP does not display any output from the **show ip bgp vpv4** command.

```

Router# show ip bgp vpv4 all labels

Network          Next Hop    In label/Out label
Route Distinguisher: 100:1 (vpn1)
10.12.12.12/32   0.0.0.0     16/aggregate(vpn1)
10.0.0.0/8       0.0.0.0     17/aggregate(vpn1)
Route Distinguisher: 609:1 (vpn0)
10.13.13.13/32   0.0.0.0     18/aggregate(vpn0)

Router# show ip bgp vpv4 vrf vpn1 labels

Network          Next Hop    In label/Out label
Route Distinguisher: 100:1 (vpn1)
10.12.12.12/32   0.0.0.0     16/aggregate(vpn1)
10.0.0.0/8       0.0.0.0     17/aggregate(vpn1)

Router# show ip bgp vpv4 all labels

Network          Masklen    In label
Route Distinguisher: 100:1
10.12.12.12      /32        16
10.0.0.0         /8         17
Route Distinguisher: 609:1
10.13.13.13     /32        18

Router# show ip bgp vpv4 vrf vpn1 labels

```

```

Network      Masklen  In label
Route Distinguisher: 100:1
10.12.12.12  /32      16
10.0.0.0     /8       17

```

The table below describes the significant fields shown in the display.

Table 80: show ip bgp vpnv4 labels Field Descriptions

Field	Description
Network	The network address from the BGP table.
Next Hop	The BGP next-hop address.
In label	The label (if any) assigned by this router.
Out label	The label assigned by the BGP next-hop router.
Masklen	The mask length of the network address.

The following example displays output, including the explicit-null label, from the **show ip bgp vpnv4 all labels** command on a CSC-PE router:

```

Router# show ip bgp vpnv4 all labels

      Network      Next Hop      In label/Out label
Route Distinguisher: 100:1 (v1)
 10.0.0.0/24      10.0.0.0      19/aggregate (v1)
 10.0.0.1/32      10.0.0.0      20/nolabel
 10.1.1.1/32      10.0.0.0      21/aggregate (v1)
 10.10.10.10/32   10.0.0.1      25/exp-null

 10.168.100.100/32      10.0.0.1      23/exp-null
 10.168.101.101/32      10.0.0.1      22/exp-null

```

The table below describes the significant fields shown in the display.

Table 81: show ip bgp vpnv4 all labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
In label	Displays the label (if any) assigned by this router.
Out label	Displays the label assigned by the BGP next-hop router.
Route Distinguisher	Displays an 8-byte value added to an IPv4 prefix to create a VPN IPv4 prefix.

The following example displays separate router IDs for each VRF in the output from an image in Cisco IOS Release 12.2(31)SB2, 12.2(33)SRA, 12.2(33)SXH, 12.4(20)T, Cisco IOS XE Release 2.1, and later releases with the Per-VRF Assignment of BGP Router ID feature configured. The router ID is shown next to the VRF name.

```
Router# show ip bgp vpnv4 all

BGP table version is 5, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network        Next Hop           Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf vrf_trans) VRF Router ID 10.99.1.2
*> 192.168.4.0        0.0.0.0                0           32768 ?
Route Distinguisher: 42:1 (default for vrf vrf_user) VRF Router ID 10.99.1.1
*> 192.168.5.0        0.0.0.0                0           32768 ?
```

The table below describes the significant fields shown in the display.

Table 82: show ip bgp vpnv4 all (VRF Router ID) Field Descriptions

Field	Description
Route Distinguisher	Displays an 8-byte value added to an IPv4 prefix to create a VPN IPv4 prefix.
vrf	Name of the VRF.
VRF Router ID	Router ID for the VRF.

In the following example, the BGP Event-Based VPN Import feature is configured in Cisco IOS Release 15.0(1)M, 12.2(33)SRE, and later releases. When the **import path selection** command is configured, but the **strict** keyword is not included, then a safe import path selection policy is in effect. When a path is imported as the best available path (when the best path or multipaths are not eligible for import), the imported path includes the wording “imported safety path,” as shown in the output.

```
Router# show ip bgp vpnv4 all 172.17.0.0

BGP routing table entry for 45000:1:172.17.0.0/16, version 10
Paths: (1 available, best #1, table vrf-A)
Flag: 0x820
      Not advertised to any peer
      2, imported safety path from 50000:2:172.17.0.0/16
      10.0.101.1 from 10.0.101.1 (10.0.101.1)
      Origin IGP, metric 200, localpref 100, valid, internal, best
      Extended Community: RT:45000:100
```

In the following example, BGP Event-Based VPN Import feature configuration information is shown for Cisco IOS Release 15.0(1)M, 12.2(33)SRE, and later releases. When the **import path selection** command is configured with the **all** keyword, any path that matches an RD of the specified VRF will be imported, even though the path does not match the Route Targets (RT) imported by the specified VRF. In this situation, the imported path is marked as “not-in-vrf” as shown in the output. Note that on the net for vrf-A, this path is not the best path because any paths that are not in the VRFs appear less attractive than paths in the VRF.

```
Router# show ip bgp vpnv4 all 172.17.0.0
```



```

BBGP routing table entry for 45000:1:172.17.0.0/16, version 11
Paths: (2 available, best #2, table vrf-A)
Flag: 0x820
  Not advertised to any peer
  2
    10.0.101.2 from 10.0.101.2 (10.0.101.2)
      Origin IGP, metric 100, localpref 100, valid, internal, not-in-vrf
      Extended Community: RT:45000:200
      mpls labels in/out nolabel/16
  2
    10.0.101.1 from 10.0.101.1 (10.0.101.1)
      Origin IGP, metric 50, localpref 100, valid, internal, best
      Extended Community: RT:45000:100
      mpls labels in/out nolabel/16

```

In the following example, the unknown attributes and discarded attributes associated with the prefix are displayed.

Device# **show ip bgp vpnv4 all 10.0.0.0/8**

```

BGP routing table entry for 100:200:10.0.0.0/8, version 0
Paths: (1 available, no best path)
  Not advertised to any peer
  Refresh Epoch 1
  Local
    10.0.103.1 from 10.0.103.1 (10.0.103.1)
      Origin IGP, localpref 100, valid, internal
      Extended Community: RT:1:100
      Connector Attribute: count=1
        type 1 len 12 value 22:22:10.0.101.22
      mpls labels in/out nolabel/16
      unknown transitive attribute: flag E0 type 129 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
      unknown transitive attribute: flag E0 type 140 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
      unknown transitive attribute: flag E0 type 120 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
      discarded unknown attribute: flag C0 type 128 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000

```

The following example is based on the BGP—VPN Distinguisher Attribute feature. The output displays an Extended Community attribute, which is the VPN distinguisher (VD) of 104:1.

Device# **show ip bgp vpnv4 unicast all 1.4.1.0/24**

```

BGP routing table entry for 104:1:1.4.1.0/24, version 28
Paths: (1 available, best #1, no table)
  Advertised to update-groups:
    1
  Refresh Epoch 1
  1001
    19.0.101.1 from 19.0.101.1 (19.0.101.1)
      Origin IGP, localpref 100, valid, external, best
      Extended Community: VD:104:1
      mpls labels in/out nolabel/16
      rx pathid: 0, tx pathid: 0x0

```

The following example includes “allow-policy” in the output, indicating that the BGP—Support for iBGP Local-AS feature was configured for the specified neighbor by configuring the **neighbor allow-policy** command.

Device# **show ip bgp vpnv4 all neighbors 192.168.3.3 policy**

show ip bgp vpnv4

```

Neighbor: 192.168.3.3, Address-Family: VPNv4 Unicast
Locally configured policies:
  route-map pe33 out
  route-reflector-client
  allow-policy
  send-community both

```

Related Commands

Command	Description
import path limit	Specifies the maximum number of BGP paths, per VRF importing net, that can be imported from an exporting net.
import path selection	Specifies the BGP import path selection policy for a specific VRF instance.
neighbor allow-policy	Allows iBGP policies to be configured for the specified neighbor.
set extcommunity vpn-distinguisher	Sets a VPN distinguisher attribute to routes that pass a route map.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

show ip bgp vpnv4 all dampening

To display BGP dampening information for the Virtual Private Network Version 4 (VPNv4) address family, use the **show ip bgp vpnv4 all dampening** command in user EXEC or privileged EXEC mode.

show ip bgp vpnv4 all dampening {**dampened-paths** | **flap-statistics** [*network-address* [*mask* | **bestpath** | **multipaths**] | *ip-prefix / length*] **cidr-only** | **filter-list** *filter-list* | **oer-paths** | **prefix-list** *prefix-list* | **quote-regexp** *regexp* | **regexp** *regexp* | **route-map** *map-name* | **version** {*number* | **recent** }] | **parameters**}

Syntax Description

dampened-paths	Display routes suppressed due to dampening.
flap-statistics	Displays flap statistics of routes.
<i>network-address</i>	(Optional) Used with the flap-statistics keyword, network in the BGP routing table to display.
<i>mask</i>	(Optional) Used with the <i>network-address</i> argument, network mask that determines the networks displayed.
bestpath	(Optional) Used with the <i>network-address</i> argument, displays the bestpath for this prefix.
multipaths	(Optional) Used with the <i>network-address</i> argument, displays the multipaths for this prefix.
<i>ip-prefix/length</i>	(Optional) Used with the flap-statistics keyword, IP prefix/network length, such as 10.0.0.0/8.
cidr-only	(Optional) Used with the flap-statistics keyword, displays only routes with non-natural netmasks.
filter-list <i>filter-list</i>	(Optional) Used with the flap-statistics keyword, displays routes that conform to the specified filter list in the range 1-500.
oer-paths	(Optional) Used with the flap-statistics keyword, displays all OER controlled paths.
prefix-list <i>prefix-list</i>	(Optional) Used with the flap-statistics keyword, displays routes allowed by the prefix list.
quote-regexp <i>regexp</i>	(Optional) Used with the flap-statistics keyword, displays routes matching the AS path "regular expression".
regexp <i>regexp</i>	(Optional) Used with the flap-statistics keyword, displays routes matching the AS path regular expression.

route-map <i>map-name</i>	(Optional) Used with the flap-statistics keyword, displays routes allowed by the route map.
version <i>number</i>	(Optional) Used with the flap-statistics keyword, displays version of BGP table.
recent	(Optional) Used with the flap-statistics keyword, displays recent version of BGP table.
parameters	Display details of configured dampening parameters.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use this command to display dampening information for the VPNv4 address family.

Examples

The following example shows dampening flap-statistics for the VPNv4 address family:

```

Router# show ip bgp vpnv4 all dampening flap-statistics

For_address_family: VPNv4 Unicast
% dampening not enabled for base
For vrf: Cust_A
BGP table version is 15, local router ID is 144.124.23.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f RT-Filter
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network        From      Flaps  Duration  Reuse      Path
*>  20.20.20.20/32    172.16.1.2      1    00:01:05      65001
For vrf: Cust_B
*d  11.11.11.11/32    192.168.1.2     3    00:04:22  00:04:49  65001
Router#

```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes BGP route dampening parameters.

show ip bgp vpnv4 all sso summary

To display information about Border Gateway Protocol (BGP) peers that support BGP nonstop routing (NSR) with stateful switchover (SSO), use the **show ip bgp vpnv4 sso summary** command in privileged EXEC mode.

show ip bgp vpnv4 all sso summary

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(28)SB	This command was introduced.
	15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
	Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
	Cisco IOS XE 3.7S	This command was implemented on the Cisco ASR 903 router.

Usage Guidelines The **show ip bgp vpnv4 all sso summary** command is used to display the number of BGP neighbors that are in SSO mode.

Examples The following is sample output from the **show ip bgp vpnv4 all sso summary** command:

```
Router# show ip bgp vpnv4 all sso summary
Stateful switchover support enabled for 40 neighbors
```

The table below describes the fields shown in the display.

Table 83: show ip bgp vpnv4 all sso summary Field Descriptions

Field	Description
Stateful Switchover support enabled for	Indicates the number of BGP neighbors that are in SSO mode.

Related Commands	Command	Description
	neighbor ha-mode sso	Configures a BGP neighbor to support SSO.

 show ip bgp vpnv4 all sso summary

show ip bgp vpnv6 unicast all dampening

To display BGP dampening information for the Virtual Private Network Version 6 (VPNv6) address family, use the **show ip bgp vpnv6 unicast all dampening** command in user EXEC or privileged EXEC mode.

show ip bgp vpnv6 unicast all dampening {**dampened-paths**|**flap-statistics**[*network / length* | **filter-list** *filter-list*]|**injected-paths**|**prefix-list** *prefix-list*|**quote-regexp** *regexp* | **regexp** *regexp* | **route-map** *map-name*]
| **parameters**}

Syntax Description

dampened-paths	Display routes suppressed due to dampening.
flap-statistics	Displays flap statistics of routes.
<i>network / length</i>	(Optional) Used with the flap-statistics keyword, IPv6 prefix network/length in the format <i>X:X:X:X::X / <0-128></i> .
filter-list <i>filter-list</i>	(Optional) Used with the flap-statistics keyword, displays routes that conform to the specified filter list in the range 1-500.
injected-paths	(Optional) Used with the flap-statistics keyword, displays all injected paths.
prefix-list <i>list</i>	(Optional) Used with the flap-statistics keyword, displays routes allowed by the prefix list.
quote-regexp <i>regexp</i>	(Optional) Used with the flap-statistics keyword, displays routes matching the AS path “regular expression”.
regexp <i>regexp</i>	(Optional) Used with the flap-statistics keyword, displays routes matching the AS path regular expression.
route-map <i>map-name</i>	(Optional) Used with the flap-statistics keyword, displays routes allowed by the route map.
parameters	Display details of configured dampening parameters.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

Use this command to display BGP dampening information for the VPNv6 address family.

Examples

The following example shows dampening VPNv6 information:

```
Router# show ip bgp vpnv6 unicast all dampening flap-statistics
For address family: VPNv6 Unicast
% dampening not enabled for base
For vrf: RED
For vrf: BLUE
BGP table version is 36, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale, m multipath, b backup-path, x best-external, f RT-Filter
Origin codes: i - IGP, e - EGP, ? - incomplete
      Network        From      Flaps  Duration Reuse      Path
*d 11::/64          20::2        3    00:03:17 00:05:59 2
*d 22::/64          20::2        3    00:03:17 00:05:59 2
*d 33::/64          20::2        3    00:03:17 00:05:59 2
*d 44::/64          20::2        3    00:03:17 00:05:59 2
*d 55::/64          20::2        3    00:03:17 00:05:59 2
R1#
```

Related Commands

Command	Description
bgp dampening	Enables BGP route dampening or changes BGP route dampening parameters.

show ip community-list

To display configured community lists, use the **show ip community-list** command in user or privileged EXEC mode.

show ip community-list [*community-list-number*| *community-list-name*] [**exact-match**]

Syntax Description

<i>community-list-number</i>	(Optional) A standard or expanded community list number in the range from 1 to 500.
<i>community-list-name</i>	(Optional) Community list name. The community list name can be standard or expanded.
exact-match	(Optional) Displays only routes that have an exact match.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.0(10)S	Named community list support was added.
12.0(16)ST	Named community lists support was integrated into Cisco IOS Release 12.0(16)ST.
12.1(9)E	Named community lists support was integrated into Cisco IOS Release 12.1(9)E.
12.2(8)T	Named community lists support was integrated into Cisco IOS Release 12.2(8)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 12.2(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 without any arguments or keywords. If no arguments are specified, this command will display all community lists. However, the community list name or number can be specified when entering the **show ip community-list** command. This option can be useful for filtering the output of this command and verifying a single named or numbered community list.

Examples

The following sample output is similar to the output that will be displayed when the **show ip community-list** command is entered in privileged EXEC mode:

```
Router# show ip community-list

Community standard list 1
    permit 3
    deny 5
Community (expanded) access list 101
    deny 4
    permit 6
Named Community standard list COMMUNITY_LIST_NAME
    permit 1
    deny 7
Named Community expanded list COMMUNITY_LIST_NAME_TWO
    deny 2
    permit 8
```

The Field Descriptions table below describes the significant fields shown in the display.

Table 84: show ip community-list Field Descriptions

Field	Description
Community standard list	If shown, this value will display a standard community list number (1 to 99). The standard community list number will immediately follow this value.
Community (expanded) access list	If shown, this value will display an expanded community list number (100 to 500). The expanded community list number will immediately follow this value.
Named community standard list	If shown, this value will display a standard community list name. The standard community list name will immediately follow this value.
Named community expanded list	If shown, this value will display an expanded community list name. The expanded community list name will immediately follow this value.

show ip extcommunity-list

To display routes that are permitted by an extended community list, use the **show ip extcommunity-list** command in user EXEC or privileged EXEC mode.

show ip extcommunity-list [*list-number*| *list-name*]

Syntax Description

<i>list-number</i>	(Optional) Specifies an extended community list number from 1 to 500. A standard extended community list number is from 1 to 99. An expanded extended list is from 100 to 500.
<i>list-name</i>	(Optional) Specifies an extended community list name. If a specific extended community list number is not specified, all locally configured extended community lists will be displayed by default.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1	This command was introduced.
12.2(25)S	Support for named extended community lists was added. Minor formatting changes were made to the output.
12.3(11)T	Support for named extended community lists was added. Minor formatting changes were made to the output.
12.2(27)SBC	This command was integrated into the Cisco IOS Release 12.2(27)SBC.
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.
12.0(32)S12	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.0(32)SY8	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.4(24)T	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.

Release	Modification
Cisco IOS XE Release 2.3	This command was modified. Support for displaying 4-byte autonomous system numbers in asdot notation only was added.
12.2(33)SX11	This command was modified. Support for 4-byte autonomous system numbers in asplain and asdot notation was added.
12.0(33)S3	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
Cisco IOS XE Release 2.4	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain notation was added and the default display format is now asplain.
12.2(33)SRE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
15.1(1)SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
15.2(1)E	This command was integrated into Cisco IOS Release 15.2(1)E.

Usage Guidelines

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain--65538 for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.

In Cisco IOS Release 12.0(32)S12, 12.4(24)T, and Cisco IOS XE Release 2.3, the Cisco implementation of 4-byte autonomous system numbers uses asdot--1.2 for example--as the only configuration format, regular expression match, and output display, with no asplain support.

If the route target--RT in the output--contains a 4-byte autonomous system number as part of the extended community list, it will be displayed in the appropriate format.

Examples

The following is sample output from the **show ip extcommunity-list** command:

```
Router# show ip extcommunity-list
Standard extended community-list 1
  10 permit RT:64512:10
  20 permit SoO:65400:20
```

```

30 deny RT:65424:30 SoO:64524:40
Standard extended community-list 99
10 permit RT:65504:40 SoO:65505:50
20 deny RT:65406:60 SoO:65307:70
Expanded extended community-list LIST_NAME
10 permit 0-9* A-Z* a-z*

```

The table below describes the significant fields shown in the display.

Table 85: show ip extcommunity-list Field Descriptions

Field	Description
... extended community-list...	The type of extended community-list (standard or expanded), and the name or number of the extended community list.
10	The sequence number of the extended community list entry. 10 is the lowest default sequence number. Extended community lists increment by 10 when default values are configured.
permit/deny	Indicates a permit or deny sequence entry.
RT/SoO	Indicates the route target or the site of origin used in a standard extended community list.
0-9* A-Z* a-z*	Regular expression used in an expanded extended community list.

The following output is from the **show ip extcommunity-list** command after a 4-byte autonomous system number has been configured as part of the route target. The 4-byte autonomous system number, 65537, is displayed in the default asplain format. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or a later release.

```

Router# show ip extcommunity-list 1
Extended community standard list 1
  permit RT:65537:100

```

The following output displays a 4-byte autonomous system number that has been configured as part of the route target. The 4-byte autonomous system number--1.1--is displayed in asdot notation. The dot notation is the only format for 4-byte autonomous system numbers in Cisco IOS Release 12.0(32)S12, 12.4(24)T, or Cisco IOS XE Release 2.3. This output can also be seen in Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SX11, Cisco IOS XE Release 2.4, or later releases. after the **bgp asnotation dot** command has been entered to display 4-byte autonomous system numbers in dot notation.

```

Router# show ip extcommunity-list 1
Extended community standard list 1
  permit RT:1.1:100

```

Related Commands

Command	Description
bgp asnotation dot	Changes the default display and the regular expression match format of BGP 4-byte autonomous system numbers from asplain (decimal values) to dot notation.
router bgp	Configures the BGP routing process.
show route-map	Displays configured route maps.

show ip policy-list

To display information about a configured policy list and policy list entries, use the **show ip policy-list** command in EXEC mode.

show ip policy-list [*policy-list-name*]

Syntax Description

policy-list-name	(Optional) Displays information about the specified policy list with this argument.

Command Modes

EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(15)T	This command was integrated into 12.2(15)T.
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.

Examples

The following is sample output from the **show ip policy-list** command. The output of this command will display the policy-list name and configured match clauses. The following sample output is similar to the output that will be displayed:

```
Router> show ip policy-list

policy-list POLICY-LIST-NAME-1 permit
  Match clauses:
    metric 20
policy-list POLICY-LIST-NAME-2 permit
  Match clauses:
    as-path (as-path filter): 1
```

Related Commands

Command	Description
show route-map	Displays configured route maps and information about referenced policy maps.

show ip prefix-list

To display information about a prefix list or prefix list entries, use the **show ip prefix-list** command in user EXEC or privileged EXEC mode.

show ip prefix-list[**detail**|**summary**]{*prefix-list-name* [**seq** *sequence-number*| *network/length* [**longer**|**first-match**]}}

Syntax Description

detail summary	(Optional) Displays detailed or summarized information about all prefix lists.
<i>prefix-list-name</i>	(Optional) Displays the entries in a specific prefix list.
seq <i>sequence-number</i>	(Optional) Displays only the prefix list entry with the specified sequence number in the specified prefix-list.
<i>network</i> / <i>length</i>	(Optional) Displays all entries in the specified prefix list that use this network address and netmask length (in bits).
longer	(Optional) Displays all entries of the specified prefix list that match or are more specific than the given <i>network/length</i> .
first-match	(Optional) Displays the first entry of the specified prefix list that matches the given <i>network / length</i> .

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into 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 the output of the **show ip prefix-list** command with details about the prefix list named test:

```
Router# show ip prefix-list detail test
ip prefix-list test:
Description: test-list
count: 1, range entries: 0, sequences: 10 - 10, refcount: 3
seq 10 permit 10.0.0.0/8 (hit count: 0, refcount: 1)
```

Related Commands

Command	Description
clear ip prefix-list	Resets the hit count of the prefix list entries.
distribute-list in (BGP)	Filters networks received in updates.
distribute-list out (BGP)	Suppresses networks from being advertised in updates.
ip prefix-list	Creates an entry in a prefix list.
ip prefix-list description	Adds a text description of a prefix list.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
neighbor prefix-list	Distributes BGP neighbor information as specified in a prefix list.

show ip route

To display contents of the routing table, use the **show ip route** command in user EXEC or privileged EXEC mode.

show ip route [*ip-address* [**repair-paths**| **next-hop-override** [**dhcp**]| *mask* [**longer-prefixes**]]| *protocol* [*process-id*]| **list** [*access-list-number* | *access-list-name*]| **static download**| **update-queue**]

Syntax Description

<i>ip-address</i>	(Optional) IP address for which routing information should be displayed.
repair-paths	(Optional) Displays the repair paths.
next-hop-override	(Optional) Displays the Next Hop Resolution Protocol (NHRP) next-hop overrides that are associated with a particular route and the corresponding default next hops.
dhcp	(Optional) Displays routes added by the Dynamic Host Configuration Protocol (DHCP) server.
<i>mask</i>	(Optional) Subnet mask.
longer-prefixes	(Optional) Displays output for longer prefix entries.
<i>protocol</i>	(Optional) The name of a routing protocol or the keyword connected , mobile , static , or summary . If you specify a routing protocol, use one of the following keywords: bgp , eigrp , hello , isis , odr , ospf , nhrp , or rip .
<i>process-id</i>	(Optional) Number used to identify a process of the specified protocol.
list	(Optional) Filters output by an access list name or number.
<i>access-list-number</i>	(Optional) Access list number.
<i>access-list-name</i>	(Optional) Access list name.
static	(Optional) Displays static routes.
download	(Optional) Displays routes installed using the authentication, authorization, and accounting (AAA) route download function. This keyword is used only when AAA is configured.

update-queue	(Optional) Displays Routing Information Base (RIB) queue updates.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
9.2	This command was introduced.
10.0	This command was modified. The “D—EIGRP, EX—EIGRP, N1—SPF NSSA external type 1 route” and “N2—OSPF NSSA external type 2 route” codes were included in the command output.
10.3	This command was modified. The <i>process-id</i> argument was added.
11.0	This command was modified. The longer-prefixes keyword was added.
11.1	This command was modified. The “U—per-user static route” code was included in the command output.
11.2	This command was modified. The “o—on-demand routing” code was included in the command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA, and the update-queue keyword was added.
11.3	This command was modified. The command output was enhanced to display the origin of an IP route in Intermediate System-to-Intermediate System (IS-IS) networks.
12.0(1)T	This command was modified. The “M—mobile” code was included in the command output.
12.0(3)T	This command was modified. The “P—periodic downloaded static route” code was included in the command output.
12.0(4)T	This command was modified. The “ia—IS-IS” code was included in the command output.
12.2(2)T	This command was modified. The command output was enhanced to display information on multipaths to the specified network.

Release	Modification
12.2(13)T	This command was modified. The <i>egp</i> and <i>igrp</i> arguments were removed because the Exterior Gateway Protocol (EGP) and the Interior Gateway Routing Protocol (IGRP) were no longer available in Cisco software.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX.
12.3(2)T	This command was modified. The command output was enhanced to display route tag information.
12.3(8)T	This command was modified. The command output was enhanced to display static routes using DHCP.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRE	This command was modified. The dhcp and repair-paths keywords were added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5. The next-hop-override and nhrp keywords were added.
15.2(2)S	This command was modified. The command output was enhanced to display route tag values in dotted decimal format.
Cisco IOS XE Release 3.6S	This command was modified. The command output was enhanced to display route tag values in dotted decimal format.
15.2(4)S	This command was implemented on the Cisco 7200 series router.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Examples

Examples

The following is sample output from the **show ip route** command when an IP address is not specified:

```
Device# show ip route
```

```
Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, El - OSPF external type 1 route,
```

```

E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
N2 - OSPF NSSA external type 2 route
Gateway of last resort is 10.119.254.240 to network 10.140.0.0
O E2 10.110.0.0 [160/5] via 10.119.254.6, 0:01:00, Ethernet2
E 10.67.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
O E2 10.68.132.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
O E2 10.130.0.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
E 10.128.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E 10.129.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E 10.65.129.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E 10.10.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E 10.75.139.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E 10.16.208.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E 10.84.148.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E 10.31.223.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E 10.44.236.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E 10.141.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E 10.140.0.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2

```

The following sample output from the **show ip route** command includes routes learned from IS-IS Level 2:

Device# **show ip route**

```

Codes: R - RIP derived, O - OSPF derived,
C - connected, S - static, B - BGP derived,
* - candidate default route, IA - OSPF inter area route,
i - IS-IS derived, ia - IS-IS, U - per-user static route,
o - on-demand routing, M - mobile, P - periodic downloaded static route,
D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
N2 - OSPF NSSA external type 2 route
Gateway of last resort is not set
10.89.0.0 is subnetted (mask is 255.255.255.0), 3 subnets
C 10.89.64.0 255.255.255.0 is possibly down,
routing via 10.0.0.0, Ethernet0
i L2 10.89.67.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0
i L2 10.89.66.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0

```

The following is sample output from the **show ip route ip-address mask longer-prefixes** command. When this keyword is included, the address-mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed. The logical AND operation is performed on the source address 10.0.0.0 and the mask 10.0.0.0, resulting in 10.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared with 10.0.0.0. Any destinations that fall into that range are displayed in the output.

Device# **show ip route 10.0.0.0 10.0.0.0 longer-prefixes**

```

Codes: R - RIP derived, O - OSPF derived,
C - connected, S - static, B - BGP derived,
* - candidate default route, IA - OSPF inter area route,
i - IS-IS derived, ia - IS-IS, U - per-user static route,
o - on-demand routing, M - mobile, P - periodic downloaded static route,
D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
N2 - OSPF NSSA external type 2 route
Gateway of last resort is not set

S 10.134.0.0 is directly connected, Ethernet0
S 10.10.0.0 is directly connected, Ethernet0
S 10.129.0.0 is directly connected, Ethernet0
S 10.128.0.0 is directly connected, Ethernet0
S 10.49.246.0 is directly connected, Ethernet0
S 10.160.97.0 is directly connected, Ethernet0
S 10.153.88.0 is directly connected, Ethernet0
S 10.76.141.0 is directly connected, Ethernet0
S 10.75.138.0 is directly connected, Ethernet0
S 10.44.237.0 is directly connected, Ethernet0
S 10.31.222.0 is directly connected, Ethernet0
S 10.16.209.0 is directly connected, Ethernet0
S 10.145.0.0 is directly connected, Ethernet0

```

show ip route

```

S    10.141.0.0 is directly connected, Ethernet0
S    10.138.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
    10.19.0.0 255.255.255.0 is subnetted, 1 subnets
C    10.19.64.0 is directly connected, Ethernet0
    10.69.0.0 is variably subnetted, 2 subnets, 2 masks
C    10.69.232.32 255.255.255.240 is directly connected, Ethernet0
S    10.69.0.0 255.255.0.0 is directly connected, Ethernet0

```

The following sample outputs from the **show ip route** command display all downloaded static routes. A “p” indicates that these routes were installed using the AAA route download function.

Device# **show ip route**

```

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR, P - periodic downloaded static route
       T - traffic engineered route

```

Gateway of last resort is 172.16.17.1 to network 10.0.0.0

```

    172.31.0.0/32 is subnetted, 1 subnets
P    172.31.229.41 is directly connected, Dialer1 10.0.0.0/8 is subnetted, 3 subnets
P    10.1.1.0 [200/0] via 172.31.229.41, Dialer1
P    10.1.3.0 [200/0] via 172.31.229.41, Dialer1
P    10.1.2.0 [200/0] via 172.31.229.41, Dialer1

```

Device# **show ip route static**

```

    172.16.4.0/8 is variably subnetted, 2 subnets, 2 masks
P    172.16.1.1/32 is directly connected, BRI0
P    172.16.4.0/8 [1/0] via 10.1.1.1, BRI0
S    172.31.0.0/16 [1/0] via 172.16.114.65, Ethernet0
S    10.0.0.0/8 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
    172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S    172.16.114.201/32 is directly connected, BRI0
S    172.16.114.205/32 is directly connected, BRI0
S    172.16.114.174/32 is directly connected, BRI0
S    172.16.114.12/32 is directly connected, BRI0
P    10.0.0.0/8 is directly connected, BRI0
P    10.1.0.0/16 is directly connected, BRI0
P    10.2.2.0/24 is directly connected, BRI0
S*   0.0.0.0/0 [1/0] via 172.16.114.65, Ethernet0
S    172.16.0.0/16 [1/0] via 172.16.114.65, Ethernet0

```

The following sample output from the **show ip route static download** command displays all active and inactive routes installed using the AAA route download function:

Device# **show ip route static download**

Connectivity: A - Active, I - Inactive

```

A    10.10.0.0 255.0.0.0 BRI0
A    10.11.0.0 255.0.0.0 BRI0
A    10.12.0.0 255.0.0.0 BRI0
A    10.13.0.0 255.0.0.0 BRI0
I    10.20.0.0 255.0.0.0 172.21.1.1
I    10.22.0.0 255.0.0.0 Serial0
I    10.30.0.0 255.0.0.0 Serial0
I    10.31.0.0 255.0.0.0 Serial1
I    10.32.0.0 255.0.0.0 Serial1
A    10.34.0.0 255.0.0.0 192.168.1.1
A    10.36.1.1 255.255.255.255 BRI0 200 name remotel
I    10.38.1.9 255.255.255.0 192.168.69.1

```

The following sample outputs from the **show ip route nhrp** command display shortcut switching on the tunnel interface:

Device# **show ip route**

```
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
Gateway of last resort is not set
10.0.0.0/16 is variably subnetted, 3 subnets, 2 masks
C      10.1.1.0/24 is directly connected, Tunnel0
C      172.16.22.0 is directly connected, Ethernet1/0
H      172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
C      10.11.11.0 is directly connected, Ethernet0/0
```

Device# **show ip route nhrp**

```
H      172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
```

The following are sample outputs from the **show ip route** command when the **next-hop-override** keyword is used. When this keyword is included, the NHRP next-hop overrides that are associated with a particular route and the corresponding default next hops are displayed.

```
=====
1) Initial configuration
=====
```

Device# **show ip route**

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      10.2.1.0/24 is directly connected, Loopback1
L      10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S      10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S      10.11.11.0 is directly connected, Ethernet0/0
```

Device# **show ip route next-hop-override**

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C      10.2.1.0/24 is directly connected, Loopback1
L      10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S      10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
```

S 10.11.11.0 is directly connected, Ethernet0/0

Device# **show ip cef**

Prefix	Next Hop	Interface
.		
.		
.		
10.2.1.255/32	receive	Loopback1
10.10.10.0/24	attached	Tunnel0 <<<<<<<
10.11.11.0/24	attached	Ethernet0/0
172.16.0.0/12	drop	

```
=====
2) Add a next-hop override
   address = 10.10.10.0
   mask = 255.255.255.0
   gateway = 10.1.1.1
   interface = Tunnel0
=====
```

Device# **show ip route**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP
 + - replicated route

Gateway of last resort is not set
 10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
 C 10.2.1.0/24 is directly connected, Loopback1
 L 10.2.1.1/32 is directly connected, Loopback1
 10.0.0.0/24 is subnetted, 1 subnets

S 10.10.10.0 is directly connected, Tunnel0
 10.11.0.0/24 is subnetted, 1 subnets
 S 10.11.11.0 is directly connected, Ethernet0/0

Device# **show ip route next-hop-override**

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
 D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
 N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
 E1 - OSPF external type 1, E2 - OSPF external type 2
 i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
 ia - IS-IS inter area, * - candidate default, U - per-user static route
 o - ODR, P - periodic downloaded static route, H - NHRP
 + - replicated route

Gateway of last resort is not set
 10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
 C 10.2.1.0/24 is directly connected, Loopback1
 L 10.2.1.1/32 is directly connected, Loopback1
 10.0.0.0/24 is subnetted, 1 subnets

S 10.10.10.0 is directly connected, Tunnel0
 [NHO][1/0] via 10.1.1.1, Tunnel0
 10.11.0.0/24 is subnetted, 1 subnets
 S 10.11.11.0 is directly connected, Ethernet0/0

Device# **show ip cef**

Prefix	Next Hop	Interface
.		
.		
.		
10.2.1.255/32	receive	Loopback1
10.10.10.0/24		


```

10.10.10.0/24      10.1.1.1      Tunnel0
10.11.11.0/24      attached      Ethernet0/0
10.12.0.0/16 drop
.
.
.
=====
3) Delete a next-hop override
   address = 10.10.10.0
   mask = 255.255.255.0
   gateway = 10.11.1.1
   interface = Tunnel0
=====

Device# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
  10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       10.2.1.0/24 is directly connected, Loopback1
L       10.2.1.1/32 is directly connected, Loopback1
       10.0.0.0/24 is subnetted, 1 subnets
S       10.10.10.0 is directly connected, Tunnel0
       10.11.0.0/24 is subnetted, 1 subnets
S       10.11.11.0 is directly connected, Ethernet0/0

Device# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
  10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       10.2.1.0/24 is directly connected, Loopback1
L       10.2.1.1/32 is directly connected, Loopback1
       10.0.0.0/24 is subnetted, 1 subnets
S       10.10.10.0 is directly connected, Tunnel0
       10.11.0.0/24 is subnetted, 1 subnets
S       10.11.11.0 is directly connected, Ethernet0/0

Device# show ip cef

Prefix          Next Hop          Interface
.
.
.
.
10.2.1.255/32    receive              Loopback1
10.10.10.0/24    attached             Tunnel0
10.11.11.0/24    attached             Ethernet0/0
10.120.0.0/16 drop
.
.
.

```

The table below describes the significant fields shown in the displays:

Table 86: show ip route Field Descriptions

Field	Description
Codes (Protocol)	Indicates the protocol that derived the route. It can be one of the following values: • B—BGP derived • C—Connected • D—Enhanced Interior Gateway Routing Protocol (EIGRP) • EX—EIGRP external • H—NHRP • i—IS-IS derived • ia—IS-IS • L—Local • M—Mobile • o—On-demand routing • O—Open Shortest Path First (OSPF) derived • P—Periodic downloaded static route • R—Routing Information Protocol (RIP) derived • S—Static • U—Per-user static route • +—Replicated route
Codes (Type)	Type of route. It can be one of the following values: • *—Indicates the last path used when a packet was forwarded. This information is specific to nonfast-switched packets. • E1—OSPF external type 1 route • E2—OSPF external type 2 route • IA—OSPF interarea route • L1—IS-IS Level 1 route • L2—IS-IS Level 2 route • N1—OSPF not-so-stubby area (NSSA) external type 1 route • N2—OSPF NSSA external type 2 route

Field	Description
10.110.0.0	Indicates the address of the remote network.
[160/5]	The first number in brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.119.254.6	Specifies the address of the next device to the remote network.
0:01:00	Specifies the last time the route was updated (in hours:minutes:seconds).
Ethernet2	Specifies the interface through which the specified network can be reached.

Examples

The following is sample output from the **show ip route** command when an IP address is specified:

```
Device# show ip route 10.0.0.1

Routing entry for 10.0.0.1/32
  Known via "isis", distance 115, metric 20, type level-1
  Redistributing via isis
  Last update from 10.191.255.251 on Fddi1/0, 00:00:13 ago
  Routing Descriptor Blocks:
    * 10.22.22.2, from 10.191.255.247, via Serial2/3
      Route metric is 20, traffic share count is 1
      10.191.255.251, from 10.191.255.247, via Fddi1/0
      Route metric is 20, traffic share count is 1
```

When an IS-IS router advertises its link-state information, the router includes one of its IP addresses to be used as the originator IP address. When other routers calculate IP routes, they store the originator IP address with each route in the routing table.

The preceding example shows the output from the **show ip route** command for an IP route generated by IS-IS. Each path that is shown under the Routing Descriptor Blocks report displays two IP addresses. The first address (10.22.22.2) is the next-hop address. The second is the originator IP address from the advertising IS-IS router. This address helps you determine the origin of a particular IP route in your network. In the preceding example, the route to 10.0.0.1/32 was originated by a device with IP address 10.191.255.247.

The table below describes the significant fields shown in the display.

Table 87: show ip route with IP Address Field Descriptions

Field	Description
Routing entry for 10.0.0.1/32	Network number and mask.
Known via...	Indicates how the route was derived.
Redistributing via...	Indicates the redistribution protocol.

Field	Description
Last update from 10.191.255.251	Indicates the IP address of the router that is the next hop to the remote network and the interface on which the last update arrived.
Routing Descriptor Blocks	Displays the next-hop IP address followed by the information source.
Route metric	This value is the best metric for this Routing Descriptor Block.
traffic share count	Indicates the number of packets transmitted over various routes.

The following sample output from the **show ip route** command displays the tag applied to the route 10.22.0.0/16. You must specify an IP prefix to see the tag value. The fields in the display are self-explanatory.

```
Device# show ip route 10.22.0.0
Routing entry for 10.22.0.0/16
  Known via "isis", distance 115, metric 12
  Tag 120, type level-1
  Redistributing via isis
  Last update from 172.19.170.12 on Ethernet2, 01:29:13 ago
  Routing Descriptor Blocks:
    * 172.19.170.12, from 10.3.3.3, via Ethernet2
      Route metric is 12, traffic share count is 1
      Route tag 120
```

Examples

The following example shows that IP route 10.8.8.0 is directly connected to the Internet and is the next-hop (option 3) default gateway. Routes 10.1.1.1 [1/0], 10.3.2.1 [24/0], and 172.16.2.2 [1/0] are static, and route 10.0.0.0/0 is a default route candidate. The fields in the display are self-explanatory.

```
Device# show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.0.19.14 to network 0.0.0.0
10.0.0.0/24 is subnetted, 1 subnets
C 10.8.8.0 is directly connected, Ethernet1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.1.1.1 [1/0] via 10.8.8.1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.3.2.1 [24/0] via 10.8.8.1
  172.16.0.0/32 is subnetted, 1 subnets
S 172.16.2.2 [1/0] via 10.8.8.1
  10.0.0.0/28 is subnetted, 1 subnets
C 10.0.19.0 is directly connected, Ethernet0
  10.0.0.0/24 is subnetted, 1 subnets
C 10.15.15.0 is directly connected, Loopback0
S* 10.0.0.0/0 [1/0] via 10.0.19.14
```

The following sample output from the **show ip route repair-paths** command shows repair paths marked with the tag [RPR]. The fields in the display are self-explanatory:

```
Device# show ip route repair-paths

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set

    10.0.0.0/32 is subnetted, 3 subnets
C       10.1.1.1 is directly connected, Loopback0
B       10.2.2.2 [200/0] via 172.16.1.2, 00:31:07
          [RPR][200/0] via 192.168.1.2, 00:31:07
B       10.9.9.9 [20/0] via 192.168.1.2, 00:29:45
          [RPR][20/0] via 192.168.3.2, 00:29:45
    172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C       172.16.1.0/24 is directly connected, Ethernet0/0
L       172.16.1.1/32 is directly connected, Ethernet0/0
    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Serial2/0
L       192.168.1.1/32 is directly connected, Serial2/0
B       192.168.3.0/24 [200/0] via 172.16.1.2, 00:31:07
          [RPR][200/0] via 192.168.1.2, 00:31:07
B       192.168.9.0/24 [20/0] via 192.168.1.2, 00:29:45
          [RPR][20/0] via 192.168.3.2, 00:29:45
B       192.168.13.0/24 [20/0] via 192.168.1.2, 00:29:45
          [RPR][20/0] via 192.168.3.2, 00:29:45

Device# show ip route repair-paths 10.9.9.9

>Routing entry for 10.9.9.9/32
>  Known via "bgp 100", distance 20, metric 0
>  Tag 10, type external
>  Last update from 192.168.1.2 00:44:52 ago
>  Routing Descriptor Blocks:
>  * 192.168.1.2, from 192.168.1.2, 00:44:52 ago, recursive-via-conn
>    Route metric is 0, traffic share count is 1
>    AS Hops 2
>    Route tag 10
>    MPLS label: none
>  [RPR]192.168.3.2, from 172.16.1.2, 00:44:52 ago
>    Route metric is 0, traffic share count is 1
>    AS Hops 2
>    Route tag 10
>    MPLS label: none
```

Related Commands

Command	Description
show interfaces tunnel	Displays tunnel interface information.
show ip route summary	Displays the current state of the routing table in summary format.

show ip route vrf

To display the IP routing table associated with a specific VPN routing and forwarding (VRF) instance, use the **show ip route vrf** command in user EXEC or privileged EXEC mode.

show ip route vrf *vrf-name* [**connected**| *protocol* [*as-number*]]| **list** [*list-number*]]| **profile**| **static**| **summary**| [*ip-prefix*| *ip-address*] [*mask*| **longer-prefixes**]]| **repair-paths**| **dhcp**| **supernets-only**| **tag** {*tag-value*| *tag-value-dotted-decimal* [*mask*]}]

Syntax Description

<i>vrf-name</i>	Name of the VRF.
connected	(Optional) Displays all connected routes in a VRF.
<i>protocol</i>	(Optional) Routing protocol. To specify a routing protocol, use one of the following keywords: bgp , egp , eigrp , hello , igrp , isis , ospf , or rip .
<i>as-number</i>	(Optional) Autonomous system number.
list number	(Optional) Specifies the IP access list to be displayed.
profile	(Optional) Displays the IP routing table profile.
static	(Optional) Displays static routes.
summary	(Optional) Displays a summary of routes.
<i>ip-prefix</i>	(Optional) Network for which routing information is displayed.
<i>ip-address</i>	(Optional) Address for which routing information is displayed.
<i>mask</i>	(Optional) Network mask.
longer-prefixes	(Optional) Displays longer prefix entries.
repair-paths	(Optional) Displays repair paths.
dhcp	(Optional) Displays routes added by the DHCP server.
supernets-only	(Optional) Displays only supernet entries.
tag	(Optional) Displays information about route tags in the VRF table.
<i>tag-value</i>	(Optional) Route tag values as a plain decimals.

<i>tag-value-dotted-decimal</i>	(Optional) Route tag values as a dotted decimals.
<i>mask</i>	(Optional) Route tag wildcard mask.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(2)T	This command was modified. The <i>ip-prefix</i> argument was added. The command output was enhanced to display information on multipaths to the specified network.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(22)S	This command was modified. Support for Enhanced Interior Gateway Routing Protocol (EIGRP) VRFs was added.
12.2(15)T	This command was modified. Support for EIGRP VRFs was added.
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.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH. The output was enhanced to display remote label information and corresponding Multiprotocol Label Switching (MPLS) flags for prefixes that have remote labels stored in the Routing Information Base (RIB).
12.2(33)SRE	This command was modified. The repair-paths , dhcp , and supernets-only keywords were added. Support for the Border Gateway Protocol (BGP) Best External and BGP Additional Path features was added.
12.2(33)XNE	This command was integrated into Cisco IOS Release 12.2(33)XNE.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.2(2)S	This command was modified. The tag keyword and <i>tag-value</i> , <i>tag-value-dotted-decimal</i> , and <i>mask</i> arguments were added to enable the display of route tags as plain or dotted decimals in the command output.
Cisco IOS XE Release 3.6S	This command was modified. The tag keyword and <i>tag-value</i> , <i>tag-value-dotted-decimal</i> , and <i>mask</i> arguments were added to enable the display of route tags as plain or dotted decimals in the command output.
15.2(4)S	This command was implemented on the Cisco 7200 series router.

Release	Modification
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Examples

The following sample output displays the IP routing table associated with the VRF named vrf1:

```
Device# show ip route vrf vrf1
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
        I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
        U - per-user static route, o - ODR
        T - traffic engineered route
```

```
Gateway of last resort is not set
```

```
B   10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:19
C   10.0.0.0/8 is directly connected, Ethernet1/3
B   10.0.0.0/8 [20/0] via 10.0.0.1, 02:10:22
B   10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:20
```

This following sample output shows BGP entries in the IP routing table associated with the VRF named vrf1:

```
Device# show ip route vrf vrf1 bgp
```

```
B 10.0.0.0/8 [200/0] via 10.13.13.13, 03:44:14
B 10.0.0.0/8 [20/0] via 10.0.0.1, 03:44:12
B 10.0.0.0/8 [200/0] via 10.13.13.13, 03:43:14
```

The following sample output displays the IP routing table associated with a VRF named PATH:

```
Device# show ip route vrf PATH 10.22.22.0
```

```
Routing entry for 10.22.22.0/24
  Known via "bgp 1", distance 200, metric 0
  Tag 22, type internal
  Last update from 10.22.5.10 00:01:07 ago
  Routing Descriptor Blocks:
  * 10.22.7.8 (Default-IP-Routing-Table), from 10.11.3.4, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.22.1.9 (Default-IP-Routing-Table), from 10.11.1.2, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.22.6.10 (Default-IP-Routing-Table), from 10.11.6.7, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.22.4.10 (Default-IP-Routing-Table), from 10.11.4.5, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
  10.22.5.10 (Default-IP-Routing-Table), from 10.11.5.6, 00:01:07 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
```

The following sample output from the **show ip route vrf vrf-name tag** command displays route tag information for routes associated with vrf1. The route tags in the sample output are displayed in dotted decimal format.

```
Device# show ip route vrf vrf1 tag 5
```

```
Routing Table: vrf1
Routing entry for 10.0.0.1/24
  Known via "static", distance 1, metric 0 (connected)
  Tag 0.0.0.5
  Routing Descriptor Blocks:
```



```
* directly connected, via Null0
  Route metric is 0, traffic share count is 1
  Route tag 0.0.0.5
```

The following sample outputs from the **show ip route vrf** command include recursive-via-host and recursive-via-connected flags:

```
Device# show ip route vrf v2 10.2.2.2
```

```
Routing Table: v2
Routing entry for 10.2.2.2/32
  Known via "bgp 10", distance 20, metric 0
  Tag 100, type external
  Last update from 192.168.1.1 00:15:54 ago
Routing Descriptor Blocks:
  * 192.168.1.1, from 192.168.1.1, 00:15:54 ago, recursive-via-conn
    Route metric is 0, traffic share count is 1
    AS Hops 1
    Route tag 100
    MPLS label: none
```

```
Device# show ip route vrf v2 10.2.2.2
```

```
Routing Table: v2
Routing entry for 10.2.2.2/32
  Known via "bgp 10", distance 200, metric 0
  Tag 100, type internal
  Last update from 10.3.3.3 00:18:11 ago
Routing Descriptor Blocks:
  * 10.3.3.3 (default), from 10.5.5.5, 00:18:11 ago, recursive-via-host
    Route metric is 0, traffic share count is 1
    AS Hops 1
    Route tag 100
    MPLS label: 16
    MPLS Flags: MPLS Required
```

The table below describes the significant fields shown in the displays.

Table 88: show ip route vrf Field Descriptions

Field	Description
Routing entry for 10.22.22.0/24	Network number.
Known via ...	Indicates how the route was derived.
distance	Administrative distance of the information source.
metric	Metric used to reach the destination network.
Tag	Integer used to tag the route.
type	Indicates whether the route is an L1 type or L2 type of route.
Last update from 10.22.5.10	Indicates the IP address of the device that is the next hop to the remote network and identifies the interface on which the last update arrived.
00:01:07 ago	Specifies the last time the route was updated (in hours:minutes:seconds).

Field	Description
Routing Descriptor Blocks	Displays the next-hop IP address followed by the information source.
10.22.6.10, from 10.11.6.7, 00:01:07 ago	Indicates the next-hop address, the address of the gateway that sent the update, and the time that has elapsed since this update was received (in hours:minutes:seconds).
Route metric	This value is the best metric for this routing descriptor block.
Traffic share count	Indicates the number of packets transmitted over various routes.
AS Hops	Number of hops to the destination or to the device where the route first enters internal BGP (iBGP).

The following is sample output from the **show ip route vrf** command on devices using the Cisco IOS Software Modularity for Layer 3 VPNs feature. The output includes remote label information and corresponding MPLS flags for prefixes that have remote labels stored in the RIB if BGP is the label distribution protocol.

```
Device# show ip route vrf v2 10.2.2.2
Routing entry for 10.2.2.2/32
  Known via "bgp 1", distance 200, metric 0, type internal
  Redistributing via ospf 2
  Advertised by ospf 2 subnets
  Last update from 10.0.0.4 00:22:59 ago
  Routing Descriptor Blocks:
    * 10.0.0.4 (Default-IP-Routing-Table), from 10.0.0.31, 00:22:59 ago
      Route metric is 0, traffic share count is 1
      AS Hops 0
      MPLS label: 1300
      MPLS Flags: MPLS Required
```

The table below describes the significant fields shown in the display.

Table 89: show ip route vrf Field Descriptions

Field	Description
MPLS label	Displays the BGP prefix from the BGP peer. The output shows one of the following values: • A label value (16–1048575). • A reserved label value, such as explicit-null or implicit-null. • The word “none” if no label is received from the peer. The MPLS label field is not displayed if any of the following conditions is true: • BGP is not the Label Distribution Protocol (LDP). However, Open Shortest Path First (OSPF) prefixes learned via sham links display an MPLS label. • MPLS is not supported. • The prefix is imported from another VRF, where the prefix was an Interior Gateway Protocol (IGP) prefix and LDP provided the remote label for it.
MPLS Flags	Name of the MPLS flag. One of the following MPLS flags is displayed: • MPLS Required—Indicates that packets are forwarded to this prefix because of the presence of the MPLS label stack. If MPLS is disabled on the outgoing interface, the packets are dropped. • No Global—Indicates that MPLS packets for this prefix are forwarded from the VRF interface and not from the interface in the global table. VRF interfaces prevent loops in scenarios that use iBGP multipaths. • NSF—Indicates that the prefix is from a nonstop forwarding (NSF)-aware neighbor. If the routing information temporarily disappears due to a disruption in the control plane, packets for this prefix are preserved.

The following sample output from the **show ip route vrf** command shows repair paths in the routing table. The fields in the display are self-explanatory.

```
Device> show ip route vrf test1 repair-paths 192.168.3.0

Routing Table: test1
Routing entry for 192.168.3.0/24
  Known via "bgp 10", distance 20, metric 0
  Tag 100, type external
  Last update from 192.168.1.1 00:49:39 ago
Routing Descriptor Blocks:
  * 192.168.1.1, from 192.168.1.1, 00:49:39 ago, recursive-via-conn
    Route metric is 0, traffic share count is 1
    AS Hops 1
    Route tag 100
    MPLS label: none
  [RPR]10.4.4.4 (default), from 10.5.5.5, 00:49:39 ago, recursive-via-host
    Route metric is 0, traffic share count is 1
    AS Hops 1
    Route tag 100
    MPLS label: 29
MPLS Flags: MPLS Required, No Global
```

Related Commands

Command	Description
show ip cache	Displays the Cisco Express Forwarding table associated with a VRF.
show ip vrf	Displays the set of defined VRFs and associated interfaces.

show tcp ha connections

To display connection-ID-to-TCP mapping data, use the **show tcp ha connections** command in privileged EXEC mode.

show tcp ha connections

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.2(28)SB	This command was introduced.
	15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
	Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines The **show tcp ha connections** command is used to display connection-ID-to-TCP mapping data.

Examples The following is sample output from the **show tcp ha connections** command:

```
Router# show tcp ha connections
SSO enabled for 40 connections
TCB      Local Address      Foreign Address      (state)      Conn Id
71EACE60 10.0.56.1.179        10.0.56.3.58671     ESTAB        37
71EA9320 10.0.53.1.179        10.0.53.3.58659     ESTAB        34
71EA35F8 10.0.41.1.179        10.0.41.3.58650     ESTAB        22
71A21FE0 10.0.39.1.179        10.0.39.3.58641     ESTAB        20
71EAA6E0 10.0.54.1.179        10.0.54.3.58663     ESTAB        35
71EA2238 10.0.40.1.179        10.0.40.3.58646     ESTAB        21
71EABAA0 10.0.55.1.179        10.0.55.3.58667     ESTAB        36
71EAE710 10.0.28.1.179        10.0.28.3.58676     ESTAB        9
71EA2728 10.0.50.1.179        10.0.50.3.58647     ESTAB        31
720541D8 10.0.49.1.179        10.0.49.3.58642     ESTAB        30
71EAA1F0 10.0.44.1.179        10.0.44.3.58662     ESTAB        25
2180B3A8 10.0.33.1.179        10.0.33.3.58657     ESTAB        14
71EAB5B0 10.0.45.1.179        10.0.45.3.58666     ESTAB        26
21809FE8 10.0.32.1.179        10.0.32.3.58653     ESTAB        13
71EA8E30 10.0.43.1.179        10.0.43.3.58658     ESTAB        24
71EAD350 10.0.27.1.179        10.0.27.3.58672     ESTAB        8
2180A9C8 10.0.52.1.179        10.0.52.3.58655     ESTAB        33
2180A4D8 10.0.42.1.179        10.0.42.3.58654     ESTAB        23
71EABF90 10.0.26.1.179        10.0.26.3.58668     ESTAB        7
71EA3AE8 10.0.51.1.179        10.0.51.3.58651     ESTAB        32
720546C8 10.0.59.1.179        10.0.59.3.58643     ESTAB        40
```

The table below describes the significant fields shown in the display.

Table 90: show tcp ha connections Field Descriptions

Field	Description
SSO enabled for	Displays the number of TCP connections that support BGP Nonstop Routing (NSR) with SSO.
TCB	An internal identifier for the endpoint.
Local Address	The local IP address and port.
Foreign Address	The foreign IP address and port (at the opposite end of the connection).
(state)	TCP connection state. A connection progresses through a series of states during its lifetime. The states that follow are shown in the order in which a connection progresses through them. • LISTEN--Waiting for a connection request from any remote TCP and port. • SYNSENT--Waiting for a matching connection request after having sent a connection request. • SYNRCVD--Waiting for a confirming connection request acknowledgment after having both received and sent a connection request. • ESTAB--Indicates an open connection; data received can be delivered to the user. This is the normal state for the data transfer phase of the connection. • FINWAIT1--Waiting for a connection termination request from the remote TCP or an acknowledgment of the connection termination request previously sent.
Conn id	Identifying number of the TCP connection.

slow-peer detection

To use a policy template to specify a threshold time that dynamically determines a BGP slow peer, use the **slow-peer detection** command in policy template configuration mode. To restore the default value, use the **no** form of this command.

slow-peer detection [**threshold** *seconds*]

no slow-peer detection

Syntax Description

threshold <i>seconds</i>	(Optional) Specifies the threshold time in seconds that the timestamp of the oldest message in a peers queue can be lagging behind the current time before the BGP peer is determined to be a slow peer. The range is from 120 to 3600; the default is 300.

Command Default

300 seconds

Command Modes

Policy template configuration (config-router-ptmp)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines

Update messages are timestamped when they are formatted. The timestamp of the oldest update message in a peers queue is compared to the current time to determine if the peer is lagging more than the configured number of seconds. When a peer is dynamically detected to be a slow peer, the system will send a syslog message. The peer will be marked as recovered and another syslog message will be generated only after the peer's update group converges.



Note

The **neighbor slow-peer detection** command performs the same function as the **bgp slow-peer detection** command (at the address-family level), except that the **neighbor slow-peer detection** command overrides the address-family level command. When the **neighbor slow-peer detection** command is unconfigured, the system will function according to the address-family level configuration. The **slow-peer detection** command performs the same function through a peer policy template.

Examples

The following example specifies that if the timestamp on a peer's update message is more than 360 seconds before the current time, the peer that sent the update message is considered to be slow. The commands configured under the peer-policy template will be applied to the neighbor once it inherits the peer-policy.

```
Router(config)# router bgp 13
Router(config-router)# template peer-policy ipv4 ucast ppl
Router(config-router-ptmp)# slow-peer detection threshold 360
Router(config-router-ptmp)# slow-peer split-update-group dynamic
```

Related Commands

Command	Description
bgp slow-peer detection	Specifies a threshold time that dynamically determines a slow peer.
bgp slow-peer split-update-group dynamic	Moves a dynamically detected slow peer to a slow update group.
clear ip bgp slow	Moves dynamically configured slow peers back to their original update groups.
neighbor slow-peer split-update-group dynamic	Moves a dynamically detected slow peer to a slow update group.
slow-peer split-update-group dynamic	Moves a dynamically detected slow peer to a slow update group.

slow-peer split-update-group dynamic

To use a policy template to move a dynamically detected slow peer to a slow update group, use the **slow-peer split-update-group dynamic** command in policy template configuration mode. To disable dynamically detected slow peers from being moved to a slow update group, use the **no** form of this command.

slow-peer split-update-group dynamic [permanent]

no slow-peer split-update-group dynamic

Syntax Description

permanent	(Optional) Specifies that after the slow peer becomes a regular peer (converges), it is not moved back to its original update group automatically. It remains in the slow update group until the network administrator uses one of the clear slow commands to move the peer to its original update group.

Command Default

No dynamically detected slow peer is moved to a slow peer update group.

Command Modes

Policy template (config-router-ptmp)

Command History

Release	Modification
15.0(1)S	This command was introduced.
Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines

When a peer is dynamically detected to be a slow peer, the slow peer is moved to a slow update group. If a *static* slow peer update group exists, the dynamic slow peer is moved to the static slow peer update group; otherwise, a new slow peer update group is created and the peer is moved to that group.

- We recommend you configure the **permanent** keyword. If the **permanent** keyword is configured, the peer is not automatically moved to its original update group. After you resolve the root cause of the slow peer, you can use the **clear bgp slow** command to move the peer back to its original update group.
- If the **permanent** keyword is not configured, the slow peer will be moved back to its regular original update group after it becomes a regular peer (converges).

**Note**

The **neighbor slow-peer split-update-group dynamic** command performs the same function as the **bgp slow-peer split-update-group dynamic** command (at the address-family level), except that the **neighbor slow-peer split-update-group dynamic** command overrides the address-family level command. When the **neighbor slow-peer split-update-group dynamic** command is unconfigured, the system will function according to the address-family level configuration. The **slow-peer split-update-group dynamic** command performs the same function through a policy template.

If **slow-peer split-update-group dynamic** is configured, but no slow peer detection is configured, the detection will be done at the default threshold of 300 seconds. That is, detection is enabled automatically with its default threshold.

Examples

In the following example, the timestamp of the oldest message in a peers queue is compared to the current time to determine if the peer is lagging more than 360 seconds. If it is, the neighbor that sent the message is determined to be a slow peer, and is put in the slow peer update group. Because the **permanent** keyword is not configured, the slow peer will be moved back to its regular original update group after it becomes a regular peer (converges).

```
Router(config)# router bgp 13
Router(config-router)# template peer-policy ipv4_ucast_pp1
Router(config-router-ptmp)# slow-peer detection threshold 360
Router(config-router-ptmp)# slow-peer split-update-group dynamic
```

Related Commands

Command	Description
slow-peer detection	Specifies a threshold time that dynamically determines a slow peer.
show ip bgp template peer-policy	Displays locally configured peer policy templates.

slow-peer split-update-group static

To mark a BGP neighbor as a slow peer and move it to a slow update group, use the **slow-peer split-update-group static** command by using a peer policy template. To unmark the slow peer and return it to its original update group, use the **no** form of this command.

slow-peer split-update-group static

no slow-peer split-update-group static

Syntax Description This command has no arguments or keywords.

Command Default No peer is marked as slow and moved to a slow peer update group in a static manner using a peer policy template.

Command Modes Peer policy template (config-router-ptmp)

Command History	Release	Modification
	15.0(1)S	This command was introduced.
	Cisco IOS XE 3.1S	This command was introduced.

Usage Guidelines Configure a static slow peer when the peer is known to be slow (perhaps due to a slow link or low processing power).
The **neighbor slow-peer split-update-group static** command performs the same function in address-family mode.

Examples In the following example, the neighbor is marked as a slow peer and is moved to a slow update group.

```
Router(config)# router bgp 13
Router(config-router)# template peer-policy ipv4 ucast ppl
Router(config-router-ptmp)# slow-peer split-update-group static
```

Related Commands	Command	Description
	neighbor slow-peer split-update-group static	Marks a BGP neighbor as a slow peer and moves it to a slow update group.

soo

To set the site-of-origin (SoO) value for a Border Gateway Protocol (BGP) peer policy template, use the **soo** command in policy-template configuration mode. To remove the SoO value, use the **no** form of this command.

soo *extended-community-value*

no soo

Syntax Description

<i>extended-community-value</i>	Specifies the VPN extended community value. The value takes one of the following formats: • A 16-bit autonomous system number, a colon, and a 32-bit number, for example: 45000:3 • A 32-bit IP address, a colon, and a 16-bit number, for example: 192.168.10.2:51 In Cisco IOS Release 12.4(24)T, 4-byte autonomous system numbers are supported in the range from 1.0 to 65535.65535 in asdot notation only. In Cisco IOS XE Release 2.4, and later releases, 4-byte autonomous system numbers are supported in the range from 65536 to 4294967295 in asplain notation and in the range from 1.0 to 65535.65535 in asdot notation. For more details about autonomous system number formats, see the router bgp command.

Command Default

No SoO value is set for a BGP peer policy template.

Command Modes

Policy-template configuration (config-router-ptmp)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.
12.4(24)T	Support for 4-byte autonomous system numbers in asdot notation only was added.

Release	Modification
Cisco IOS XE Release 2.4	This command was modified. Support for asplain notation was added and the default format for 4-byte autonomous system numbers is now asplain.
12.2(33)SRE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
12.2(33)XNE	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.
Cisco IOS XE Release 3.3SG	This command was modified. Support for displaying 4-byte autonomous system numbers in asplain and asdot notation was added.

Usage Guidelines

Use this command to set the SoO value for a BGP peer policy template that a BGP neighbor can inherit. The SoO value is set for a peer policy template, and a BGP neighbor is identified under address family IPv4 VRF configuration mode to inherit the peer policy that contains the SoO value.

The SoO extended community is a BGP extended community attribute that is used to identify routes that have originated from a site so that the readvertisement of that prefix back to the source site can be prevented. The SoO extended community uniquely identifies the site from which a router has learned a route. BGP can use the SoO value associated with a route to prevent routing loops.

In releases prior to Cisco IOS Release 12.4(11)T, 12.2(33)SRB, and 12.2(33)SB, the SoO extended community attribute is configured using an inbound route map that sets the SoO value during the update process. The introduction of the **neighbor soo** and **soo** commands simplifies the SoO value configuration.

In Cisco IOS Release 12.4(24)T, the Cisco implementation of 4-byte autonomous system numbers uses asdot--1.2 for example--as the only configuration format, regular expression match, and output display, with no asplain support.

In Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain--65538 for example--as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the **bgp asnotation dot** command followed by the **clear ip bgp *** command to perform a hard reset of all current BGP sessions.



Note

If a BGP peer inherits from several peer policy templates that specify different SoO values, the SoO value in the last template applied takes precedence and is applied to the peer. However, direct configuration of the SoO value on the BGP neighbor overrides any inherited template configurations of the SoO value.

Examples

The following example shows how to create a peer policy template and configure an SoO value as part of the peer policy. Under address family IPv4 VRF, a neighbor is identified and configured to inherit the peer policy that contains the SoO value.

```
router bgp 45000
 template peer-policy SOO_POLICY
   soo 45000:3
 exit-peer-policy
 address-family ipv4 vrf SOO_VRF
   neighbor 192.168.3.2 remote-as 50000
   neighbor 192.168.3.2 activate
   neighbor 192.168.3.2 inherit peer-policy SOO_POLICY
 end
```

The following example shows how to create a peer policy template and configure an SoO value using a 4-byte autonomous system number, 1.2 in asdot format, as part of the peer policy. Under address family IPv4 VRF, a neighbor is identified and configured to inherit the peer policy that contains the SoO value. This example requires Cisco IOS Release 12.4(24)T, Cisco IOS XE Release 2.4, or a later release.

```
router bgp 1.2
 template peer-policy SOO_POLICY
   soo 1.2:3
 exit-peer-policy
 address-family ipv4 vrf SOO_VRF
   neighbor 192.168.3.2 remote-as 1.14
   neighbor 192.168.3.2 activate
   neighbor 192.168.3.2 inherit peer-policy SOO_POLICY
 end
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Enters address family configuration mode to configure a routing session using standard IP Version 4 address prefixes.
neighbor soo	Sets the SoO value for a BGP neighbor or peer group.
router bgp	Configures the BGP routing process.
template peer-policy	Creates a peer policy template and enters policy-template configuration mode.

stats-reporting-period (bmp)

To configure the time interval in which the BGP Monitoring Protocol (BMP) server receives the statistics report from the BGP BMP neighbors, use the **stats-reporting-period** command in BMP server configuration mode. To disable the reporting period for statistics, use the **no** form of the command.

stats-reporting-period *report-period*

no stats-reporting-period

Syntax Description

<i>report-period</i>	Specifies the interval, in seconds, in which a specific BMP server receives the statistics report from its connected BGP BMP neighbors. The value of the reporting period that you can configure, ranges from 1 to 3600 seconds.

Command Default

The BMP server does not receive statistics reporting from the BGP BMP neighbors at periodic intervals.

Command Modes

BMP server configuration (config-router-bmpsrvr)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use the **bmp server** command to enter BMP server configuration mode and configure a specific BMP server. To configure BGP BMP neighbors to which the BMP servers establish a connection, use the **neighbor bmp-activate** command in router configuration mode. Use the **show ip bgp bmp** command to verify the statistics reporting period that is configured for BMP server.

Examples

The following example show how to enter BMP server configuration mode and configure the statistics reporting period for BMP server 1 and 2:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp server 1
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 10.1.1.1 port-number 8000
Device(config-router-bmpsrvr)# stats-reporting-period 30
Device(config-router-bmpsrvr)# exit-bmp-server-mode
Device(config-router)# bmp server 2
Device(config-router-bmpsrvr)# activate
```

```
Device(config-router-bmpsrvr)# address 20.1.1.1 port-number 9000
Device(config-router-bmpsrvr)# stats-reporting-period 30
Device(config-router-bmpsrvr)# end
```

The following is sample output from the **show ip bgp bmp server** command for BMP server number 1 and 2. The statistics reporting interval on BMP server 1 and 2 has been set to 30 seconds, therefore each server receives statistics messages from its connected BGP BMP neighbor in each cycle of 30 seconds:

```
Device# show ip bgp bmp server summary
```

```
Number of BMP servers configured: 2
Number of BMP neighbors configured: 10
Number of neighbors on TransitionQ: 0, MonitoringQ: 0, ConfigQ: 0
Number of BMP servers on StatsQ: 0
BMP Refresh not in progress, refresh not scheduled
Initial Refresh Delay configured, refresh value 30s
BMP buffer size configured, buffer size 2048 MB, buffer size bytes used 0 MB
```

ID	Host/Net	Port	TCB	Status	Uptime	MsgSent	LastStat
1	10.1.1.1	8000	0x2A98B07138	Up	00:38:49	162	00:00:09
2	20.1.1.1	9000	0x2A98E17C88	Up	00:38:49	46	00:00:04

```
Device# show ip bgp bmp server summary
```

```
Number of BMP servers configured: 2
Number of BMP neighbors configured: 10
Number of neighbors on TransitionQ: 0, MonitoringQ: 0, ConfigQ: 0
Number of BMP servers on StatsQ: 0
BMP Refresh not in progress, refresh not scheduled
Initial Refresh Delay configured, refresh value 30s
BMP buffer size configured, buffer size 2048 MB, buffer size bytes used 0 MB
```

ID	Host/Net	Port	TCB	Status	Uptime	MsgSent	LastStat
1	10.1.1.1	8000	0x2A98B07138	Up	00:40:19	189	00:00:07
2	20.1.1.1	9000	0x2A98E17C88	Up	00:40:19	55	00:00:02

**Note**

If we configure several BGP BMP neighbors to be monitored by the BMP servers, for example 10, then 10 statistics messages are received by both servers in each periodic cycle that is configured.

Related Commands

Command	Description
bmp server	Enters BMP server configuration mode to configure specific BMP servers.
neighbor bmp-activate	Activates BMP monitoring for BGP neighbors.
show ip bgp bmp	Displays information about BMP servers and neighbors.

synchronization

To enable the synchronization between BGP and your Interior Gateway Protocol (IGP) system, use the **synchronization** command in address family or router configuration mode. To enable the Cisco IOS software to advertise a network route without waiting for the IGP, use the **no** form of this command.

synchronization

no synchronization

Syntax Description This command has no arguments or keywords.

Command Default The behavior of this command is disabled by default.

Command Modes Address family configuration
Router configuration

Command History	Release	Modification
	10.0	This command was introduced.
	12.0(7)T	Address family configuration mode was added.
	12.2(8)T	Command default behavior changed to disabled.
	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 Usually, a BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the IGP. By default, synchronization between BGP and the IGP is turned off to allow the Cisco IOS software to advertise a network route without waiting for route validation from the IGP. This feature allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems.

Use the **synchronization** command if routers in the autonomous system do not speak BGP.

Examples The following example shows how to enable synchronization in router configuration mode. The router validates the network route in its IGP before advertising the route externally.

```
router bgp 65120
 synchronization
```

The following example shows how to enable synchronization in address family configuration mode. The router validates the network route in its IGP before advertising the route externally.

```
router bgp 65120
address-family ipv4 unicast
  synchronization
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family vpnv4	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard VPN Version 4 address prefixes.

table-map

To specify a route map that modifies a metric, tag, or traffic index value (of routes that pass the route map) when the IP routing table is updated with BGP learned routes, or to selectively download BGP routes to the RIB, use the **table-map** command in address family or router configuration mode. To disable either function, use the **no** form of the command.

table-map *route-map-name* [**filter**]

no table-map *route-map-name* [**filter**]

Syntax Description

<i>route-map-name</i>	Name of the route map that controls what gets put into the BGP routing table (RIB).
filter	(Optional) Specifies that the route map controls not only the metrics on a BGP route, but also whether the route is downloaded into the RIB. A BGP route is not downloaded to the RIB if it is denied by the route map.

Command Default

This command is disabled by default.

Command Modes

Address family configuration (config-router-af)

Router configuration (config-router)

Command History

Release	Modification
10.0	This command was introduced.
12.0(7)T	This command was modified. Address family configuration mode 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.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
Cisco IOS XE Release 2.5	This command was modified. The filter keyword was added.

Release	Modification
Cisco IOS XE Release 3.9S	This command was modified. Support for the IPv6 address family was added.

Usage Guidelines

A table map references a route map that sets metrics, a tag value, or a traffic index for routes that are updated in the BGP routing table, or controls whether routes are downloaded to the RIB.

When the **table-map** command:

- Does not include the **filter** keyword, the route map referenced is used to set certain properties of a route before the route is installed (downloaded) into the RIB. The route is always downloaded, regardless of whether it is permitted or denied by the route map.
- Includes the **filter** keyword, the route map referenced also controls whether the BGP route is downloaded to the RIB. A BGP route is not downloaded to the RIB if it is denied by the route map.

You can use **match** clauses in the route map that the table map references. The route map can support existing policies similar to the ones available for inbound and outbound route maps of a neighbor, including **match as-path**, **match community**, **match extcommunity**, **match ip address prefix-list**, and **match ip next-hop**.

Unlike a route map, a table map is not followed by **match** or **set** commands.



Note

After changing the **table-map** configuration or the route map that it references, you must issue the **clear ip bgp table-map** command in order for the changes to take effect. The **clear ip bgp table-map** command causes a re-download of routes from BGP to the RIB.

Examples

In the following example, a prefix list called NEWNAME permits certain routes. Those routes are subject to the route map named TRAFFIC_BUCKET, which sets the traffic index of those routes to 5. That route map is referenced by the table map, which means that those routes are downloaded and installed in the RIB with their traffic index set to 5. The table map controls which routes had their traffic index set. Because the **filter** keyword is omitted, the table map does not filter routes from being downloaded and installed in the RIB.

```
ip prefix-list NEWNAME
 permit 192.168.35.0/24
 permit 192.168.36.0/24
!
route-map TRAFFIC_BUCKET
 match ip address prefix-list NEWNAME
 set traffic-index 5
!
router bgp 100
 address-family ipv4 unicast
  table-map TRAFFIC_BUCKET
!
clear ip bgp ipv4 unicast table-map
```

In the following example, the Selective Route Download feature is configured by specifying the **filter** keyword. Only routes that pass the route map named FEW_ROUTES are downloaded to the RIB:

```
ip prefix-list NAME3
 permit 192.168.1.1/24
 permit 192.168.5.1/24
```

```

route-map FEW_ROUTES permit 10
 match ip address prefix-list NAME3
!
router bgp 100
 neighbor 192.168.1.1 remote-as
 neighbor 192.168.5.1 remote-as
 address-family ipv4 unicast
  table-map FEW_ROUTES filter
!
clear ip bgp ipv4 unicast table-map

```

Related Commands

Command	Description
address-family ipv4 (BGP)	Places the router in address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Places the router in IPv6 address family configuration mode for configuring routing sessions, such as BGP, that use standard IPv6 address prefixes.
clear ip bgp table-map	Initiates a re-download of BGP routes to the RIB.
match as-path	Matches a BGP autonomous system path access list.
match community	Matches a community list number or name.
match extcommunity	Matches an extended community list name.
match ip address prefix-list	Matches routes that pass a prefix list.
match ip next-hop	Matches routes that have a next hop address passed by one of the access lists specified.
route-map (IP)	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.

template peer-policy

To create a peer policy template and enter policy-template configuration mode, use the **template peer-policy** command in router configuration mode. To remove a peer policy template, use the **no** form of this command.

template peer-policy *policy-template-name*

no template peer-policy *policy-template-name*

Syntax Description

<i>policy-template-name</i>	Name or tag for the peer policy template.

Command Default

Removing a peer policy template by using the no form of this command removes all policy configurations inside of the template.

Command Modes

Router configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
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

Peer policy templates are used to group and apply the configuration of commands that are applied within specific address-families and NLRI configuration mode. Peer policy templates are created and configured in peer policy configuration mode. BGP policy commands that are configured for specific address-families or NLRI configuration modes are configured in a peer policy template. The following BGP policy commands are supported by peer policy templates:

- **advertisement-interval**
- **allowas-in**
- **as-override**
- **capability**

- **default-originate**
- **distribute-list**
- **dmzlink-bw**
- **exit-peer-policy**
- **filter-list**
- **inherit peer-policy**
- **maximum-prefix**
- **next-hop-self**
- **next-hop-unchanged**
- **prefix-list**
- **remove-private-as**
- **route-map**
- **route-reflector-client**
- **send-community**
- **send-label**
- **soft-reconfiguration**
- **unsuppress-map**
- **weight**

Peer policy templates are used to configure BGP policy commands that are configured for neighbors that belong to specific address-families and NLRI configuration modes. Like peer session templates, peer policy templates are configured once and then applied to many neighbors through the direct application of a peer policy template or through inheritance from peer policy templates. The configuration of peer policy templates simplifies the configuration of BGP policy commands that are applied to all neighbors within an autonomous system.

Peer policy templates support direct and indirect inheritance from up to eight peer policy templates. Inherited peer policy templates are configured with sequence numbers like route-maps. An inherited peer policy template, like a route-map, is evaluated starting with the inherit statement with the lowest sequence number and ending with the highest sequence number. However, there is a difference; a peer policy template will not fall through like a route-map. Every sequence is evaluated, and if a BGP policy command is reapplied with different value, it will overwrite any previous value from a lower sequence number.

Peer policy templates support only general policy commands. BGP policy configuration commands that are configured only for specific address families or NLRI configuration modes are configured with peer policy templates.

**Note**

A BGP neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured to belong only to a peer group or to inherit policies from only peer templates.

Examples

The following example creates a peer policy template named CUSTOMER-A. This peer policy template is configured to inherit the configuration from the peer policy templates named PRIMARY-IN and GLOBAL.

```
Router(config-router)# template peer-policy CUSTOMER-A
Router(config-router-ptmp)# route-map SET-COMMUNITY in
Router(config-router-ptmp)# filter-list 20 in

Router(config-router-ptmp)# inherit peer-policy PRIMARY-IN 20
Router(config-router-ptmp)# inherit peer-policy GLOBAL 10
Router(config-router-ptmp)# exit-peer-policy
Router(config-router)#
```

Related Commands

Command	Description
advertisement-interval	Sets the minimum interval between the sending of BGP routing updates.
allowas-in	Configures PE routers to allow readvertisement of all prefixes containing duplicate autonomous system numbers.
as-override	Configures a PE router to override the ASN of a site with the ASN of a provider.
capability orf prefix-list	Configures outbound route filtering and advertises the capability to send and receive ORF updates to the neighbor routers.
default-originate	Originates a default route to the local router.
distribute-list	Distributes BGP neighbor information as specified in an access list.
dmzlink-bw	Advertises the bandwidth of links that are used to exit an autonomous system.
exit peer-policy	Exits policy-template configuration mode and enters router configuration mode.
filter-list	Sets up a BGP filter.
inherit peer-policy	Configures a peer policy template to inherit the configuration from another peer policy template.
maximum-prefix	Controls how many prefixes can be received from a neighbor.
neighbor inherit peer-policy	Configures a router to send a peer policy template to a neighbor so that the neighbor can inherit the configuration.

Command	Description
neighbor send-label	Enables a BGP router to send MPLS labels with BGP routes to a neighboring BGP router.
next-hop-self	Disables next-hop processing of BGP updates on the router.
next-hop-unchanged	Propagates the next- hop unchanged for iBGP paths to this router.
prefix-list	Specifies a prefix list, a CLNS filter set, or a CLNS filter expression to be used to filter BGP advertisements.
remove-private-as	Removes the private autonomous system number from outbound routing updates.
route-map	Defines the conditions for redistributing routes from one routing protocol into another, or enables policy routing.
route-reflector-client	Configures the router as a BGP route reflector and configures the specified neighbor as its client.
send-community	Specifies that the BGP community attribute should be sent to the specified neighbor.
show ip bgp template peer-policy	Displays locally configured peer policy templates.
show ip bgp template peer-session	Displays locally configured peer session templates.
soft-reconfiguration	Configures the Cisco IOS software to start storing updates.
template peer-session	Creates a peer session template and enters session-template configuration mode.
unsuppress-map	Selectively unsuppresses suppressed routes.
weight	Assigns a weight to a neighbor connection.

template peer-session

To create a peer session template and enter session-template configuration mode, use the **template peer-session** command in router configuration mode. To remove a peer session template, use the **no** form of this command.

template peer-session *session-template-name*

no template peer-session *session-template-name*

Syntax Description

<i>session-template-name</i>	Name or tag for the peer session template.

Command Default

Removing a peer session template by using the **no** form of this command removes all session command configurations inside of the template.

Command Modes

Address family configuration
Router configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
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

Peer session templates are used to group and apply the configuration of general session commands to groups of neighbors that share common session configuration elements. General session commands that are common for neighbors that are configured in different address families can be configured within the same peer session template. Peer session templates are created and configured in peer session configuration mode. Only general session commands can be configured in a peer session template. The following general session commands are supported by peer session templates:

- **description**
- **disable-connected-check**
- **ebgp-multihop**

- **exit peer-session**
- **inherit peer-session**
- **local-as**
- **password**
- **remote-as**
- **shutdown**
- **timers**
- **translate-update**
- **update-source**
- **version**

General session commands can be configured once in a peer session template and then applied to many neighbors through the direct application of a peer session template or through indirect inheritance from a peer session template. The configuration of peer session templates simplify the configuration of general session commands that are commonly applied to all neighbors within an autonomous system.

Peer session templates support direct and indirect inheritance. A peer can be configured with only one peer session template at a time, and that peer session template can contain only one indirectly inherited peer session template. However, each inherited session template can also contain one indirectly inherited peer session template. So, only one directly applied peer session template and up to seven additional indirectly inherited peer session templates can be applied, allowing you to apply up to a maximum of eight peer session configurations to a neighbor: the configuration from the directly inherited peer session template and the configurations from up to seven indirectly inherited peer session templates. Inherited peer session templates are evaluated first, and the directly applied template will be evaluated and applied last. So, if a general session command is reapplied with a different value, the subsequent value will have priority and overwrite the previous value that was configured in the indirectly inherited template.

Peer session templates support only general session commands. BGP policy configuration commands that are configured only for specific address families or NLRI configuration modes are configured with peer policy templates.

**Note**

A BGP neighbor cannot be configured to work with both peer groups and peer templates. A BGP neighbor can be configured only to belong to a peer group or to inherit policies from peer templates.

Examples

The following example creates a peer session template named CORE1. This example inherits the configuration of the peer session template named INTERNAL-BGP.

```
Router(config-router)# template peer-session CORE1
Router(config-router-stmp)# description CORE-123
Router(config-router-stmp)# update-source loopback 1
Router(config-router-stmp)# inherit peer-session INTERNAL-BGP
Router(config-router-stmp)# exit-peer-session
Router(config-router)#
```

Related Commands

Command	Description
description	Configures a description to be displayed by the local or a peer router.
disable-connected-check	Disables connection verification for eBGP peers no more than one hop away when the eBGP peer is configured with a loopback interface.
ebgp-multihop	Accepts or initiates BGP connections to external peers residing on networks that are not directly connected.
exit peer-session	Exits session-template configuration mode and enters router configuration mode.
inherit peer-session	Configures a peer session template to inherit the configuration from another peer session template.
local-as	Allows the customization of the autonomous system number for eBGP peer groupings.
neighbor inherit peer-session	Configures a router to send a peer session template to a neighbor so that the neighbor can inherit the configuration.
neighbor translate-update	Upgrades a router running BGP in the NLRI format to support multiprotocol BGP.
password	Enables MD5 authentication on a TCP connection between two BGP peers.
remote-as	Adds an entry to the BGP or multiprotocol BGP neighbor table.
show ip bgp template peer-policy	Displays locally configured peer policy templates.
show ip bgp template peer-session	Displays locally configured peer session templates.
shutdown	Disables a neighbor or peer group.
timers bgp	Adjusts BGP network timers.
update-source	Specifies that the Cisco IOS software allow internal BGP sessions to use any operational interface for TCP connections.
version	Configures the Cisco IOS software to accept only a particular BGP version.

timers bgp

To adjust BGP network timers, use the **timers bgp** command in router configuration mode. To reset the BGP timing defaults, use the **no** form of this command.

timers bgp *keepalive holdtime* [*min-holdtime*]

no timers bgp

Syntax Description

<i>keepalive</i>	Frequency (in seconds) with which the Cisco IOS software sends <i>keepalive</i> messages to its peer. The default is 60 seconds. The range is from 0 to 65535.
<i>holdtime</i>	Interval (in seconds) after not receiving a <i>keepalive</i> message that the software declares a peer dead. The default is 180 seconds. The range is from 0 to 65535.
<i>min-holdtime</i>	(Optional) Interval (in seconds) specifying the minimum acceptable hold-time from a BGP neighbor. The minimum acceptable hold-time must be less than, or equal to, the interval specified in the <i>holdtime</i> argument. The range is from 0 to 65535.

Command Default

keepalive : 60 seconds *holdtime*: 180 seconds

Command Modes

Router configuration

Command History

Release	Modification
10.0	This command was introduced.
12.0(26)S	The <i>min-holdtime</i> argument was added.
12.3(7)T	The <i>min-holdtime</i> argument was added.
12.2(22)S	The <i>min-holdtime</i> argument was added.
12.2(27)SBC	The <i>min-holdtime</i> argument was added and this command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	The <i>min-holdtime</i> argument was added and this command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SXH	The <i>min-holdtime</i> argument was added and this command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

When configuring the *holdtime* argument for a value of less than twenty seconds, the following warning is displayed:

```
% Warning: A hold time of less than 20 seconds increases the chances of peer flapping
If the minimum acceptable hold-time interval is greater than the specified hold-time, a notification is displayed:
```

```
% Minimum acceptable hold time should be less than or equal to the configured hold time
```



Note

When the minimum acceptable hold-time is configured on a BGP router, a remote BGP peer session is established only if the remote peer is advertising a hold-time that is equal to, or greater than, the minimum acceptable hold-time interval. If the minimum acceptable hold-time interval is greater than the configured hold-time, the next time the remote session tries to establish, it will fail and the local router will send a notification stating “unacceptable hold time.”

Examples

The following example changes the keepalive timer to 70 seconds, the hold-time timer to 130 seconds, and the minimum acceptable hold-time interval to 100 seconds:

```
router bgp 45000
 timers bgp 70 130 100
```

Related Commands

Command	Description
clear ip bgp peer-group	Removes all the members of a BGP peer group.
router bgp	Configures the BGP routing process.
show ip bgp	Displays entries in the BGP routing table.

update-source (bmp)

To configure the interface source for routing updates on the BGP Monitoring Protocol (BMP) server, use the **update-source** command in BMP server configuration mode. To disable configuration of the interface source, use the **no** form of the command.

update-source *interface-type interface-number*

Syntax Description

<i>interface-type interface-number</i>	Specifies the interface type and number as the source for the BMP server routing updates.

Command Default

No interface source is configured on the BMP servers.

Command Modes

BMP server configuration (config-router-bmpsrvr)

Command History

Release	Modification
15.4(1)S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

Use the **bmp server** command to enter BMP server configuration mode and configure a specific BMP server. To configure BGP BMP neighbors to which the BMP servers establish a connection, use the **neighbor bmp-activate** command in router configuration mode. Use the **show running-config** command to verify the interface that has been configured.

Examples

The following example show how to enter BMP server configuration mode and configure an interface source for routing updates:

```
Device> enable
Device# configure terminal
Device(config)# router bgp 65000
Device(config-router)# bmp server 1
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 10.1.1.1 port-number 8000
Device(config-router-bmpsrvr)# update-source ethernet 0/0
Device(config-router-bmpsrvr)# exit-bmp-server-mode
Device(config-router)# bmp server 2
Device(config-router-bmpsrvr)# activate
Device(config-router-bmpsrvr)# address 20.1.1.1 port-number 9000
Device(config-router-bmpsrvr)# update-source ethernet 2/0
Device(config-router-bmpsrvr)# end
```


The following is sample output from the **show ip bgp bmp server** command for BMP server number 1 and 2. The “update-source” field in the output displays the interface source configured for BMP servers 1 and 2 for routing updates:

Device# **show running-config | section bmp**

```

bmp server 1
address 10.1.1.1 port-number 8000
description SERVER1
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
update-source Ethernet0/0
activate
exit-bmp-server-mode
bmp server 2
address 20.1.1.1 port-number 9000
description SERVER2
session-startup route-refresh
initial-delay 20
failure-retry-delay 40
flapping-delay 120
update-source Ethernet2/0
activate
exit-bmp-server-mode
neighbor 30.1.1.1 bmp-activate all
neighbor 40.1.1.1 bmp-activate all
neighbor 50.1.1.1 bmp-activate all
```

Related Commands

Command	Description
bmp server	Enters BMP server configuration mode to configure specific BMP servers.
neighbor bmp-activate	Activates BMP monitoring for BGP neighbors.
show running-config	Displays the running configuration on a device.

ve

To specify the Virtual Private LAN Service (VPLS) endpoint (VE) ID value or ID range value for a VPLS configuration, use the **ve** command in L2VPN VFI autodiscovery configuration mode. To remove the entry, use the **no** form of this command.

ve {**id** *id-value* | **range** *range-value*}

no ve {**id** | **range**}

Syntax Description

id <i>id-value</i>	ID value of the VE device. The range is from 1 to 16384.
range <i>range-value</i>	ID range value of the VE device. The range is from 11 to 512.

Command Default

No VE ID value or ID range value is specified.

Command Modes

L2VPN VFI autodiscovery configuration (config-vfi-autodiscovery)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

The **ve id** *id-value* command specifies the local VE identifier for the VFI for a VPLS configuration.

The VE ID identifies a VFI within a VPLS service. This means that VFIs in the same VPLS service cannot share the same VE ID. The scope of the VE ID is only within a bridge domain. Therefore, VFIs in different bridge domains within a PE can still use the same VE ID.

The **ve range** *range-value* command overrides the minimum size of the VE block. The default minimum size is 10. Any configured VE range must be higher than 10.

Examples

The following example specifies the VE with the ID value of 1001:

```
Device(config-vfi-autodiscovery)# ve id 1001
```

The following example specifies an ID range of 12:

```
Device(config-vfi-autodiscovery)# ve range 12
```

Related Commands

Command	Description
autodiscovery (MPLS)	Designates a Layer 2 VFI as having BGP autodiscovered pseudowire members.

 ve