



## show auto discovery qos through show ip rsvp hello client lsp detail

---

- [show auto discovery qos, page 3](#)
- [show auto qos, page 7](#)
- [show class-map, page 12](#)
- [show class-map type nat, page 15](#)
- [show class-map type port-filter, page 17](#)
- [show control-plane cef-exception counters, page 19](#)
- [show control-plane cef-exception features, page 21](#)
- [show control-plane counters, page 23](#)
- [show control-plane features, page 25](#)
- [show control-plane host counters, page 27](#)
- [show control-plane host features, page 29](#)
- [show control-plane host open-ports, page 31](#)
- [show control-plane transit counters, page 33](#)
- [show control-plane transit features, page 35](#)
- [show cops servers, page 37](#)
- [show crypto eng qos, page 38](#)
- [show crypto entropy status, page 39](#)
- [show frame-relay ip rtp header-compression, page 41](#)
- [show frame-relay ip tcp header-compression, page 46](#)
- [show interfaces fair-queue, page 49](#)
- [show interfaces random-detect, page 52](#)
- [show interfaces rate-limit, page 55](#)
- [show iphc-profile, page 58](#)

- [show ip nat translations rsvp, page 60](#)
- [show ip nbar attribute, page 62](#)
- [show ip nbar link-age, page 64](#)
- [show ip nbar pdlm, page 66](#)
- [show ip nbar port-map, page 67](#)
- [show ip nbar protocol activated, page 69](#)
- [show ip nbar protocol-attribute, page 70](#)
- [show ip nbar protocol-discovery, page 72](#)
- [show ip nbar protocol-id, page 76](#)
- [show ip nbar protocol-pack, page 88](#)
- [show ip nbar resources flow, page 90](#)
- [show ip nbar statistics , page 91](#)
- [show ip nbar trace, page 92](#)
- [show ip nbar unclassified-port-stats, page 94](#)
- [show ip nbar version, page 97](#)
- [show ip rsvp, page 100](#)
- [show ip rsvp aggregation ip, page 108](#)
- [show ip rsvp aggregation ip endpoints, page 112](#)
- [show ip rsvp atm-peak-rate-limit, page 116](#)
- [show ip rsvp authentication, page 118](#)
- [show ip rsvp counters, page 125](#)
- [show ip rsvp counters state teardown, page 129](#)
- [show ip rsvp fast bw-protect, page 131](#)
- [show ip rsvp fast detail, page 134](#)
- [show ip rsvp fast-reroute, page 139](#)
- [show ip rsvp fast-reroute bw-protect, page 143](#)
- [show ip rsvp fast-reroute detail, page 147](#)
- [show ip rsvp hello, page 153](#)
- [show ip rsvp hello client lsp detail, page 155](#)

# show auto discovery qos

To display the data collected during the Auto-Discovery (data collection) phase of the AutoQoS for the Enterprise feature, use the **show autodiscovery qos** command in privileged EXEC mode.

**show auto discovery qos** [**interface** *[type number]*]

## Syntax Description

<b>interface</b>	(Optional) Indicates that the configurations for a specific interface type will be displayed.
<i>type number</i>	(Optional) Specifies the interface type and number.

## Command Default

Displays the configurations created for all interface types.

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(11)T	Command output was modified to include suggested policy map information.

## Usage Guidelines

The suggested policy output (shown in the example below) lets you preview class maps and policy maps before you issue the **autoqos** command on an interface. You can then continue with the Auto-Discovery phase until more data is gathered or you can cut and paste the existing data and edit it as desired.

## Examples

The following is sample output from the **show autodiscovery qos** command. This example displays the data collected during the Auto-Discovery (data collection) phase using DSCP classification in trusted mode and includes suggested policy map information.

```
Router# show auto discovery qos
Serial2/1.1
AutoQoS Discovery enabled for trusted DSCP
Discovery up time: 2 hours, 42 minutes
AutoQoS Class information:
Class Voice:
  Recommended Minimum Bandwidth: 118 Kbps/1% (PeakRate)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
-----      (kbps/%)      (kbps/%)      (bytes)
-----
46/ef          106/1          118/1          129510064
Class Interactive Video:
```

```

Recommended Minimum Bandwidth: 25 Kbps/<1% (AverageRate)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
                (kbps/%)        (kbps/%)      (bytes)
-----
34/af41         25/<1            28/<1          31084292
Class Signaling:
Recommended Minimum Bandwidth: 50 Kbps/<1% (AverageRate)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
                (kbps/%)        (kbps/%)      (bytes)
-----
24/cs3         50/<1            56/<1          61838040
Class Streaming Video:
Recommended Minimum Bandwidth: 79 Kbps/<1% (AverageRate)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
                (kbps/%)        (kbps/%)      (bytes)
-----
32/cs4         79/<1            88/<1          96451788
Class Transactional:
Recommended Minimum Bandwidth: 105 Kbps/1% (AverageRate)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
                (kbps/%)        (kbps/%)      (bytes)
-----
18/af21         105/1            117/1          127798678
Class Bulk:
Recommended Minimum Bandwidth: 132 Kbps/1% (AverageRate)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
                (kbps/%)        (kbps/%)      (bytes)
-----
10/af11         132/1            147/1          160953984
Class Scavenger:
Recommended Minimum Bandwidth: 24 Kbps (AverageRate)/0% (fixed)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
                (kbps/%)        (kbps/%)      (bytes)
-----
8/cs1          24/<1            27/<1          30141238
Class Management:
Recommended Minimum Bandwidth: 34 Kbps/<1% (AverageRate)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
                (kbps/%)        (kbps/%)      (bytes)
-----
16/cs2         34/<1            38/<1          41419740
Class Routing:
Recommended Minimum Bandwidth: 7 Kbps/<1% (AverageRate)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
                (kbps/%)        (kbps/%)      (bytes)
-----
48/cs6         7/<1             7/<1           8634024
Class Best Effort:
Current Bandwidth Estimation: 820 Kbps/8% (AverageRate)
Detected DSCPs and data:
DSCP value      AverageRate      PeakRate      Total
                (kbps/%)        (kbps/%)      (bytes)
-----
0/default      820/8            915/9          997576380
Suggested AutoQoS Policy based on a discovery uptime of 2 hours, 42 minutes:
!
class-map match-any AutoQoS-Voice-Trust
 match ip dscp ef
!
class-map match-any AutoQoS-Inter-Video-Trust
 match ip dscp af41
!
class-map match-any AutoQoS-Signaling-Trust
 match ip dscp cs3
!

```

```

class-map match-any AutoQoS-Stream-Video-Trust
  match ip dscp cs4
!
class-map match-any AutoQoS-Transactional-Trust
  match ip dscp af21
  match ip dscp af22
  match ip dscp af23
!
class-map match-any AutoQoS-Bulk-Trust
  match ip dscp af11
  match ip dscp af12
  match ip dscp af13
!
class-map match-any AutoQoS-Scavenger-Trust
  match ip dscp cs1
!
class-map match-any AutoQoS-Management-Trust
  match ip dscp cs2
!
class-map match-any AutoQoS-Routing-Trust
  match ip dscp cs6
!
policy-map AutoQoS-Policy-S2/1.1Trust
  class AutoQoS-Voice-Trust
    priority percent 1
  class AutoQoS-Inter-Video-Trust
    bandwidth remaining percent 1
  class AutoQoS-Signaling-Trust
    bandwidth remaining percent 1
  class AutoQoS-Stream-Video-Trust
    bandwidth remaining percent 1
  class AutoQoS-Transactional-Trust
    bandwidth remaining percent 1
    random-detect dscp-based
  class AutoQoS-Bulk-Trust
    bandwidth remaining percent 1
    random-detect dscp-based
  class AutoQoS-Scavenger-Trust
    bandwidth remaining percent 1
  class AutoQoS-Management-Trust
    bandwidth remaining percent 1
  class AutoQoS-Routing-Trust
    bandwidth remaining percent 1
  class class-default
    fair-queue

```

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

**Table 1: show auto discovery qos Field Descriptions**

Field	Description
Serial2/1.1	The interface or subinterface on which data is being collected.
AutoQoS Discovery enabled for trusted DSCP	Indicates that the data collection phase of AutoQoS has been enabled.
Discovery up time	Indicates the period of time in which data was collected.
AutoQoS Class information	Displays information for each AutoQoS class.

Field	Description
Class Voice	Information for the named class, along with data pertaining to the detected applications. This data includes DSCP value, average rate (in kilobits per second (kbps)), peak rate (kbps), and total packets (bytes).
Suggested AutoQoS Policy based on a discovery uptime of hours and minutes	Policy-map and class-map statistics based on a specified discovery time.

**Related Commands**

Command	Description
<b>auto qos</b>	Installs the QoS class maps and policy maps created by the AutoQoS for the Enterprise feature.
<b>auto discovery qos</b>	Begins discovering and collecting data for configuring the AutoQoS for the Enterprise feature.
<b>show auto qos</b>	Displays the interface configurations, policy maps, and class maps created by AutoQoS on a specific interface or all interfaces.

## show auto qos

To display the interface configurations, policy maps, and class maps created by AutoQoS on a specific interface or all interfaces, use the **show auto qos** command in privileged EXEC mode.

**show auto qos** [**interface** [*type slot/ port*]]

### Syntax Description

<b>interface</b>	(Optional) Displays the configurations created by the AutoQoS--VoIP feature on all the interfaces or PVCs on which the AutoQoS--VoIP feature is enabled. <ul style="list-style-type: none"> <li>If you configure the <b>interface</b> keyword but do not specify an interface type, the <b>show auto qos interface</b> command displays the configurations created by the AutoQoS--VoIP feature on all the interfaces or PVCs on which the AutoQoS--VoIP feature is enabled.</li> </ul>
<i>type</i>	(Optional) Interface type; valid values are <b>atm</b> , <b>ethernet</b> , <b>fastethernet</b> , <b>ge-wan</b> , <b>gigabitethernet</b> , <b>pos</b> , and <b>tengigabitethernet</b> .
<i>slot / port</i>	(Optional) Slot and port number.

### Command Default

If no arguments or keywords are specified, configurations created for all interface types are displayed.

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
12.2(15)T	This command was introduced as part of the AutoQoS--VoIP feature.
12.3(7)T	This command was modified for the AutoQoS for the Enterprise feature. The output was modified to display the classes, class maps, and policy maps created on the basis of the data collected during the Auto-Discovery phase of the AutoQoS for the Enterprise feature.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.2(1)T	This command was modified. The output does not display the Frame Relay traffic shaping configuration.

## Usage Guidelines

The **showautoqosinterface** command can be used with Frame Relay data-link connection identifiers (DLCIs) and ATM PVCs.

When the AutoQoS--VoIP or the AutoQoS for the Enterprise features are enabled, configurations are generated for each interface or PVC. These configurations are then used to create the interface configurations, policy maps, class maps, and access control lists (ACLs) for use on the network. The **showautoqos** command can be used to verify the contents of the interface configurations, policy maps, class maps, and ACLs.

### Catalyst 6500 Series Switches

AutoQoS is supported on the following modules:

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

## Examples

### Examples

The **showautoqosinterfacetypeslot/port** command displays the configurations created by the AutoQoS--VoIP feature on the specified interface.

In the following example, the serial subinterface 6/1.1 has been specified:

```
Router# show auto qos interface serial 6/1.1
S6/1.1: DLCI 100 -
!
interface Serial6/1.1 point-to-point
  frame-relay interface-dlci 100
  class AutoQoS-VoIP-FR-Serial6/1-100
  frame-relay ip rtp header-compression
!
map-class frame-relay AutoQoS-VoIP-FR-Serial6/1-100
  frame-relay cir 512000
  frame-relay bc 5120
  frame-relay be 0
  frame-relay mincir 512000
  service-policy output AutoQoS-Policy-UnTrust
  frame-relay fragment 640
```

When the **interface** keyword is configured but an interface type is not specified, the **showautoqosinterface** command displays the configurations created by the AutoQoS--VoIP feature on all the interfaces or PVCs on which the AutoQoS--VoIP feature is enabled.

```
Router# show auto qos interface
Serial6/1.1: DLCI 100 -
!
interface Serial6/1.1 point-to-point
```

```

frame-relay interface-dlci 100
  class AutoQoS-VoIP-FR-Serial6/1-100
frame-relay ip rtp header-compression
!
map-class frame-relay AutoQoS-VoIP-FR-Serial6/1-100
frame-relay cir 512000
frame-relay bc 5120
frame-relay be 0
frame-relay mincir 512000
service-policy output AutoQoS-Policy-UnTrust
frame-relay fragment 640
ATM2/0.1: PVC 1/100 -
!
interface ATM2/0.1 point-to-point
  pvc 1/100
    tx-ring-limit 3
    encapsulation aal5mux ppp Virtual-Template200
!
interface Virtual-Template200
  bandwidth 512
  ip address 10.10.107.1 255.255.255.0
  service-policy output AutoQoS-Policy-UnTrust
  ppp multilink
  ppp multilink fragment-delay 10
  ppp multilink interleave

```

The following example displays all of the configurations created by the AutoQoS--VoIP feature:

```

Router# show auto qos
Serial6/1.1: DLCI 100 -
!
interface Serial6/1.1 point-to-point
  frame-relay interface-dlci 100
    class AutoQoS-VoIP-FR-Serial6/1-100
frame-relay ip rtp header-compression
!
map-class frame-relay AutoQoS-VoIP-FR-Serial6/1-100
frame-relay cir 512000
frame-relay bc 5120
frame-relay be 0
frame-relay mincir 512000
service-policy output AutoQoS-Policy-UnTrust
frame-relay fragment 640

```

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

**Table 2: show auto qos Field Descriptions (AutoQoS--VoIP Feature Configured)**

Field	Description
class AutoQoS-VoIP-FR-Serial6/1-100	Name of the class created by the AutoQoS-VoIP feature. In this instance, the name of the class is AutoQoS-VoIP-FR-Serial6/1-100.
service-policy output AutoQoS-Policy-UnTrust	Indicates that the policy map called "AutoQoS-Policy-UnTrust" has been attached to an interface in the outbound direction of the interface.

show auto qos interface Command: Configured for the AutoQoS for the Enterprise Feature

The following is sample output from the **showautoqos** command. This example displays the classes, class maps, and policy maps created on the basis of the data collected during the Auto-Discovery phase of the AutoQoS for the Enterprise feature.

```
Router# show auto qos
!
policy-map AutoQoS-Policy-Se2/1.1
class AutoQoS-Voice-Se2/1.1
  priority percent 70
  set dscp ef
class AutoQoS-Inter-Video-Se2/1.1
  bandwidth remaining percent 10
  set dscp af41
class AutoQoS-Stream-Video-Se2/1.1
  bandwidth remaining percent 1
  set dscp cs4
class AutoQoS-Transactional-Se2/1.1
  bandwidth remaining percent 1
  set dscp af21
class AutoQoS-Scavenger-Se2/1.1
  bandwidth remaining percent 1
  set dscp cs1
class class-default
  fair-queue
!
policy-map AutoQoS-Policy-Se2/1.1-Parent
class class-default
  shape average 1024000
  service-policy AutoQoS-Policy-Se2/1.1
!
class-map match-any AutoQoS-Stream-Video-Se2/1.1
match protocol cuseeme
!
class-map match-any AutoQoS-Transactional-Se2/1.1
match protocol sqlnet
!
class-map match-any AutoQoS-Voice-Se2/1.1
match protocol rtp audio
!
class-map match-any AutoQoS-Inter-Video-Se2/1.1
match protocol rtp video
!
rmon event 33333 log trap AutoQoS description "AutoQoS SNMP traps for Voice Drops" owner
AutoQoS
Serial2/1.1: DLCI 58 -
!
interface Serial2/1.1 point-to-point
frame-relay interface-dlci 58
  class AutoQoS-FR-Serial2/1-58
!
map-class frame-relay AutoQoS-FR-Serial2/1-58
frame-relay cir 1024000
frame-relay bc 10240
frame-relay be 0
frame-relay mincir 1024000
service-policy output AutoQoS-Policy-Se2/1.1-Parent
```

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

**Table 3: show auto qos Field Descriptions (AutoQoS for the Enterprise Feature Configured)**

Field	Description
policy-map AutoQoS-Policy-Se2/1.1	Name of the policy map created by the AutoQoS feature. In this instance, the name of the policy map is AutoQoS-Policy-Se2/1.1.

Field	Description
class AutoQoS-Voice-Se2/1.1 priority percent 70 set dscp ef	Name of the class created by the AutoQoS feature. In this instance, the name of the class is AutoQoS-Voice-Se2/1.1. Following the class name, the specific QoS features configured for the class are displayed.
class-map match-any AutoQoS-Stream-Video-Se2/1.1 match protocol cuseeme	Name of the class map and the packet matching criteria specified.

**Related Commands**

Command	Description
<b>auto discovery qos</b>	Begins discovering and collecting data for configuring the AutoQoS for the Enterprise feature.
<b>auto qos</b>	Installs the QoS class maps and policy maps created by the AutoQoS for the Enterprise feature.
<b>auto qos voip</b>	Configures the AutoQoS--VoIP feature on an interface.
<b>show auto discovery qos</b>	Displays the data collected during the Auto-Discovery phase of the AutoQoS for the Enterprise feature.

# show class-map

To display class maps and their matching criteria, use the **showclass-map** command in user EXEC or privileged EXEC mode.

## Cisco 3660, 3845, 6500, 7400, and 7500 Series Routers

```
show class-map [type {stack| access-control}] [ class-map-name ]
```

## Cisco 7600 and ASR 1000 Series Routers

```
show class-map [ class-map-name ]
```

### Syntax Description

<b>type stack</b>	(Optional) Displays class maps configured to determine the correct protocol stack in which to examine via flexible packet matching (FPM).
<b>type access-control</b>	(Optional) Displays class maps configured to determine the exact pattern to look for in the protocol stack of interest.
<i>class-map-name</i>	(Optional) Name of the class map. The class map name can be a maximum of 40 alphanumeric characters.

### Command Default

All class maps are displayed.

### Command Modes

User EXEC (>) Privileged EXEC (#)

### Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(13)T	This command was modified to display the Frame Relay data-link connection identifier (DLCI) number or Layer 3 packet length as a criterion for matching traffic inside a class map.
12.2(14)SX	This command was implemented on the Cisco 7600 series routers.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 and integrated into Cisco IOS Release 12.2(17d)SXB.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.4(4)T	The <b>type</b> , <b>stack</b> and <b>access-control</b> keywords were added to support FPM.
Cisco IOS XE Release 2.2	This command was implemented on Cisco ASR Aggregation Services 1000 series routers.
15.0(1)M	This command was modified. The output was modified to display encrypted filter information.

### Usage Guidelines

You can use the **showclass-map** command to display all class maps and their matching criteria. If you enter the optional *class-map-name* argument, the specified class map and its matching criteria will be displayed.

### Examples

In the following example, three class maps are defined. Packets that match access list 103 belong to class c3, IP packets belong to class c2, and packets ingressing through Ethernet interface 1/0 belong to class c1. The output from the **showclass-map** command shows the three defined class maps.

```
Router# show class-map
Class Map c3
Match access-group 103
Class Map c2
Match protocol ip
Class Map c1
Match input-interface Ethernet1/0
```

In the following example, a class map called c1 has been defined, and the Frame Relay DLCI number of 500 has been specified as a match criterion:

```
Router# show class-map
class map match-all c1
  match fr-dlci 500
```

The following example shows how to display class-map information for all class maps:

```
Router# show class-map
Class Map match-any class-default (id 0)
  Match any
Class Map match-any class-simple (id 2)
  Match any
Class Map match-all ipp5 (id 1)
  Match ip precedence 5
Class Map match-all agg-2 (id 3)
```

The following example shows how to display class-map information for a specific class map:

```
Router# show class-map ipp5
Class Map match-all ipp5 (id 1)
  Match ip precedence 5
```

The following is sample output from the **showclass-map type access-control** command for an encrypted FPM filter:

```
Router# show class-map type access-control accesscontrol1
Class Map type access-control match-all accesscontrol1 (id 4)
  Match encrypted FPM filter
    filter-hash      : FC50BED10521002B8A170F29AF059C53
    filter-version: 0.0_DummyVersion_20090101_1830
    filter-id       : cisco-sa-20090101-dummy_ddts_001
```

```
Match start TCP payload-start offset 0 size 10 regex "abc.*def"
Match field TCP source-port eq 1234
```

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

**Table 4: show class-map Field Descriptions**A number in parentheses may appear next to the class-map name and match criteria information. The number is for Cisco internal use only and can be disregarded.

Field	Description
Class Map	Class of traffic being displayed. Output is displayed for each configured class map in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
Match	Match criteria specified for the class map. Criteria include the Frame Relay DLCI number, Layer 3 packet length, IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental value, access groups, and quality of service (QoS) groups.

#### Related Commands

Command	Description
<b>class-map</b>	Creates a class map to be used for matching packets to a specified class.
<b>match fr-dlci</b>	Specifies the Frame Relay DLCI number as a match criterion in a class map.
<b>match packet length (class-map)</b>	Specifies and uses the length of the Layer 3 packet in the IP header as a match criterion in a class map.
<b>show policy-map</b>	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
<b>show policy-map interface</b>	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

# show class-map type nat

To display network address translation (NAT) class maps and their matching criteria, use the **showclass-maptypenat** command in privileged EXEC mode.

**show class-map type nat** [ *class-map-name* ]

## Syntax Description

<i>class-map-name</i>	(Optional) Name of the NAT class map. The name can be a maximum of 40 alphanumeric characters.
-----------------------	--

## Command Default

Information for all NAT class maps is displayed.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.4(11)T	This command was introduced.

## Usage Guidelines

The **showclass-maptypenat** command displays all NAT class maps and their matching criteria. To display a particular NAT class map and its matching criteria, specify the class-map name.

## Examples

The following is sample output from the **showclass-maptypenat** command that displays all the class maps:

```
Router# show class-map type nat
Class Map match-all ipnat-class-acl-we (id 5)
  Match access-group 0
```

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

**Table 5: show class-map type nat Field Descriptions**

Field	Description
Class Map	Displays the name of the class map along with the conditions applied for the class map to match the incoming packets.
Match	Match criteria specified for the class map.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show class-map type inspect</b>	Displays Layer 3 and Layer 4 or Layer 7 (application-specific) inspect type class maps and their matching criteria.
<b>show class-map type port-filter</b>	Displays port-filter class maps and their matching criteria.

# show class-map type port-filter

To display class maps for port filters and their matching criteria, use the **showclass-matypeport-filter** command in privileged EXEC mode.

**show class-map type port-filter** [ *class-map-name* ]

## Syntax Description

<i>class-map-name</i>	(Optional) Name of the port-filter class map. The name can be a maximum of 40 alphanumeric characters.
-----------------------	--

## Command Default

If no argument is specified, information for all port-filter class maps is displayed.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.4(11)T	This command was introduced.

## Usage Guidelines

Use the **showclass-matypeport-filter** command to display TCP/UDP port policing of control plane packets. The **showclass-matypeport-filter** command displays all port-filter class maps and their matching criteria. To display class maps for a particular port-filter class map, specify the class map name.

## Examples

The following is sample output from the **showclass-matypeport-filter** command that displays all the class maps:

```
Router# show class-map type port-filter
Class Map type port-filter match-all pf-policy (id 9)
  Match port tcp 45 56
  Class Map type port-filter match-any c11 (id 4)
  Match none
  Class Map type port-filter match-all pf-class (id 8)
  Match not port udp 123
  Match closed-ports
```

The following is sample output from the **showclass-matypeport-filter** command that displays the class map pf-class:

```
Router# show class-map type port-filter pf-class
Class Map type port-filter match-all pf-class (id 8)
  Match not port udp 123
  Match closed-ports
```

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

**Table 6: show class-map type port-filter Field Descriptions**

Field	Description
Class Map	Port-filter class maps being displayed. Output is displayed for each configured class map. The choice for implementing class matches (for example, match-all or match-any) appears next to the traffic class.
Match	Match criteria specified for the class map. Valid matching criteria are <b>closed-ports</b> , <b>not</b> , and <b>port</b> .

**Related Commands**

Command	Description
<b>class-map</b>	Creates a class map to be used for matching packets to a specified class.

# show control-plane cef-exception counters

To display the control-plane packet counters for the control-plane cef-exception subinterface, use the **show control-plane cef-exception counters** command in privileged EXEC mode.

**show control-plane cef-exception counters**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

The **show control-plane cef-exception counters** command displays the following packet counts for features configured on the control-plane cef-exception subinterface:

- Total number of packets that were processed by the cef-exception subinterface
- Total of packets that were dropped
- Total number of errors

## Examples

The following is sample output from the **show control-plane cef-exception counters** command:

```
Router# show control-plane cef-exception counters
Control plane cef-exception path counters:
Feature      Packets Processed/Dropped/Errors
Control Plane Policing      63456/9273/0
```

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

**Table 7: show control-plane cef-exception counters Field Descriptions**

Field	Description
Feature	Name of the configured feature on this subinterface.
Packets Processed	Total number of packets that were processed by the feature.
Dropped	Total number of packets that were dropped by the feature.
Errors	Total number of errors detected by the feature.

**Related Commands**

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

# show control-plane cef-exception features

To display the control-plane features for control-plane cef-exception subinterface, use the **show control-plane cef-exception features** command in privileged EXEC mode.

**show control-plane cef-exception features**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

The **show control-plane cef-exception features** command displays the following aggregate feature configurations for the control-plane cef-exception subinterface:

- Number of features configured for the control-plane cef-exception subinterface.
- Name of the feature
- Date and time the feature was activated

## Examples

The following is sample output from the **show control-plane cef-exception features** command:

```
Router# show control-plane cef-exception features
Total 1 features configure
Control plane cef-exception path features:
Control Plane Policing activated Nov 09 2005 12:40
```

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

**Table 8: show control-plane cef-exception features Field Descriptions**

Field	Description
Total features configured	Number of features configured.
Feature Name	Name of the configured features.
Activated	Date and time the feature was activated.

**Related Commands**

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

# show control-plane counters

To display the control-plane counters for all control-plane interfaces, use the **showcontrol-planecounters** command in privileged EXEC mode.

**show control-plane counters**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.4(4)T	This command was introduced.

**Usage Guidelines** The **showcontrol-planecounters** command displays the following aggregate packet counts for all control-plane interfaces and subinterface:

- Total number of packets that were processed by control-plane aggregate host, transit, and cef-exception subinterfaces
- Total number of packets that were dropped
- Total number of errors

**Examples** The following is sample output from the **showcontrol-planecounters** command:

```
Router# show control-plane counters
Feature Path      Packets Processed/Dropped/Errors
aggregate         43271/6759/0
host              24536/4238/0
transit           11972/2476/0
cef-exception path 6345/0/0
```

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

**Table 9: show control-plane counters Field Descriptions**

Field	Description
Feature	Name of the interface or subinterface displayed.
Packets Processed	Total number of packets that were processed by the subinterface.
Dropped	Total number of packets that were dropped.

Field	Description
Errors	Total number of errors detected.

**Related Commands**

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

# show control-plane features

To display the configured control-plane features, use the **showcontrol-planefeatures** command in privileged EXEC mode.

**show control-plane features**

## Syntax Description

This command has no arguments or keywords

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

The **showcontrol-planefeatures** command displays control-plane features enabled on the control-plane aggregate sub-interfaces. Information includes the following:

- Number of features configured for the control plane
- Name of the feature
- Date and time the feature was activated

## Examples

The following is sample output from the **showcontrol-planefeatures** command:

```
Router# show control-plane features
Total 1 features configured
Control plane host path features:
TCP/UDP Portfilter activated Nov 09 2005 12:40
```

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

**Table 10: show control-plane features Field Descriptions**

Field	Description
Total features configured	Number of features configured.
Feature Name	Name of the configured features.
activated	Date and time the feature was activated.

**Related Commands**

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

# show control-plane host counters

To display the control-plane packet counters for the control-plane host subinterface, use the **showcontrol-planehostcounters** command in privileged EXEC mode.

**show control-plane host counters**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.4(4)T	This command was introduced.

**Usage Guidelines** The **showcontrol-planehostcounters** command displays the following packet counts for the control-plane host subinterface:

- Total number of packets that were processed by features configured on the host subinterface
- Total number of packets that were dropped
- Total number of errors

**Examples** The following is sample output from the **showcontrol-planehostcounters** command:

```
Router# show control-plane host counters
Control plane host path counters:
Feature          Packets Processed/Dropped/Errors
TCP/UDP portfilter  46/46/0
```

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

**Table 11: show control-plane host counters Field Descriptions**

Field	Description
Feature	Name of the feature configured on the host subinterface.
Packets Processed	Total number of packets that were processed by the feature.
Dropped	Total number of packets that were dropped.
Errors	Total number of errors detected.

**Related Commands**

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

# show control-plane host features

To display the configured control-plane features for the control-plane host sub-interface, use the **show control-plane host features** command in privileged EXEC mode.

**show control-plane host features**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

The **show control-plane host features** command displays the features configured for the control-plane host subinterface. Information includes the following:

- Number of features configured for the control plane
- Name of the feature
- Date and time the feature was activated

## Examples

The following is sample output from the **show control-plane host features** command:

```
Router# show control-plane host features
Control plane host path features:
TCP/UDP Portfilter activated Nov 09 2005 12:40
```

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

**Table 12: show control-plane host features Field Descriptions**

Field	Description
Feature Name	Name of the configured features.
activated	Date and time the feature was activated.

**Related Commands**

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

# show control-plane host open-ports

To display a list of open TCP/UDP ports that are registered with the port-filter database, use the **show control-plane host open-ports** command in privileged EXEC mode.

## show control-plane host open-ports

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.4(4)T	This command was introduced.

**Usage Guidelines** The **show control-plane host open-ports** command displays a list of open TCP/UDP ports that are registered with the port-filter database.

**Examples** The following is sample output from the **show control-plane host open-ports** command.

```
Router# show control-plane host open-ports

Active internet connections (servers and established)
Port      Local Address      Foreign Address      Service      State
tcp       *:23               *:0                  Telnet       LISTEN
tcp       *:53               *:0                  DNS Server   LISTEN
tcp       *:80               *:0                  HTTP CORE    LISTEN
tcp       *:1720             *:0                  H.225       LISTEN
tcp       *:5060             *:0                  SIP          LISTEN
tcp       *:23               192.0.2.18:58714    Telnet       ESTABLISHED
udp       *:53               *:0                  DNS Server   LISTEN
udp       *:67               *:0                  DHCPD Receive LISTEN
udp       *:52824            *:0                  IP SNMP     LISTEN
udp       *:161              *:0                  IP SNMP     LISTEN
udp       *:162              *:0                  IP SNMP     LISTEN
udp       *:5060             *:0                  SIP          LISTEN
udp       *:2517             *:0                  CCH323_CT   LISTEN
```

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

**Table 13: show control-plane host open-ports Field Descriptions**

Field	Description
Port	Port type, either TCP or UDP.
Local Address	Local IP address and port number. An asterisk (*) indicates that the service is listening on all configured network interfaces.

Field	Description
Foreign Address	Remote IP address and port number. An asterisk (*) indicates that the service is listening on all configured network interfaces.
Service	Name of the configured Cisco IOS service listening on the port.
State	Listen or Established.

**Related Commands**

Command	Description
<b>clear control-plane</b>	Clears packet counters for control-plane interfaces and subinterfaces.
<b>control-plane</b>	Enters control-plane configuration mode, which allows you to associate or modify attributes or parameters that are associated with the control plane of the device.
<b>debug control-plane</b>	Displays debugging output from the control-plane routines.
<b>show control-plane cef-exception counters</b>	Displays the control-plane packet counters for the control-plane CEF-exception subinterface.
<b>show control-plane cef-exception features</b>	Displays the configured features for the control-plane CEF-exception subinterface.
<b>show control-plane counters</b>	Displays the control-plane packet counters for the aggregate control-plane interface.
<b>show control-plane features</b>	Displays the configured features for the aggregate control-plane interface.
<b>show control-plane host counters</b>	Displays the control plane packet counters for the control-plane host subinterface.
<b>show control-plane host features</b>	Displays the configured features for the control-plane host subinterface.
<b>show control-plane transit counters</b>	Displays the control plane packet counters for the control-plane transit subinterface.
<b>show control-plane transit features</b>	Displays the configured features for the control-plane transit subinterface.

# show control-plane transit counters

To display the control-plane packet counters for the control-plane transit sub-interface, use the **show control-plane transit counters** command in privileged EXEC mode.

**show control-plane transit counters**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.4(4)T	This command was introduced.

**Usage Guidelines** The **show control-plane transit counters** command displays the following packet counts for the control-plane transit subinterface:

- Total number of packets that were processed by the transit subinterface
- Total number of packets that were dropped
- Total number of errors

**Examples** The following is sample output from the **show control-plane transit counters** command.

```
Router# show control-plane transit counters
Control plane transit path counters:
Feature          Packets Processed/Dropped/Errors
Control Plane Policing      63456/2391/0
```

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

**Table 14: show control-plane transit counters Field Descriptions**

Field	Description
Feature	Name of the feature configured on the transit sub-interface.
Packets Processed	Total number of packets that were processed by the configured feature.
Dropped	Total number of packets that were dropped.
Errors	Total number of errors detected.

**Related Commands**

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

# show control-plane transit features

To display the configured control-plane features for the control-plane transit subinterface, use the **show control-plane transit features** command in privileged EXEC mode.

**show control-plane transit features**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.4(4)T	This command was introduced.

**Usage Guidelines** The **show control-plane transit features** command displays the control-plane features configured for the control-plane transit subinterface. Information includes the following:

- Number of features configured for the control plane
- Name of the feature
- Date and time the feature was activated

**Examples** The following is sample output from the **show control-plane transit features** command:

```
Router# show control-plane transit features
Control plane transit path features:
Control Plane Policing activated Nov 09 2005 12:40
```

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

**Table 15: show control-plane transit features Field Descriptions**

<b>Field</b>	<b>Description</b>
Total Features Configured	Number of features configured.
Feature Name	Name of the configured features.
Activated	Date and time the feature was activated.

**Related Commands**

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

# show cops servers

To display the IP address and connection status of the policy servers for which the router is configured, use the **showcopservers** command in EXEC mode.

**show cops servers**

**Syntax Description** This command has no keywords or arguments.

**Command Modes** EXEC

Command History	Release	Modification
	12.1(1)T	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

**Usage Guidelines** You can also use the show cops server command to display information about the Common Open Policy Service (COPS) client on the router.

**Examples** In the following example, information is displayed about the current policy server and client. When Client Type appears followed by an integer, 1 stands for Resource Reservation Protocol (RSVP) and 2 stands for Differentiated Services Provisioning. (0 indicates keepalive.)

```
Router# show cops servers
COPS SERVER: Address: 10.0.0.1. Port: 3288. State: 0. Keepalive: 120 sec
Number of clients: 1. Number of sessions: 1.
COPS CLIENT: Client type: 1. State: 0.
```

## Related Commands

Command	Description
<b>show ip rsvp policy cops</b>	Displays policy server address(es), ACL IDs, and current state of the router-server connection.

## show crypto eng qos

To monitor and maintain low latency queuing (LLQ) for IPsec encryption engines, use the show crypto eng qos command in privileged EXEC mode.

**show crypto eng qos**

**Syntax Description** This command has no keywords or arguments.

**Command Modes** Privileged EXEC

Command History	Release	Modification
	12.2(13)T	This command was introduced in Cisco IOS Release 12.2(13)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
	12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

**Usage Guidelines** Use the **show crypto eng qos** command to determine if QoS is enabled on LLQ for IPsec encryption engines.

**Examples** The following example shows how to determine if LLQ for IPsec encryption engines is enabled:

```
Router# show crypto eng qos
crypto engine name: Multi-ISA Using VAM2
  crypto engine type: hardware
    slot: 5
    queuing: enabled
  visible bandwidth: 30000 kbps
  llq size: 0
  default queue size/max: 0/64
  interface table size: 32
  FastEthernet0/0 (3), iftype 1, ctable size 16, input filter:ip
precedence 5
  class voice (1/3), match ip precedence 5
    bandwidth 500 kbps, max token 100000
    IN match pkt/byte 0/0, police drop 0
    OUT match pkt/byte 0/0, police drop 0
  class default, match pkt/byte 0/0, qdrop 0
crypto engine bandwidth:total 30000 kbps, allocated 500 kbps
```

The field descriptions in the above display are self-explanatory.

# show crypto entropy status

To display the status of crypto entropy on the Cisco ASR 1000 Series Aggregation Services Routers, use the **show crypto entropy status** command in the EXEC mode.

**show crypto entropy status**

## Syntax Description

This command has no arguments or keywords.

## Command Default

None

## Command Modes

EXEC(#)

## Command History

Release	Modification
Cisco IOS XE Release 3.7.3S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.8S	The command outputs were modified on the Cisco ASR 1000 Series Aggregation Services Routers.

## Examples

The following is a sample output of the **show crypto entropy status** command when crypto entropy is enabled:

```
Router# show crypto entropy status
```

```
# Entropy source      Type Status Entropy Bits
1 randfill           SW Working 128(*)
2 getrandombytes     SW Working 160(*)
3 Nitrox / Octeon    HW Working 256
```

(\*) - The entropy collected from SW sources were not counted as a part of achieving the entropy target!

[Table 16: Table 1 show crypto entropy status Field Descriptions](#) describes the significant fields shown in the display.

**Table 16: Table 1 show crypto entropy status Field Descriptions**

Field	Description
Entropy source	Source of crypto entropy.

Field	Description
Type	Type of crypto entropy. It can be one of the following values: <ul style="list-style-type: none"> <li>SW-Entropy originated from the software.</li> <li>HW-Entropy originated from the hardware.</li> </ul>
Status	Status of crypto entropy. It can be one of the following values: <ul style="list-style-type: none"> <li>Working-Entropy is working.</li> <li>Offline-Entropy is offline.</li> </ul>
Entropy Bits	Size of crypto entropy, in bits.

The following is a sample output of the **show crypto entropy status** command when crypto entropy is disabled:

Router# **show crypto entropy status**

```
# Entropy source      Type Status Entropy Bits
1 randfill           SW  Working 128
2 getrandombytes     SW  Working 160
3 Nitrox / Octeon    HW  Offline  --
```



**Note**

The fields in the display are explained in [Table 16: Table 1 show crypto entropy status Field Descriptions](#)

**Related Commands**

Command	Description
platform ipsec fips-mode	

# show frame-relay ip rtp header-compression

To display Frame Relay Real-Time Transport Protocol (RTP) header compression statistics, use the **show frame-relay ip rtp header-compression** command in user EXEC or privileged EXEC mode.

**show frame-relay ip rtp header-compression** [*interface type number*] [*dlci*]

## Syntax Description

<b>interface</b> <i>type number</i>	(Optional) Specifies an interface for which information will be displayed. A space between the interface type and number is optional.
<i>dlci</i>	(Optional) Specifies a data-link connection identifier (DLCI) for which information will be displayed. The range is from 16 to 1022.

## Command Default

RTP header compression statistics are displayed for all DLCIs on interfaces that have RTP header compression configured.

## Command Modes

User EXEC Privileged EXEC

## Command History

Release	Modification
11.3	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. The output for this command was modified to display RTP header compression statistics for Frame Relay permanent virtual circuit (PVC) bundles.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC, and the <i>dlci</i> argument was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(9)T	The <i>dlci</i> argument was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The output for this command was modified to display Enhanced Compressed Real-Time Transport Protocol (ECRTP) header compression statistics for Frame Relay permanent virtual circuit (PVC) bundles.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

**Examples**

The following is sample output from the **show frame-relay ip rtp header-compression** command:

```
Router# show frame-relay ip rtp header-compression
DLCI 21      Link/Destination info: ip 10.1.4.1
Interface Serial3/0 DLCI 21 (compression on, Cisco)
  Rcvd:      0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
  Sent:      0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
  Connect:   256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
DLCI 20      Link/Destination info: ip 10.1.1.1
Interface Serial3/1 DLCI 20 (compression on, Cisco)
  Rcvd:      0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
  Sent:      0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
  Connect:   256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
DLCI 21      Link/Destination info: ip 10.1.2.1
Interface Serial3/1 DLCI 21 (compression on, Cisco)
  Rcvd:      0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
  Sent:      0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
  Connect:   256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
DLCI 22      Link/Destination info: ip 10.1.3.1
Interface Serial3/1 DLCI 22 (compression on, Cisco)
  Rcvd:      0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
  Sent:      0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
  Connect:   256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

The following is sample output from the **show frame-relay ip rtp header-compression** command when ECRTTP is enabled:

```
Router# show frame-relay ip rtp header-compression
DLCI 16      Link/Destination info: ip 10.0.0.1
Interface Serial4/1 DLCI 16 (compression on, IETF, ECRTTP)
  Rcvd:      0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
  Sent:      0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
  Connect:   16 rx slots, 16 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 16 free contexts
```

In the following example, the **show frame-relay ip rtp header-compression** command displays information about DLCI 21:

```
Router# show frame-relay ip rtp header-compression 21
DLCI 21      Link/Destination info: ip 10.1.4.1
Interface Serial3/0 DLCI 21 (compression on, Cisco)
  Rcvd:      0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
  Sent:      0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
  Connect:   256 rx slots, 256 tx slots,
             0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
DLCI 21      Link/Destination info: ip 10.1.2.1
Interface Serial3/1 DLCI 21 (compression on, Cisco)
  Rcvd:      0 total, 0 compressed, 0 errors, 0 status msgs
             0 dropped, 0 buffer copies, 0 buffer failures
  Sent:      0 total, 0 compressed, 0 status msgs, 0 not predicted
             0 bytes saved, 0 bytes sent
```

```
Connect: 256 rx slots, 256 tx slots,
         0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

In the following example, the **showframe-relayiprtpheader-compression** command displays information for all DLCIs on serial interface 3/1:

```
Router# show frame-relay ip rtp header-compression interface serial3/1
DLCI 20      Link/Destination info: ip 10.1.1.1
Interface Serial3/1 DLCI 20 (compression on, Cisco)
Rcvd:       0 total, 0 compressed, 0 errors, 0 status msgs
            0 dropped, 0 buffer copies, 0 buffer failures
Sent:       0 total, 0 compressed, 0 status msgs, 0 not predicted
            0 bytes saved, 0 bytes sent
Connect:    256 rx slots, 256 tx slots,
            0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
DLCI 21      Link/Destination info: ip 10.1.2.1
Interface Serial3/1 DLCI 21 (compression on, Cisco)
Rcvd:       0 total, 0 compressed, 0 errors, 0 status msgs
            0 dropped, 0 buffer copies, 0 buffer failures
Sent:       0 total, 0 compressed, 0 status msgs, 0 not predicted
            0 bytes saved, 0 bytes sent
Connect:    256 rx slots, 256 tx slots,
            0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
DLCI 22      Link/Destination info: ip 10.1.3.1
Interface Serial3/1 DLCI 22 (compression on, Cisco)
Rcvd:       0 total, 0 compressed, 0 errors, 0 status msgs
            0 dropped, 0 buffer copies, 0 buffer failures
Sent:       0 total, 0 compressed, 0 status msgs, 0 not predicted
            0 bytes saved, 0 bytes sent
Connect:    256 rx slots, 256 tx slots,
            0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

In the following example, the **showframe-relayiprtpheader-compression** command displays information only for DLCI 21 on serial interface 3/1:

```
Router# show frame-relay ip rtp header-compression interface serial3/1 21
DLCI 21      Link/Destination info: ip 10.1.2.1
Interface Serial3/1 DLCI 21 (compression on, Cisco)
Rcvd:       0 total, 0 compressed, 0 errors, 0 status msgs
            0 dropped, 0 buffer copies, 0 buffer failures
Sent:       0 total, 0 compressed, 0 status msgs, 0 not predicted
            0 bytes saved, 0 bytes sent
Connect:    256 rx slots, 256 tx slots,
            0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
```

The following sample output from the **showframe-relayiprtpheader-compression** command shows statistics for a PVC bundle called MP-3-static:

```
Router# show frame-relay ip rtp header-compression interface Serial1/4
vc-bundle MP-3-static      Link/Destination info:ip 10.1.1.1
Interface Serial1/4:
Rcvd:   14 total, 13 compressed, 0 errors
        0 dropped, 0 buffer copies, 0 buffer failures
Sent:   15 total, 14 compressed,
        474 bytes saved, 119 bytes sent
        4.98 efficiency improvement factor
Connect:256 rx slots, 256 tx slots,
        1 long searches, 1 misses 0 collisions, 0 negative cache hits
        93% hit ratio, five minute miss rate 0 misses/sec, 0 max
```

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

**Table 17: show frame-relay ip rtp header-compression Field Descriptions**

Field	Description
Interface	Type and number of the interface and type of header compression.

Field	Description
Rcvd:	Table of details concerning received packets.
total	Number of packets received on the interface.
compressed	Number of packets with compressed headers.
errors	Number of errors.
dropped	Number of dropped packets.
buffer copies	Number of buffers that were copied.
buffer failures	Number of failures in allocating buffers.
Sent:	Table of details concerning sent packets.
total	Total number of packets sent.
compressed	Number of packets sent with compressed headers.
bytes saved	Total savings in bytes because of compression.
bytes sent	Total bytes sent after compression.
efficiency improvement factor	Compression efficiency.
Connect:	Table of details about the connections.
rx slots	Total number of receive slots.
tx slots	Total number of transmit slots.
long searches	Searches that needed more than one lookup.
misses	Number of new states that were created.
hit ratio	Number of times that existing states were revised.
five minute miss rate	Average miss rate.
max	Maximum miss rate.

**Related Commands**

Command	Description
<b>frame-relay ip rtp compression-connections</b>	Specifies the maximum number of RTP header compression connections on a Frame Relay interface.

<b>Command</b>	<b>Description</b>
<b>frame-relay ip rtp header-compression</b>	Enables RTP header compression for all Frame Relay maps on a physical interface.
<b>frame-relay map ip compress</b>	Enables both RTP and TCP header compression on a link.
<b>frame-relay map ip nocompress</b>	Disables both RTP and TCP header compression on a link.
<b>frame-relay map ip rtp header-compression</b>	Enables RTP header compression per DLCI.
<b>show ip rpf events</b>	Displays RTP header compression statistics.

## show frame-relay ip tcp header-compression

To display Frame Relay Transmission Control Protocol (TCP)/IP header compression statistics, use the **show frame-relay ip tcp header-compression** command in user EXEC or privileged EXEC mode.

**show frame-relay ip tcp header-compression** [*interface type number*] [*dci*]

### Syntax Description

<b>interface</b> <i>type number</i>	(Optional) Specifies an interface for which information will be displayed. A space is optional between the type and number.
<i>dci</i>	(Optional) Specifies a data-link connection identifier (DLCI) for which information will be displayed. Range is from 16 to 1022.

### Command Modes

User EXEC Privileged EXEC

### Command History

Release	Modification
10.3	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T. The command was modified to support display of RTP header compression statistics for Frame Relay permanent virtual circuit (PVC) bundles.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC, and the <i>dci</i> argument was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4(9)T	The <i>dci</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.

### Examples

The following is sample output from the **show frame-relay ip tcp header-compression** command:

```
Router# show frame-relay ip tcp header-compression
DLCI 200          Link/Destination info: ip 10.108.177.200
Interface Serial0:
```

```

Rcvd:      40 total, 36 compressed, 0 errors
           0 dropped, 0 buffer copies, 0 buffer failures
Sent:      0 total, 0 compressed
           0 bytes saved, 0 bytes sent
Connect:   16 rx slots, 16 tx slots, 0 long searches, 0 misses, 0% hit ratio
           Five minute miss rate 0 misses/sec, 0 max misses/sec

```

The following sample output from the **showframe-relayiptcpheader-compression** command shows statistics for a PVC bundle called "MP-3-static":

```

Router# show frame-relay ip tcp header-compression interface Serial1/4
vc-bundle MP-3-static      Link/Destination info:ip 10.1.1.1
Interface Serial1/4:
  Rcvd:    14 total, 13 compressed, 0 errors
           0 dropped, 0 buffer copies, 0 buffer failures
  Sent:    15 total, 14 compressed,
           474 bytes saved, 119 bytes sent
           4.98 efficiency improvement factor
  Connect: 256 rx slots, 256 tx slots,
           1 long searches, 1 misses 0 collisions, 0 negative cache hits
           93% hit ratio, five minute miss rate 0 misses/sec, 0 max

```

In the following example, the **showframe-relayiptcpheader-compression** command displays information about DLCI 21:

```

Router# show frame-relay ip tcp header-compression 21
DLCI 21      Link/Destination info: ip 10.1.2.1
Interface POS2/0 DLCI 21 (compression on, VJ)
  Rcvd:      0 total, 0 compressed, 0 errors, 0 status msgs
           0 dropped, 0 buffer copies, 0 buffer failures
  Sent:      0 total, 0 compressed, 0 status msgs, 0 not predicted
           0 bytes saved, 0 bytes sent
  Connect:   256 rx slots, 256 tx slots,
           0 misses, 0 collisions, 0 negative cache hits, 256 free contexts
DLCI 21      Link/Destination info: ip 10.1.4.1
Interface Serial3/0 DLCI 21 (compression on, VJ)
  Rcvd:      0 total, 0 compressed, 0 errors, 0 status msgs
           0 dropped, 0 buffer copies, 0 buffer failures
  Sent:      0 total, 0 compressed, 0 status msgs, 0 not predicted
           0 bytes saved, 0 bytes sent
  Connect:   256 rx slots, 256 tx slots,
           0 misses, 0 collisions, 0 negative cache hits, 256 free contexts

```

The following is sample output from the **showframe-relayiptcpheader-compression** command for a specific DLCI on a specific interface:

```

Router# show frame-relay ip tcp header-compression pos2/0 21
DLCI 21      Link/Destination info: ip 10.1.2.1
Interface POS2/0 DLCI 21 (compression on, VJ)
  Rcvd:      0 total, 0 compressed, 0 errors, 0 status msgs
           0 dropped, 0 buffer copies, 0 buffer failures
  Sent:      0 total, 0 compressed, 0 status msgs, 0 not predicted
           0 bytes saved, 0 bytes sent
  Connect:   256 rx slots, 256 tx slots,
           0 misses, 0 collisions, 0 negative cache hits, 256 free contexts

```

The table below describes the fields shown in the display.

**Table 18: show frame-relay ip tcp header-compression Field Descriptions**

Field	Description
Rcvd:	Table of details concerning received packets.
total	Sum of compressed and uncompressed packets received.

Field	Description
compressed	Number of compressed packets received.
errors	Number of errors caused by errors in the header fields (version, total length, or IP checksum).
dropped	Number of packets discarded. Seen only after line errors.
buffer failures	Number of times that a new buffer was needed but was not obtained.
Sent:	Table of details concerning sent packets.
total	Sum of compressed and uncompressed packets sent.
compressed	Number of compressed packets sent.
bytes saved	Number of bytes reduced because of the compression.
bytes sent	Actual number of bytes transmitted.
Connect:	Table of details about the connections.
rx slots, tx slots	Number of states allowed over one TCP connection. A state is recognized by a source address, a destination address, and an IP header length.
long searches	Number of times that the connection ID in the incoming packet was not the same as the previous one that was processed.
misses	Number of times that a matching entry was not found within the connection table and a new entry had to be entered.
hit ratio	Percentage of times that a matching entry was found in the compression tables and the header was compressed.
Five minute miss rate	Miss rate computed over the most recent 5 minutes and the maximum per-second miss rate during that period.

# show interfaces fair-queue



## Note

Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **showinterfacesfair-queue** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.



## Note

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

To display information and statistics about weighted fair queueing (WFQ) for a Versatile Interface Processor (VIP)-based interface, use the **showinterfacesfair-queue** command in EXEC mode.

**show interfaces** [*type number*] **fair-queue**

## Syntax Description

<i>type</i>	(Optional) The type of the interface.
<i>number</i>	(Optional) The number of the interface.

## Command Modes

EXEC

## Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.
15.0(1)S	This command was modified. This command was hidden.

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

## Examples

The following is sample output from the **show interfaces fair-queue** command for VIP-distributed WFQ (DWFQ):

```
Router# show interfaces fair-queue
Hssi0/0/0 queue size 0
      packets output 1417079, drops 2
WFQ: aggregate queue limit 54, individual queue limit 27
      max available buffers 54

      Class 0: weight 10 limit 27 qsize 0 packets output 1150 drops 0
      Class 1: weight 20 limit 27 qsize 0 packets output 0 drops 0
      Class 2: weight 30 limit 27 qsize 0 packets output 775482 drops 1
      Class 3: weight 40 limit 27 qsize 0 packets output 0 drops 0
```

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

**Table 19: show interfaces fair-queue Field Descriptions**

Field	Description
queue size	Current output queue size for this interface.
packets output	Number of packets sent out this interface or number of packets in this class sent out the interface.
drops	Number of packets dropped or number of packets in this class dropped.
aggregate queue limit	Aggregate limit, in number of packets.
individual queue limit	Individual limit, in number of packets.
max available buffers	Available buffer space allocated to aggregate queue limit, in number of packets.
Class	QoS group or type of service (ToS) class.
weight	Percent of bandwidth allocated to this class during periods of congestion.
limit	Queue limit for this class in number of packets.
qsize	Current size of the queue for this class.

**Related Commands**

Command	Description
<b>show interfaces</b>	Displays statistics for all interfaces configured on the router or access server.

# show interfaces random-detect



## Note

Effective with Cisco IOS XE Release 2.6, Cisco IOS Release 15.0(1)S, and Cisco IOS Release 15.1(3)T, the **showinterfacesrandom-detect** command is hidden. Although this command is still available in Cisco IOS software, the CLI interactive Help does not display it if you attempt to view it by entering a question mark at the command line. This command will be completely removed in a future release, which means that you will need to use the appropriate replacement command (or sequence of commands). For more information (including a list of replacement commands), see the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS XE Quality of Service Solutions Configuration Guide* or the "Legacy QoS Command Deprecation" feature document in the *Cisco IOS Quality of Service Solutions Configuration Guide*.



## Note

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

To display information about Weighted Random Early Detection (WRED) for a Versatile Interface Processor (VIP)-based interface, use the **showinterfacesrandom-detect** command in EXEC mode.

**show interfaces** [*type number*] **random-detect**

## Syntax Description

<i>type</i>	(Optional) The type of the interface.
<i>number</i>	(Optional) The number of the interface.

## Command Modes

EXEC

## Command History

Release	Modification
11.1CC	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.6	This command was modified. This command was hidden.
15.0(1)S	This command was modified. This command was hidden.

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

## Examples

The following is sample output from the **show interfaces random-detect** command for VIP-distributed WRED (DWRED):

```
Router# show interfaces random-detect
FastEthernet1/0/0 queue size 0
      packets output 29692, drops 0
WRED: queue average 0
      weight 1/512
      Precedence 0: 109 min threshold, 218 max threshold, 1/10 mark weight
          1 packets output, drops: 0 random, 0 threshold
      Precedence 1: 122 min threshold, 218 max threshold, 1/10 mark weight
          (no traffic)
      Precedence 2: 135 min threshold, 218 max threshold, 1/10 mark weight
          14845 packets output, drops: 0 random, 0 threshold
      Precedence 3: 148 min threshold, 218 max threshold, 1/10 mark weight
          (no traffic)
      Precedence 4: 161 min threshold, 218 max threshold, 1/10 mark weight
          (no traffic)
      Precedence 5: 174 min threshold, 218 max threshold, 1/10 mark weight
          (no traffic)
      Precedence 6: 187 min threshold, 218 max threshold, 1/10 mark weight
          14846 packets output, drops: 0 random, 0 threshold
      Precedence 7: 200 min threshold, 218 max threshold, 1/10 mark weight
          (no traffic)
```

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

**Table 20: show interfaces random-detect Field Descriptions**

Field	Description
queue size	Current output queue size for this interface.
packets output	Number of packets sent out this interface.
drops	Number of packets dropped.
queue average	Average queue length.
weight	Weighting factor used to determine the average queue size.
Precedence	WRED parameters for this precedence.
min threshold	Minimum threshold for this precedence.
max threshold	Maximum length of the queue. When the average queue is this long, any additional packets will be dropped.

Field	Description
mark weight	Probability of a packet being dropped if the average queue is at the maximum threshold.
packets output	Number of packets with this precedence that have been sent.
random	Number of packets dropped randomly through the WRED process.
threshold	Number of packets dropped automatically because the average queue was at the maximum threshold length.
(no traffic)	No packets with this precedence.

**Related Commands**

Command	Description
<b>random-detect (interface)</b>	Enables WRED or DWRED.
<b>random-detect flow</b>	Enables flow-based WRED.
<b>show interfaces</b>	Displays statistics for all interfaces configured on the router or access server.
<b>show queueing</b>	Lists all or selected configured queueing strategies.

# show interfaces rate-limit

To display information about committed access rate (CAR) for an interface, use the **show interfaces rate-limit** command in EXEC mode.

**show interfaces** [*type number*] **rate-limit**

## Syntax Description

<i>type</i>	(Optional) The type of the interface.
<i>number</i>	(Optional) The number of the interface.

## Command Modes

EXEC

## Command History

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

## Examples

The following is sample output from the **show interfaces rate-limit** command:

```
Router# show interfaces fddi2/1/0 rate-limit
Fddi2/1/0
  Input
    matches: access-group rate-limit 100
    params: 800000000 bps, 64000 limit, 80000 extended limit
    conformed 0 packets, 0 bytes; action: set-prec-continue 1
    exceeded 0 packets, 0 bytes; action: set-prec-continue 0
    last packet: 4737508ms ago, current burst: 0 bytes
    last cleared 01:05:47 ago, conformed 0 bps, exceeded 0 bps
    matches: access-group 101
    params: 800000000 bps, 56000 limit, 72000 extended limit
    conformed 0 packets, 0 bytes; action: set-prec-transmit 5
    exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
    last packet: 4738036ms ago, current burst: 0 bytes
    last cleared 01:02:05 ago, conformed 0 bps, exceeded 0 bps
    matches: all traffic
    params: 50000000 bps, 48000 limit, 64000 extended limit
    conformed 0 packets, 0 bytes; action: set-prec-transmit 5
    exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
    last packet: 4738036ms ago, current burst: 0 bytes
    last cleared 01:00:22 ago, conformed 0 bps, exceeded 0 bps
  Output
    matches: all traffic
    params: 800000000 bps, 64000 limit, 80000 extended limit
```

```

conformed 0 packets, 0 bytes; action: transmit
exceeded 0 packets, 0 bytes; action: drop
last packet: 4809528ms ago, current burst: 0 bytes
last cleared 00:59:42 ago, conformed 0 bps, exceeded 0 bps

```

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

**Table 21: show interfaces rate-limit Field Descriptions**

Field	Description
Input	These rate limits apply to packets received by the interface.
matches	Packets that match this rate limit.
params	Parameters for this rate limit, as configured by the <b>rate-limit</b> command.
bps	Average rate, in bits per second.
limit	Normal burst size, in bytes.
extended limit	Excess burst size, in bytes.
conformed	Number of packets that have conformed to the rate limit.
action	Conform action.
exceeded	Number of packets that have exceeded the rate limit.
action	Exceed action.
last packet	Time since the last packet, in milliseconds.
current burst	Instantaneous burst size at the current time.
last cleared	Time since the burst counter was set back to zero by the <b>clearcounters</b> command.
conformed	Rate of conforming traffic.
exceeded	Rate of exceeding traffic.
Output	These rate limits apply to packets sent by the interface.

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>access-list rate-limit</b>	Configures an access list for use with CAR policies.
<b>clear counters</b>	Clears the interface counters.
<b>shape</b>	Specifies average or peak rate traffic shaping.
<b>show access-lists</b>	Displays the contents of current IP and rate-limit access lists.
<b>show interfaces</b>	Displays statistics for all interfaces configured on the router or access server.

# show iphc-profile

To display configuration information for one or more IP Header Compression (IPHC) profiles, use the **show iphc-profile** command in user EXEC or privileged EXEC mode.

**show iphc-profile** [ *profile-name* ]

## Syntax Description

<i>profile-name</i>	(Optional) Name of an IPHC profile to display.
---------------------	--

## Command Default

If you do not specify an IPHC profile name, all IPHC profiles are displayed.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(24)T	This command was modified. The output was enhanced to display recoverable loss when EcRTP is configured.

## Usage Guidelines

### Information Included in Display

The display includes information such as the profile type, the type of header compression enabled, the number of contexts, the refresh period (for Real-Time Transport [RTP] header compression), whether feedback messages are disabled, and the interfaces to which the IPHC profile is attached.

### For More Information About IPHC Profiles

An IPHC profile is used to enable and configure header compression on your network. For more information about using IPHC profiles to configure header compression, see the “Header Compression” module and the “Configuring Header Compression Using IPHC Profiles” module of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

## Examples

The following is sample output from the **show iphc-profile** command. In the output, information about two IPHC profiles, profile19 and profile20, is displayed.

```
Router# show iphc-profile
IPHC Profile "profile19"
Type: IETF
  Compressing: NON-TCP (RTP)
  Contexts    : NON-TCP fixed at 0
  Refresh     : NON-TCP every 5 seconds or 256 packets
  EcRTP       : recoverable loss enabled 1
  Controlled interfaces: (0)
```

```

Reference Count: (1)
IPHC Profile "profile20"
Type: IETF
  Compressing: NON-TCP (RTP)
  Contexts    : NON-TCP fixed at 0
  Refresh     : NON-TCP every 5 seconds or 256 packets
  EcRTP      : recoverable loss enabled 4 (dynamic)
  Controlled interfaces: (0)
  Reference Count: (0)

```

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

**Table 22: show iphc-profile Field Descriptions**

Field	Description
IPHC Profile	IPHC profile name.
Type	IPHC profile type: either VJ (for van-jacobson) or IETF.
Compressing	Type of header compression used, such as TCP, non-TCP, or RTP.
Contexts	Number of contexts and setting used to calculate the context number.
Refresh	Indicates maximum number of packets or maximum time between context refresh.
EcRTP	Indicates if recoverable loss is enabled and if EcRTP recoverable loss is configured to dynamic.
Controlled interfaces	Interfaces to which the IPHC profile is attached.
Reference Count	Indicates the number of active IPHC-profile submodes.

#### Related Commands

Command	Description
<b>iphc-profile</b>	Creates an IPHC profile.

# show ip nat translations rsvp

To display active Network Address Translations (NAT) for Resource Reservation Protocol (RSVP) messages, use the **show ip nat translations rsvp** command in privileged EXEC mode.

**show ip nat translations rsvp** [ *vrf vrf-name* ]

## Syntax Description

<i>vrf vrf-name</i>	(Optional) Displays VPN routing and forwarding (VRF) traffic-related information.
---------------------	---

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
15.2(2)T	This command was introduced.

## Usage Guidelines

Use the **show ip nat translations rsvp** command to display the IP address/port translations performed by the RSVP-NAT-Application Layer Gateway (ALG) on RSVP packets.

## Examples

The following is sample output from the **show ip nat translations rsvp** command:

```
Router# show ip nat translations rsvp

RSVP-NAT-ALG:
  Inside Local: Address: <ip-address>, Port: <port-number>
  Outside Local: Address: <ip-address>, Port: <port-number>
  Inside Global: Address: <ip-address>, Port: <port-number>
  Outside Global: Address: <ip-address>, Port: <port-number>
  L4-Protocol: <protocol-number>
  Local Path Phop: <ip-address>
  Local Resv Phop: <ip-address>
  Local Resv Confirm: <ip-address>
```

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

**Table 23: show ip nat translations rsvp Field Descriptions**

Field	Description
Inside Local	The IP address and port number assigned to a host on the inside network; probably not a legitimate address assigned by the Network Interface Card (NIC) or service provider.

Field	Description
Outside Local	IP address and port number of an outside host as it appears to the inside network; probably not a legitimate address assigned by the NIC or service provider.
Inside Global	The legitimate IP address and port number that represents one or more inside local IP addresses to the outside world.
Outside Global	The IP address and port number assigned to a host on the outside network by its owner.
Address	The IP address representing the appropriate category of translation.
Port	The port number representing the appropriate category of translation.
L4-Protocol	The Layer 4 protocol of the port identifying the address.
Local Path Phop	Address of the previous local hop that is used to send the Resv message from global to local.
Local Resv Phop	Address of previous local hop that is saved when Resv message comes from local to global. This address is used in traversing the Resv error message.
Local Resv Confirm	Address of the local hop saved when processing the Resv message, which is used to traverse the Resv confirm message.

# show ip nbar attribute

To display the configured attributes used by the Network-Based Application Recognition (NBAR), use the **show ip nbar attribute** command in privileged EXEC mode.

**show ip nbar attribute** [**application-group**| **category**| **encrypted**| **sub-category**| **tunnel**]

## Syntax Description

<b>application-group</b>	(Optional) Specifies the application-group attribute.
<b>category</b>	(Optional) Specifies the category attribute.
<b>encrypted</b>	(Optional) Specifies the encrypted applications.
<b>sub-category</b>	(Optional) Specifies the subcategory attribute.
<b>tunnel</b>	(Optional) Specifies the tunneled applications.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

## Usage Guidelines

The **show ip nbar attribute** command displays all the attributes used by the NBAR. Use the keywords to display only the specified attribute.

## Examples

The following is the sample output from the **show ip nbar attribute** command:

```
Router# show ip nbar attribute
  Name : category
  Help : category attribute
  Type : group
  Groups : email, newsgroup, location-based-services, instant-messaging, netg
  Need : Mandatory
Default : other
  Name : sub-category
  Help : sub-category attribute
  Type : group
  Groups : routing-protocol, terminal, epayment, remote-access-terminal, nen
  Need : Mandatory
Default : other
  Name : application-group
  Help : application-group attribute
  Type : group
  Groups : skype-group, wap-group, pop3-group, kerberos-group, tftp-group, bp
  Need : Mandatory
```

```

Default : other
Name : tunnel
Help : Tunnelled applications
Type : group
Groups : tunnel-no, tunnel-yes, tunnel-unassigned
Need : Mandatory
Default : tunnel-unassigned
Name : encrypted
Help : Encrypted applications
Type : group
Groups : encrypted-yes, encrypted-no, encrypted-unassigned
Need : Mandatory
Default : encrypted-unassigned

```

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

**Table 24: show ip nbar attribute Field Descriptions**

Field	Description
Name	Indicates the name of the attribute.
Help	Provides the attribute information.
Type	Indicates the attribute type.
Groups	Specifies the groups within the attribute.
Need	Specifies the need of the attribute.
Default	Provides the default status of the attribute.

#### Related Commands

Command	Description
<b>match protocol attribute application-group</b>	Configures the match criterion for a class map based on the application group.
<b>match protocol attribute category</b>	Configures the match criterion for a class map based on the category.
<b>match protocol attribute encrypted</b>	Configures the match criterion for a class map based on the encryption.
<b>match protocol attribute sub-category</b>	Configures the match criterion for a class map based on the subcategory.
<b>match protocol attribute tunnel</b>	Configures the match criterion for a class map based on tunneling.

# show ip nbar link-age

To display the protocol linkage by network-based application recognition (NBAR), use the **show ip nbar link-age** command in privileged EXEC mode.

**show ip nbar link-age** [ *protocol-name* ]

## Syntax Description

<i>protocol-name</i>	(Optional) Displays the linkage for only the specified protocol name.
----------------------	---

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was implemented on Cisco ASR 1000 series routers.

## Usage Guidelines

The **show ip nbar link-age** command displays the linkage of all the NBAR protocols. The *protocol-name* argument can be used to limit the display for a specific protocol.

## Examples

The following is sample output from the **show ip nbar link-age** command:

```
Router# show ip nbar link-age

System Link Age: 30 seconds
No.  Protocol                Link Age (seconds)
1    skype                      120
2    bittorrent                 120
3    winmx                      120
```

The following is sample output from the **show ip nbar link-age** command for a specific protocol:

```
Router# show ip nbar link-age
eigrp
System Link Age: 30 seconds
Protocol                Link Age (seconds)
eigrp                   120
```

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

**Table 25: show ip nbar link-age Field Descriptions**

Field	Description
No.	Serial number of the list of protocols displayed.
Protocol	Name of the NBAR protocol.
Link Age (seconds)	Time, in seconds, at which the links for a protocol are aged (expire).

**Related Commands**

Command	Description
<b>ip nbar resources protocol</b>	Sets the expiration time for NBAR flow-link tables on a protocol basis.

# show ip nbar pdlm

To display the Packet Description Language Module (PDLM) in use by network-based application recognition (NBAR), use the **show ip nbar pdlm** command in privileged EXEC mode.

## show ip nbar pdlm

### Syntax Description

This command has no arguments or keywords.

### Command Modes

Privileged EXEC

### Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)E	This command was implemented on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

### Usage Guidelines

This command is used to display a list of all the PDLMs that have been loaded into NBAR using the **ipnbarpdlm** command.

### Examples

In this example of the **show ip nbar pdlm** command, the **citrix.pdlm** PDLM has been loaded from Flash memory:

```
Router# show ip nbar pdlm

The following PDLMs have been loaded:
flash://citrix.pdlm
```

### Related Commands

Command	Description
<b>ip nbar pdlm</b>	Extends or enhances the list of protocols recognized by NBAR through a Cisco-provided PDLM.

# show ip nbar port-map

To display the current protocol-to-port mappings in use by network-based application recognition (NBAR), use the **showipnbarport-map** command in privileged EXEC mode.

```
show ip nbar port-map [protocol-name [ protocol-type ]]
```

## Syntax Description

<i>protocol-name</i>	(Optional) Name of the protocol. For more information on the available protocols, use the question mark (?) online help function.
<i>protocol-type</i>	(Optional) Type of the protocol. Two types of protocols can be specified: <ul style="list-style-type: none"> <li>• <b>tcp</b> --Displays information related to Transmission Control Protocol (TCP) ports.</li> <li>• <b>udp</b> --Displays information related to User Datagram Protocol (UDP) ports.</li> </ul>

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(13)E	This command was implemented on Catalyst 6000 family switches. The FlexWAN modules were removed.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

## Usage Guidelines

The **showipnbarport-map** command displays port assignments for NBAR protocols.

You can use the **show ip nbar port-map** command to display the current protocol-to-port mappings in use by NBAR. When you use the **ip nbar port-map** command, the **show ip nbar port-map** command displays the ports you have assigned to the protocol. If you do not use the **ip nbar port-map** command to configure any protocol, the **show ip nbar port-map** command displays the default ports. Use the *protocol-name* argument to limit the display to a specific protocol. You can either use the UDP or the TCP *protocol-type* argument type.

## Examples

The following is sample output from the **show ip nbar port-map** command:

```
Router# show ip nbar port-map
port-map cuseeme udp 7648 7649 24032
port-map cuseeme tcp 7648 7649
port-map dhcp udp 67 68
port-map dhcp tcp 67 68
```

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

**Table 26: show ip route track-table Field Descriptions**

Field	Description
port-map	Specifies the ports assigned.
cuseeme	Specifies that the CU-SeeMe Protocol is used.
udp	Specifies the User Datagram Protocol type.
tcp	Specifies the Transmission Control Protocol type.
dhcp	Specifies the Dynamic Host Configuration Protocol type.

## Related Commands

Command	Description
<b>ip nbar port-map</b>	Configures NBAR to search for a protocol or protocol name using a port number other than the well-known port number.

# show ip nbar protocol activated

To display all the activated Network-Based Application Recognition (NBAR) protocols on a device, use the **show ip nbar protocol activated** command in privileged EXEC mode.

**show ip nbar protocol activated**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

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

**Usage Guidelines** NBAR must be enabled for debugging.

**Examples** The following is sample output from the **show ip nbar protocol activated** command.

```
Device# show ip nbar protocol activated
Following Protocol are enabled
Feature:PD
      Hwidb:Ethernet0/0 MI:1 SI:0 FR:0 PVC:0
All iana protocols
```

The table below describes significant fields shown in this output.

**Table 27: show ip nbar protocol activated Field Descriptions**

Field	Description
Hwidb	Displays the configured hardware IDB.
MT1	Displays the configured main interface.
SI	Displays the configured sub interface.
FR	Displays the configured frame relay.
PVC	Displays the configured ATM PVC.

# show ip nbar protocol-attribute

To display the protocol attributes used by the Network-Based Application Recognition (NBAR), use the **show ip nbar protocol-attribute** command in privileged EXEC mode.

**show ip nbar protocol-attribute** [*protocol-name*]

## Syntax Description

<i>protocol-name</i>	(Optional) Name of the protocol for which to display the attributes.
----------------------	--

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

## Usage Guidelines

The **show ip nbar protocol-attribute** command is used to display the attributes of all the protocols. To display the attributes of a specific protocol, specify the protocol name.

## Examples

The following is sample output from the **show ip nbar protocol-attribute** command. The fields in the display are self-explanatory.

```
Router# show ip nbar protocol-attribute ospf
  Protocol Name : ospf
    category : net-admin
  sub-category : routing-protocol
application-group : other
    tunnel : tunnel-no
    encrypted : encrypted-no
```

```
Router# show ip nbar protocol-attribute
  Protocol Name : ftp
    category : file-sharing
  sub-category : client-server
application-group : ftp-group
    tunnel : tunnel-no
    encrypted : encrypted-no

  Protocol Name : http
    category : browsing
  sub-category : other
application-group : other
    tunnel : tunnel-no
    encrypted : encrypted-no

  Protocol Name : egp
    category : net-admin
  sub-category : routing-protocol
application-group : other
```

```

        tunnel : tunnel-no
        encrypted : encrypted-no

    Protocol Name : gre
        category : net-admin
        sub-category : tunneling-protocols
    application-group : other
        tunnel : tunnel-yes
        encrypted : encrypted-no

    Protocol Name : icmp
        category : net-admin
        sub-category : network-management
    application-group : other
        tunnel : tunnel-no
        encrypted : encrypted-no

    Protocol Name : eigrp
        category : net-admin
        sub-category : routing-protocol
    application-group : other
        tunnel : tunnel-no
        encrypted : encrypted-no

```

**Related Commands**

Command	Description
<b>match protocol attribute application-group</b>	Configures the match criterion for a class map based on the application group.
<b>match protocol attribute category</b>	Configures the match criterion for a class map based on the category.
<b>match protocol attribute encrypted</b>	Configures the match criterion for a class map based on encryption.
<b>match protocol attribute sub-category</b>	Configures the match criterion for a class map based on the subcategory.
<b>match protocol attribute tunnel</b>	Configures the match criterion for a class map based on tunneling.

## show ip nbar protocol-discovery

To display the statistics gathered by the Network-Based Application Recognition (NBAR) Protocol Discovery feature, use the **show ip nbar protocol-discovery** command in privileged EXEC mode.

```
show ip nbar protocol-discovery [interface type number] [stats {byte-count| bit-rate| packet-count|
max-bit-rate}] [protocol protocol-name] [top-n number]
```

### Syntax Description

<b>interface</b>	(Optional) Specifies that Protocol Discovery statistics for the interface are to be displayed.
<i>type</i>	Type of interface or subinterface whose policy configuration is to be displayed.
<i>number</i>	Port, connector, VLAN, or interface card number.
<b>stats</b>	(Optional) Specifies that the byte count, byte rate, or packet count is to be displayed.
<b>byte-count</b>	(Optional) Specifies that the byte count is to be displayed.
<b>max-bit-rate</b>	(Optional) Specifies that the maximum bit rate is to be displayed.
<b>packet-count</b>	(Optional) Specifies that the packet count is to be displayed.
<b>protocol</b>	(Optional) Specifies that statistics for a specific protocol are to be displayed.
<i>protocol-name</i>	(Optional) User-specified protocol name for which the statistics are to be displayed.
<b>top-n</b>	(Optional) Specifies that a top-n is to be displayed. A top-n is the number of most active NBAR-supported protocols, where n is the number of protocols to be displayed. For instance, if top-n 3 is entered, the three most active NBAR-supported protocols will be displayed.
<i>number</i>	(Optional) Specifies the number of most active NBAR-supported protocols to be displayed.

### Command Default

Statistics for all interfaces on which the NBAR Protocol Discovery feature is enabled are displayed.

**Command Modes** Privileged EXEC (#)

**Command History**

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)E	This command was implemented on Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.3(7)T	The command output was modified to include Max Bit Rate.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)ZYA	This command was integrated into Cisco IOS Release 12.2(18)ZYA. This command was modified to include information about VLANs (as applicable) and to provide support for both Layer 2 and Layer 3 Etherchannels (Catalyst switches only).
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

**Usage Guidelines**

Use the **showipnbarprotocol-discovery** command to display statistics gathered by the NBAR Protocol Discovery feature. This command, by default, displays statistics for all interfaces on which protocol discovery is currently enabled. The default output of this command includes, in the following order, input bit rate (in bits per second), input byte count, input packet count, and protocol name.

Protocol discovery can be used to monitor both input and output traffic and may be applied with or without a service policy enabled. NBAR protocol discovery gathers statistics for packets switched to output interfaces. These statistics are not necessarily for packets that exited the router on the output interfaces, because packets may have been dropped after switching for various reasons, including policing at the output interface, access lists, or queue drops.

**Layer 2/3 Etherchannel Support**

With Cisco IOS Release 12.2(18)ZYA, intended for use on the Cisco 6500 series switch that is equipped with a Supervisor 32/programmable intelligent services accelerator (PISA), the **showipnbarprotocol-discovery** command is supported on both Layer 2 and Layer 3 Etherchannels.

**Examples**

The following example displays output from the **show ip nbar protocol-discovery** command for the five most active protocols on an Ethernet interface:

```
Router# show ip nbar protocol-discovery top-n 5

Ethernet2/0

          Input                               Output
          ----                               -----
Protocol  Packet Count                       Packet Count
          Byte Count                       Byte Count
          30sec Bit Rate (bps)             30sec Bit Rate (bps)
          30sec Max Bit Rate (bps)         30sec Max Bit Rate (bps)
-----
rtp       3272685                               3272685
          242050604                               242050604

          768000                               768000
          2002000                               2002000
gnutella  513574                               513574
          118779716                              118779716
          383000                               383000
          987000                               987000
ftp       482183                               482183
          37606237                              37606237
          121000                               121000
          312000                               312000
http     144709                               144709
          32351383                              32351383
          105000                               105000
          269000                               269000
netbios  96606                               96606
          10627650                              10627650
          36000                               36000
          88000                               88000
unknown  1724428                               1724428
          534038683                              534038683
          2754000                               2754000
          4405000                               4405000
Total    6298724                               6298724
          989303872                              989303872
          4213000                               4213000
          8177000                               8177000
```

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

**Table 28: show ip nbar protocol-discovery Field Descriptions**

Field	Description
Interface	Type and number of an interface.
Input	Incoming traffic on an interface.
Output	Outgoing traffic on an interface.
Protocol	The protocols being used. Unknown is the sum of all the protocols that NBAR could not classify for some reason.
Packet Count	Number of packets coming in and going out the interface.

Field	Description
Byte Count	Number of bytes coming in and going out the interface.
30sec Bit Rate	Average value of the bit rate in bits per second (bps) since protocol discovery was enabled, per protocol, over the last 30 seconds.
30sec Max Bit Rate	Highest value of the bit rate in bits per second (bps) since protocol discovery was enabled, per protocol, over the last 30 seconds.
Total	Total input and output traffic.

**Related Commands**

Command	Description
<b>ip nbar protocol-discovery</b>	Configures NBAR to discover traffic for all protocols known to NBAR on a particular interface.

## show ip nbar protocol-id

To display information about Network-Based Application Recognition (NBAR) protocol IDs, use the **show ip nbar protocol-id** command in privileged EXEC mode.

**show ip nbar protocol-id** [*protocol-name*]

### Syntax Description

<i>protocol-name</i>	(Optional) Name of the protocol.
----------------------	----------------------------------

### Command Default

If the optional argument is not specified, NBAR protocol IDs for all protocols are displayed.

### Command Modes

Privileged EXEC (#)

### Command History

Release	Modification
15.0(1)M	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.
Cisco IOS Release XE 3.2S	This command was modified. Support for additional IANA protocols was added.

### Examples

The following is sample output from the **show ip nbar protocol-id** command:

```
Router# show ip nbar protocol-id
Protocol Name      id      type
-----
ftp                2      Standard
http               3      Standard
egp                8      L3 IANA
gre               47     L3 IANA
icmp              1      L3 IANA
eigrp             88     L3 IANA
ipinip            4      L3 IANA
ipsec             9      Standard
ospf              89     L3 IANA
bgp               179    L4 IANA
cuseeme           12     Standard
dhcp              13     Standard
finger            79     L4 IANA
gopher            70     L4 IANA
secure-http       16     Standard
imap              17     Standard
secure-imap       18     Standard
irc               194    L4 IANA
secure-irc        994    L4 IANA
```

kerberos	21	Standard
l2tp	1701	L4 IANA
ldap	389	L4 IANA
secure-ldap	636	L4 IANA
sqlserver	1433	L4 IANA
netbios	26	Standard
nfs	2049	L4 IANA
nntp	28	Standard
secure-nntp	563	L4 IANA
notes	1352	L4 IANA
ntp	123	L4 IANA
pcanywhere	32	Standard
pop3	110	L4 IANA
secure-pop3	995	L4 IANA
pptp	1723	L4 IANA
rip	520	L4 IANA
rsvp	37	Standard
snmp	38	Standard
socks	39	Standard
ssh	22	L4 IANA
syslog	41	Standard
telnet	23	L4 IANA
secure-telnet	992	L4 IANA
secure-ftp	990	L4 IANA
xwindows	45	Standard
printer	515	L4 IANA
novadigm	47	Standard
tftp	48	Standard
exchange	49	Standard
vdolive	50	Standard
sqlnet	51	Standard
rcmd	52	Standard
netshow	53	Standard
sunrpc	54	Standard
streamwork	55	Standard
citrix	56	Standard
fasttrack	57	Standard
gnutella	58	Standard
kazaa2	59	Standard
rtsp	60	Standard
rtp	61	Standard
mgcp	62	Standard
skinny	63	Standard
h323	64	Standard
sip	65	Standard
rtcp	66	Standard
winmx	68	Standard
bittorrent	69	Standard
directconnect	70	Standard
smtp	71	Standard
dns	72	Standard
hl7	73	Standard
fix	74	Standard
msn-messenger	75	Standard
dicom	76	Standard
yahoo-messenger	77	Standard
mapi	78	Standard
aol-messenger	79	Standard
cifs	80	Standard
cisco-phone	81	Standard
youtube	82	Standard
skype	83	Standard
sap	84	Standard
blizwow	85	Standard
whois++	63	L4 IANA
klogin	543	L4 IANA
kshell	544	L4 IANA
ora-srv	1525	L4 IANA
sqlexec	9088	L4 IANA
clearcase	371	L4 IANA
appleqtz	458	L4 IANA
rcp	469	L4 IANA
isakmp	500	L4 IANA

## show ip nbar protocol-id

ibm-db2	523	L4 IANA
lockd	4045	L4 IANA
npp	92	L4 IANA
microsoftds	98	Standard
doom	666	L4 IANA
vnc	100	Standard
echo	7	L4 IANA
systat	11	L4 IANA
daytime	13	L4 IANA
chargen	19	L4 IANA
time	37	L4 IANA
isi-gl	55	L4 IANA
rtelnet	107	L4 IANA
server-ipx	213	L4 IANA
xdmcp	177	L4 IANA
nicname	43	L4 IANA
corba-iiop	111	Standard
tacacs	112	Standard
telepresence-media	113	Standard
telepresence-control	114	Standard
edonkey	243	Custom
custom-10	244	Custom
custom-09	245	Custom
custom-08	246	Custom
custom-07	247	Custom
custom-06	248	Custom
custom-05	249	Custom
custom-04	250	Custom
custom-03	251	Custom
custom-02	252	Custom
custom-01	253	Custom
mftp	349	L4 IANA
matip-type-a	350	L4 IANA
matip-type-b	351	L4 IANA
dtag-ste-sb	352	L4 IANA
ndsauth	353	L4 IANA
datex-asn	355	L4 IANA
cloanto-net-1	356	L4 IANA
bhevent	357	L4 IANA
shrinkwrap	358	L4 IANA
nsrcmp	359	L4 IANA
scoi2odialog	360	L4 IANA
semantix	361	L4 IANA
srssend	362	L4 IANA
rsvp_tunnel	363	L4 IANA
aurora-cmgr	364	L4 IANA
dtk	365	L4 IANA
odmr	366	L4 IANA
mortgageware	367	L4 IANA
qbikgdp	368	L4 IANA
rpc2portmap	369	L4 IANA
codaaauth2	370	L4 IANA
ulistproc	372	L4 IANA
legent-1	373	L4 IANA
legent-2	374	L4 IANA
hassle	375	L4 IANA
tnETOS	377	L4 IANA
is99c	379	L4 IANA
is99s	380	L4 IANA
hp-collector	381	L4 IANA
hp-managed-node	382	L4 IANA
hp-alarm-mgr	383	L4 IANA
arns	384	L4 IANA
ibm-app	385	L4 IANA
asa	386	L4 IANA
aurp	387	L4 IANA
unidata-ldm	388	L4 IANA
fatserf	347	L4 IANA
uis	390	L4 IANA
synotics-relay	391	L4 IANA
synotics-broker	392	L4 IANA
meta5	393	L4 IANA
embl-ndt	394	L4 IANA

netware-ip	396	L4	IANA
mptn	397	L4	IANA
kryptolan	398	L4	IANA
iso-tsap-c2	399	L4	IANA
ups	401	L4	IANA
genie	402	L4	IANA
decap	403	L4	IANA
nced	404	L4	IANA
ncld	405	L4	IANA
imsp	406	L4	IANA
timbuktu	407	L4	IANA
prm-sm	408	L4	IANA
prm-nm	409	L4	IANA
decladebug	410	L4	IANA
rmt	411	L4	IANA
synoptics-trap	412	L4	IANA
smsp	413	L4	IANA
infoseek	414	L4	IANA
bnet	415	L4	IANA
onmux	417	L4	IANA
hyper-g	418	L4	IANA
ariell	419	L4	IANA
ariel2	421	L4	IANA
ariel3	422	L4	IANA
opc-job-start	423	L4	IANA
opc-job-track	424	L4	IANA
smartsdp	426	L4	IANA
svrloc	427	L4	IANA
ocs_cmu	428	L4	IANA
ocs_amu	429	L4	IANA
utmpsd	430	L4	IANA
utmpcd	431	L4	IANA
iasd	432	L4	IANA
nnsd	433	L4	IANA
mobileip-agent	434	L4	IANA
mobilip-mn	435	L4	IANA
dna-cml	436	L4	IANA
comscm	437	L4	IANA
dsfgw	438	L4	IANA
dasp	439	L4	IANA
sgcp	440	L4	IANA
decvms-sysmgt	441	L4	IANA
cvc_hostd	442	L4	IANA
snpp	444	L4	IANA
ddm-rdb	446	L4	IANA
ddm-dfm	447	L4	IANA
ddm-ssl	448	L4	IANA
as-servermap	449	L4	IANA
tserver	450	L4	IANA
sfs-smp-net	451	L4	IANA
sfs-config	452	L4	IANA
creativeserver	453	L4	IANA
contentserver	3365	L4	IANA
creativepartnr	455	L4	IANA
scohelp	457	L4	IANA
skronk	460	L4	IANA
datasurfsrv	461	L4	IANA
datasurfsrvsec	462	L4	IANA
alpes	463	L4	IANA
kpasswd	464	L4	IANA
digital-vrc	466	L4	IANA
mylex-mapd	467	L4	IANA
photuris	468	L4	IANA
scx-proxy	470	L4	IANA
mondex	471	L4	IANA
ljk-login	472	L4	IANA
hybrid-pop	473	L4	IANA
tn-tl-fd1	476	L4	IANA
ss7ns	477	L4	IANA
spsc	478	L4	IANA
iafserver	479	L4	IANA
iafdbase	480	L4	IANA
bgs-nsi	482	L4	IANA

## show ip nbar protocol-id

ulpnet	483	L4	IANA
integra-sme	484	L4	IANA
powerburst	485	L4	IANA
avian	486	L4	IANA
saft	487	L4	IANA
gss-http	488	L4	IANA
nest-protocol	489	L4	IANA
micom-pfs	490	L4	IANA
go-login	491	L4	IANA
ticf-1	492	L4	IANA
ticf-2	493	L4	IANA
pov-ray	494	L4	IANA
intecourier	495	L4	IANA
pim-rp-disc	496	L4	IANA
dantz	497	L4	IANA
siam	498	L4	IANA
iso-ill	499	L4	IANA
stmf	501	L4	IANA
asa-appl-proto	502	L4	IANA
intrinsic	503	L4	IANA
mailbox-lm	505	L4	IANA
ohimsrv	506	L4	IANA
crs	507	L4	IANA
xvttp	508	L4	IANA
snare	509	L4	IANA
fcf	510	L4	IANA
passgo	511	L4	IANA
exec	512	L4	IANA
shell	430		Standard
videotex	516	L4	IANA
talk	517	L4	IANA
ntalk	518	L4	IANA
utime	519	L4	IANA
ripng	521	L4	IANA
ulp	522	L4	IANA
pdap	344	L4	IANA
nep	524	L4	IANA
timed	525	L4	IANA
tempo	526	L4	IANA
stx	527	L4	IANA
custix	528	L4	IANA
irc-serv	529	L4	IANA
courier	530	L4	IANA
conference	531	L4	IANA
netnews	532	L4	IANA
netwall	533	L4	IANA
iiop	535	L4	IANA
opalis-rdv	536	L4	IANA
nmsp	537	L4	IANA
gdomap	538	L4	IANA
apertus-ldp	539	L4	IANA
uucp	540	L4	IANA
uucp-rlogin	541	L4	IANA
commerce	542	L4	IANA
appleqtcsrvr	545	L4	IANA
dhcpx6-client	546	L4	IANA
dhcpx6-server	547	L4	IANA
idfp	549	L4	IANA
new-rwho	550	L4	IANA
cybercash	551	L4	IANA
pirp	553	L4	IANA
remotefs	556	L4	IANA
openvms-sysipc	557	L4	IANA
sdnskmp	558	L4	IANA
teedtap	559	L4	IANA
rmonitor	560	L4	IANA
monitor	561	L4	IANA
chshell	562	L4	IANA
9pfs	564	L4	IANA
whoami	565	L4	IANA
streettalk	566	L4	IANA
banyan-rpc	567	L4	IANA
ms-shuttle	568	L4	IANA

ms-rome	569	L4 IANA
meter	570	L4 IANA
sonar	572	L4 IANA
banyan-vip	573	L4 IANA
ftp-agent	574	L4 IANA
vemmi	575	L4 IANA
ipcd	576	L4 IANA
vnas	577	L4 IANA
ipdd	578	L4 IANA
decbsrv	579	L4 IANA
sntp-heartbeat	580	L4 IANA
bdp	581	L4 IANA
scc-security	582	L4 IANA
philips-vc	583	L4 IANA
keyserver	584	L4 IANA
password-chg	586	L4 IANA
submission	587	L4 IANA
tns-cml	590	L4 IANA
http-alt	8008	L4 IANA
eudora-set	592	L4 IANA
http-rpc-epmap	593	L4 IANA
tpip	594	L4 IANA
cab-protocol	595	L4 IANA
smsd	596	L4 IANA
ptcnameservice	597	L4 IANA
sco-websrvrmg3	598	L4 IANA
acp	599	L4 IANA
ipcserver	600	L4 IANA
urm	606	L4 IANA
nqs	607	L4 IANA
sift-uft	608	L4 IANA
npmp-trap	609	L4 IANA
npmp-local	610	L4 IANA
npmp-gui	611	L4 IANA
hmmp-ind	612	L4 IANA
hmmp-op	613	L4 IANA
sshell	614	L4 IANA
sco-inetmgr	615	L4 IANA
sco-sysmgr	616	L4 IANA
sco-dtmgr	617	L4 IANA
dei-icda	618	L4 IANA
sco-websrvrmgr	620	L4 IANA
escp-ip	621	L4 IANA
collaborator	622	L4 IANA
cryptoadmin	624	L4 IANA
dec_dlm	625	L4 IANA
passgo-tivoli	627	L4 IANA
qmcp	628	L4 IANA
3com-amp3	629	L4 IANA
rda	630	L4 IANA
ipp	631	L4 IANA
bmpp	632	L4 IANA
servstat	633	L4 IANA
ginad	634	L4 IANA
rlzdbase	635	L4 IANA
lanserver	637	L4 IANA
mcns-sec	638	L4 IANA
msdp	639	L4 IANA
entrust-sps	640	L4 IANA
repcmd	641	L4 IANA
esro-emsdp	642	L4 IANA
sanity	643	L4 IANA
dwr	644	L4 IANA
ldp	646	L4 IANA
dhcp-failover	647	L4 IANA
rrp	648	L4 IANA
aminet	2639	L4 IANA
obex	650	L4 IANA
ieee-mms	651	L4 IANA
hello-port	652	L4 IANA
repscmd	653	L4 IANA
aodv	654	L4 IANA
tinc	655	L4 IANA

## show ip nbar protocol-id

spmp	656	L4	IANA
rmc	657	L4	IANA
tenfold	658	L4	IANA
mac-srvr-admin	660	L4	IANA
hap	661	L4	IANA
pftp	662	L4	IANA
purenoise	663	L4	IANA
sun-dr	665	L4	IANA
disclose	667	L4	IANA
mecomm	668	L4	IANA
mereregister	669	L4	IANA
vacdsm-sws	670	L4	IANA
vacdsm-app	671	L4	IANA
vpps-qua	672	L4	IANA
cimplex	673	L4	IANA
acap	674	L4	IANA
dctp	675	L4	IANA
vpps-via	676	L4	IANA
vpp	677	L4	IANA
ggf-ncp	678	L4	IANA
mrm	679	L4	IANA
entrust-aaas	680	L4	IANA
entrust-aams	681	L4	IANA
mdc-portmapper	685	L4	IANA
hcp-wismar	686	L4	IANA
asipregistry	687	L4	IANA
realm-rusd	688	L4	IANA
nmap	689	L4	IANA
vatp	690	L4	IANA
msexch-routing	691	L4	IANA
hyperwave-isp	692	L4	IANA
connendp	693	L4	IANA
ha-cluster	694	L4	IANA
ieee-mms-ssl	695	L4	IANA
rushd	696	L4	IANA
uuidgen	697	L4	IANA
olsr	698	L4	IANA
accessnetwork	699	L4	IANA
elcsd	704	L4	IANA
agentx	705	L4	IANA
silc	706	L4	IANA
borland-dsj	707	L4	IANA
entrust-kmsh	709	L4	IANA
entrust-ash	710	L4	IANA
cisco-tdp	711	L4	IANA
netviewdm1	729	L4	IANA
netviewdm2	730	L4	IANA
netviewdm3	731	L4	IANA
netgw	741	L4	IANA
netrcs	742	L4	IANA
flexlm	744	L4	IANA
fujitsu-dev	747	L4	IANA
ris-cm	748	L4	IANA
pump	751	L4	IANA
qrh	752	L4	IANA
rrh	753	L4	IANA
tell	754	L4	IANA
nlogin	758	L4	IANA
con	759	L4	IANA
ns	760	L4	IANA
rx	761	L4	IANA
quotad	762	L4	IANA
cycleserv	763	L4	IANA
omserv	764	L4	IANA
webster	765	L4	IANA
phonebook	767	L4	IANA
vid	769	L4	IANA
cadlock	770	L4	IANA
rtip	771	L4	IANA
cycleserv2	772	L4	IANA
submit	643		Standard
entomb	775	L4	IANA
multiling-http	777	L4	IANA

wpgs	780	L4	IANA
device	801	L4	IANA
itm-mcell-s	828	L4	IANA
pkix-3-ca-ra	829	L4	IANA
dhcp-failover2	847	L4	IANA
rsync	873	L4	IANA
iclcnet-locate	886	L4	IANA
iclcnet_svinfo	887	L4	IANA
accessbuilder	888	L4	IANA
omginitialrefs	900	L4	IANA
smpnameres	901	L4	IANA
xact-backup	911	L4	IANA
ftps-data	989	L4	IANA
nas	991	L4	IANA
vsinet	996	L4	IANA
maitrd	997	L4	IANA
applix	999	L4	IANA
surf	1010	L4	IANA
rmiactivation	1098	L4	IANA
rmiregistry	1099	L4	IANA
ms-sql-m	1434	L4	IANA
ms-olap	2393	L4	IANA
msft-gc	3268	L4	IANA
msft-gc-ssl	3269	L4	IANA
tlisrv	1527	L4	IANA
coauthor	1529	L4	IANA
rdb-dbs-disp	1571	L4	IANA
oraclenames	1575	L4	IANA
oraclenet8cman	1630	L4	IANA
net8-cman	1830	L4	IANA
micromuse-lm	1534	L4	IANA
orbix-locator	3075	L4	IANA
orbix-config	3076	L4	IANA
orbix-loc-ssl	3077	L4	IANA
shockwave	1626	L4	IANA
sitaraserver	2629	L4	IANA
sitarangmt	2630	L4	IANA
sitaradir	2631	L4	IANA
mysql	3306	L4	IANA
net-assistant	3283	L4	IANA
msnp	1863	L4	IANA
groove	2492	L4	IANA
directplay	2234	L4	IANA
directplay8	6073	L4	IANA
kali	2213	L4	IANA
worldfusion	2595	L4	IANA
directv-web	3334	L4	IANA
directv-soft	3335	L4	IANA
directv-tick	3336	L4	IANA
directv-catlg	3337	L4	IANA
wap-push	2948	L4	IANA
wap-pushsecure	2949	L4	IANA
wap-push-http	4035	L4	IANA
wap-push-https	4036	L4	IANA
wap-wsp	9200	L4	IANA
wap-wsp-wtp	9201	L4	IANA
wap-wsp-s	9202	L4	IANA
wap-wsp-wtp-s	9203	L4	IANA
wap-vcard	9204	L4	IANA
wap-vcal	9205	L4	IANA
wap-vcard-s	9206	L4	IANA
wap-vcal-s	9207	L4	IANA
ibprotocol	6714	L4	IANA
gtp-user	2152	L4	IANA
xdtp	3088	L4	IANA
parsec-game	6582	L4	IANA
hopopt	0	L3	IANA
gpp	3	L3	IANA
st	5	L3	IANA
cbt	7	L3	IANA
zserv	346	L4	IANA
igrp	9	L3	IANA
bbnrccmon	10	L3	IANA

## show ip nbar protocol-id

pawserv	345	L4	IANA
texar	333	L4	IANA
rtsp	322	L4	IANA
pip	1321	L4	IANA
ptp-general	320	L4	IANA
nat-stun	3478	L4	IANA
compressnet	2	L4	IANA
rje	5	L4	IANA
discard	9	L4	IANA
qotd	17	L4	IANA
misp	18	L4	IANA
ftp-data	20	L4	IANA
nsw-fe	27	L4	IANA
msg-icp	29	L4	IANA
csi-sgwp	348	L4	IANA
msg-auth	31	L4	IANA
dsp	33	L4	IANA
rap	38	L4	IANA
rlp	39	L4	IANA
graphics	41	L4	IANA
name	42	L4	IANA
profile	136	L4	IANA
mpm-flags	44	L4	IANA
mpm	45	L4	IANA
mpm-snd	46	L4	IANA
ni-ftp	47	L4	IANA
auditd	48	L4	IANA
emfis-data	140	L4	IANA
re-mail-ck	50	L4	IANA
la-maint	51	L4	IANA
xns-time	52	L4	IANA
emfis-cntl	141	L4	IANA
xns-ch	54	L4	IANA
bl-idm	142	L4	IANA
xns-auth	56	L4	IANA
xns-mail	58	L4	IANA
ni-mail	61	L4	IANA
acas	62	L4	IANA
covia	64	L4	IANA
sql*net	66	L4	IANA
bootps	67	L4	IANA
bootpc	68	L4	IANA
uaac	145	L4	IANA
iso-tp0	146	L4	IANA
netrjs-1	71	L4	IANA
netrjs-2	72	L4	IANA
netrjs-3	73	L4	IANA
netrjs-4	74	L4	IANA
deos	76	L4	IANA
iso-ip	147	L4	IANA
xfer	82	L4	IANA
mit-ml-dev	83	L4	IANA
ctf	84	L4	IANA
mfcobol	86	L4	IANA
jargon	148	L4	IANA
su-mit-tg	89	L4	IANA
dnsix	90	L4	IANA
mit-dov	91	L4	IANA
aed-512	149	L4	IANA
dcp	93	L4	IANA
objcall	94	L4	IANA
supdup	95	L4	IANA
dixie	96	L4	IANA
swift-rvf	97	L4	IANA
tacnews	98	L4	IANA
metagram	99	L4	IANA
hostname	101	L4	IANA
iso-tsap	102	L4	IANA
acr-nema	104	L4	IANA
csnet-ns	105	L4	IANA
3com-tsmux	106	L4	IANA
sql-net	150	L4	IANA
snagas	108	L4	IANA

pop2	109	L4	IANA
hems	151	L4	IANA
mcidas	112	L4	IANA
auth	113	L4	IANA
sftp	115	L4	IANA
ansanotify	116	L4	IANA
uucp-path	117	L4	IANA
sqlserv	118	L4	IANA
cfdpkt	120	L4	IANA
erpc	121	L4	IANA
smakynet	122	L4	IANA
bftp	152	L4	IANA
ansatrader	124	L4	IANA
locus-map	125	L4	IANA
nxedit	126	L4	IANA
locus-con	127	L4	IANA
gss-xlicen	128	L4	IANA
pwdgen	129	L4	IANA
cisco-fna	130	L4	IANA
sgmp	153	L4	IANA
netsc-prod	154	L4	IANA
netsc-dev	155	L4	IANA
knet-cmp	157	L4	IANA
pcmail-srv	158	L4	IANA
nss-routing	159	L4	IANA
sgmp-traps	160	L4	IANA
cmip-man	163	L4	IANA
cmip-agent	164	L4	IANA
xns-courier	165	L4	IANA
s-net	166	L4	IANA
namp	167	L4	IANA
rsvd	168	L4	IANA
send	169	L4	IANA
print-srv	170	L4	IANA
multiplex	171	L4	IANA
xyplex-mux	173	L4	IANA
mailq	174	L4	IANA
vmnet	175	L4	IANA
genrad-mux	176	L4	IANA
nextstep	178	L4	IANA
ris	180	L4	IANA
unify	181	L4	IANA
audit	182	L4	IANA
ocbinder	183	L4	IANA
ocserver	184	L4	IANA
remote-kis	185	L4	IANA
kis	186	L4	IANA
mumps	188	L4	IANA
qft	189	L4	IANA
gacp	190	L4	IANA
prospero	191	L4	IANA
osu-nms	192	L4	IANA
srmp	193	L4	IANA
dn6-nlm-aud	195	L4	IANA
dls	197	L4	IANA
dls-mon	198	L4	IANA
smux	199	L4	IANA
src	200	L4	IANA
at-rtmp	201	L4	IANA
at-nbp	202	L4	IANA
at-3	203	L4	IANA
at-echo	204	L4	IANA
at-5	205	L4	IANA
at-zis	206	L4	IANA
at-7	207	L4	IANA
at-8	208	L4	IANA
qmtp	209	L4	IANA
z39.50	210	L4	IANA
914c/g	211	L4	IANA
anet	212	L4	IANA
vmpwscs	214	L4	IANA
softpc	215	L4	IANA
CAIllic	216	L4	IANA

```

dbase                217          L4 IANA
mpp                  218          L4 IANA
uarps                219          L4 IANA
fln-spx              221          L4 IANA
rsh-spx              222          L4 IANA
cdc                  223          L4 IANA
masqdialer           224          L4 IANA
sur-meas             243          L4 IANA
inbusiness           244          L4 IANA
dsp3270              246          L4 IANA
subntbcst_tftp      247          L4 IANA
bhfhs                248          L4 IANA
set                  257          L4 IANA
esro-gen             259          L4 IANA
openport             260          L4 IANA
nsiiops              261          L4 IANA
arcisdms             262          L4 IANA
hdap                 263          L4 IANA
bgmp                 264          L4 IANA
x-bone-ctl           265          L4 IANA
sst                  266          L4 IANA
td-service           267          L4 IANA
td-replica           268          L4 IANA
http-mgmt            280          L4 IANA
personal-link        281          L4 IANA
cableport-ax         282          L4 IANA
rescap               283          L4 IANA
corerjd              284          L4 IANA
k-block              287          L4 IANA
novastorbakcup       308          L4 IANA
bhmds                310          L4 IANA
asip-webadmin        311          L4 IANA
vslmp                312          L4 IANA
magenta-logic        313          L4 IANA
opalys-robot         314          L4 IANA
dpsi                 315          L4 IANA
decauth              316          L4 IANA
zannet               317          L4 IANA
pkix-timestamp       318          L4 IANA
ptp-event            319          L4 IANA
cisco-tna            131          L4 IANA
cisco-sys            132          L4 IANA
statsrv              133          L4 IANA
ingres-net           134          L4 IANA
Konspire2b           6085         L4 IANA
Total protocols:     721

```

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

**Table 29: show ip nbar protocol-id Field Descriptions**

Field	Description
Protocol Name	Name of the NBAR protocol.
id	Unique identifier assigned to the NBAR protocol.
type	Indicates whether the protocol is standard or customized.

**Related Commands**

Command	Description
<b>ip nbar custom</b>	Extends the capability of NBAR Protocol Discovery to classify and monitor additional static port applications or allows NBAR to classify nonsupported static port traffic.

# show ip nbar protocol-pack

To display protocol pack information, use the **show ip nbar protocol-pack** command in user EXEC or privileged EXEC mode.

**show ip nbar protocol-pack** *{protocol-pack| active}* [**detail**]

## Syntax Description

<i>protocol-pack</i>	Protocol pack file path and name.
<b>active</b>	Displays active protocol pack information.
<b>detail</b>	(Optional) Displays detailed protocol pack information.

## Command Modes

User EXEC (>)

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

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

## Examples

The following sample output from the **show ip nbar protocol-pack** command shows information about the active protocol pack:

```
Router# show ip nbar protocol-pack active
ACTIVE protocol pack:
Name:                               Default Protocol Pack
Version:                             1.0
Publisher:                           Cisco Systems Inc.
```

The following sample output from the **show ip nbar protocol-pack** command shows detailed information about the active protocol pack:

```
Router# show ip nbar protocol-pack active detail
ACTIVE protocol pack:
Name:                               Default Protocol Pack
Version:                             1.0
```

```

Publisher:                Cisco Systems Inc.
Protocols:
base                      Mv: 4
ftp                       Mv: 5
http                      Mv: 18
static                    Mv: 6
socks                     Mv: 2
nntp                      Mv: 2
tftp                      Mv: 2
exchange                  Mv: 3
vdolive                   Mv: 1
sqlnet                    Mv: 2
netshow                   Mv: 3
sunrpc                    Mv: 3
streamwork                Mv: 2
citrix                    Mv: 11
fasttrack                 Mv: 3
gnutella                  Mv: 7
kazaa2                    Mv: 11

```

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

**Table 30: show ip nbar protocol-pack Field Descriptions**

Field	Description
Name	Name of the protocol pack.
Version	Protocol pack version.
Publisher	Name of the publisher of the protocol pack.
Protocols	List of protocols present in the protocol pack.

#### Related Commands

Command	Description
<b>default ip nbar protocol-pack</b>	Loads the base version of the protocol pack and removes all other loaded protocol packs.
<b>ip nbar protocol-pack</b>	Loads a protocol pack.

# show ip nbar resources flow

To display the current configuration and the utilization of resources in the Network-Based Application Recognition (NBAR), use the **show ip nbar resources flow** command in privileged EXEC mode.

**show ip nbar resources flow**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

## Examples

The following is the sample output from the **show ip nbar resources flow** command. The fields in the display are self-explanatory.

```
Router# show ip nbar resources flow

NBAR flow statistics
  Maximum no of sessions allowed : 3500000
  Maximum memory usage allowed   : 734003 KBytes
  Active sessions                 : 3499950
  Active memory usage             : 665364 KBytes
  Peak session                    : 3499950
  Peak memory usage               : 672396 KBytes
```

## Related Commands

Command	Description
<b>ip nbar resources flow max-session</b>	Configures the maximum flow sessions to be allowed in a flow table.

## show ip nbar statistics

To display failure statistics, the number of packets per flow, and different types of classifications on a device that runs Network-Based Application Recognition (NBAR), use the **show ip nbar statistics** command in privileged EXEC mode.

**show ip nbar statistics**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Privileged EXEC (#)

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

**Examples** The following is sample output from the **show ip nbar statistics** command. The fields in the output are self-explanatory.

```
Device# show ip nbar statistics
Compiler statistics
Malloc failure = 0
Control-plane statistics
Malloc failure = 0
Invalid iterators = 0
Data-plane statistics
Malloc failure = 0
FO create failure = 0
CFT Age set failure = 0
```

# show ip nbar trace

To display the path traversed by a packet on a data plane, use the **show ip nbar trace** command in privileged EXEC mode.

**show ip nbar trace**{detail|summary}[config]

## Syntax Description

<b>detail</b>	Displays the classification trace in detail.
<b>summary</b>	Displays the classification trace summary.
<b>config</b>	(Optional) Displays the configuration information for state-graph tracing.

## Command Default

Information about all paths traversed by a packet is displayed.

## Command Modes

Privileged EXEC (#)

## Command History

Release	Modification
15.2(4)M	This command was introduced.

## Usage Guidelines

Trace and summary debugging must be enabled.

## Examples

The following is sample output from the **show ip nbar trace summary** command. The fields in the output are self-explanatory.

```
Device# show ip nbar trace summary

Classification: 76, flag: 163
Searched Source WKP
Searched Dest WKP
Classifying using Heuristic regexp
Classifying using Heuristic General
Classifying using MPE

Classification: 1, flag: 160
Searched Source WKP
Searched Dest WKP
Classifying using Heuristic regexp
Classifying using Heuristic General
Classifying using MPE
```

The following is sample output from the **show ip nbar trace detail** command. The fields in the output are self-explanatory.

```
Device# show ip nbar trace detail

Graph Id 1
Classification: 82, flag: 163
Packet No: 1
String: Searching Source V4 WKP
String: Searching Destination V4 WKP
String: Entering loop core from Heuristic Regex
State Node:http-verify-heuristic-entry-point-get
State Node:http-verify-heuristic-entry-point-get
State Node:HTTP-url-get-check
State Node:HTTP-url-get-check
State Node:HTTP-url-get-check
State Node:HTTP-url-get-check
State Node:youtube-found-url
State Node:http-check-url-fe
State Node:HTTP-request-advance-packet-pointer-to-next-http-header
State Node:HTTP-request-advance-packet-pointer-to-next-http-header
State Node:HTTP-request-advance-packet-pointer-to-next-http-header
State Node:HTTP-request-end-of-request-check
State Node:HTTP-request-check-end-of-packet
State Node:HTTP-request-check-end-of-packet
State Node:HTTP-request-headers-parser
State Node:HTTP-request-headers-parser
Graph Id 1
```

#### Related Commands

Command	Description
<b>clear ip nbar trace summary</b>	Clears classification modules.
<b>debug ip nbar config</b>	Enables debugging of all commands configured for activation and deactivation of the NBAR.

## show ip nbar unclassified-port-stats

To display the network-based application recognition (NBAR) port statistics for unclassified packets, use the **show ip nbar unclassified-port-stats** command in privileged EXEC mode.

```
show ip nbar unclassified-port-stats [top-talkers] ip [protocol-number [number-protocols ]] top top-talkers]
[tcp | udp] [port-number [number-ports ]] top top-talkers | bottom bottom-talkers]]
```

### Syntax Description

<i>top-talkers</i>	(Optional) Number of top talkers to show.
ip	(Optional) Displays port statistics for unclassified non-TCP/non-UDP packets.
<i>protocol-number</i>	(Optional) Starting IP protocol number.
<i>number-protocols</i>	(Optional) Number of protocols to show.
top	(Optional) Specifies that a top-n is to be displayed. A top-n is the number of most active NBAR-supported protocols, where n is the number of protocols to be displayed. For instance, if top-n 3 is entered, the three most active NBAR-supported protocols are displayed.
tcp	(Optional) Displays port statistics for unclassified TCP packets.
udp	(Optional) Displays port statistics for unclassified UDP packets.
<i>port-number</i>	(Optional) Starting TCP or UDP port number.
<i>number-ports</i>	(Optional) Number of ports to show.
bottom	(Optional) Specifies that a bottom-n is to be displayed. A bottom-n is the number of least active NBAR-supported protocols, where n is the number of protocols to be displayed. For instance, if bottom-n 3 is entered, the three least active NBAR-supported protocols are displayed.
<i>bottom-talkers</i>	(Optional) Number of bottom talkers to show.

### Command Modes

Privileged EXEC (#)

**Command History**

Release	Modification
12.0(5)XE2	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(13)E	This command was implemented on Cisco Catalyst 6000 family switches without FlexWAN modules.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)ZYA	This command was integrated into Cisco IOS Release 12.2(18)ZYA. This command was modified to include information about VLANs (as applicable) and to provide support for both Layer 2 and Layer 3 Etherchannels (Cisco Catalyst switches only).

**Usage Guidelines**

By default, NBAR unclassified mechanisms are not enabled. Use the **debugipnbarunclassified-port-stats** command to configure the router to begin tracking the ports on which packets arrive. Then use the **showipnbarunclassified-port-stats** command to verify the collected information.

**Examples**

The following is sample output from **showipnbarunclassified-port-stats** command:

```
Router# show ip nbar unclassified-port-stats
-tcp-
  80/tcp:48
 1443/tcp:3
 1423/tcp:2
 1424/tcp:2
 1425/tcp:2
-udp-
 1985/udp:158
 1029/udp:13
  496/udp:4
 1445/udp:3
 1449/udp:2
```

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

**Table 31: show ip nbar unclassified-port-stats Field Descriptions**

Field	Description
-tcp-	TCP Protocol.

Field	Description
80/tcp:48	80 represents the port number, tcp the protocol and 48 the number of packets.
-udp-	UDP protocol.
1985/udp:158	1855 represents the port number, udp the protocol and 158 the number of packets.

The output displays the port number, the protocol and the number of packets. For example, in 80/tcp:48, 80 represents the port number, tcp the protocol and 48 the number of packets.

### Related Commands

Command	Description
<b>ip nbar custom</b>	Extends the capability of NBAR Protocol Discovery to classify and monitor additional static port applications or to allow NBAR to classify unsupported static port traffic.
<b>ip nbar pdlm</b>	Extends or enhances the list of protocols recognized by NBAR through a Cisco-provided PDLM.
<b>ip nbar port-map</b>	Configures NBAR to search for a protocol or protocol name using a port number other than the well-known port number.
<b>ip nbar protocol-discovery</b>	Configures NBAR to discover traffic for all protocols that are known to NBAR on a particular interface.
<b>ip nbar resources protocol</b>	Sets the expiration time for NBAR flow-link tables on a protocol basis.
<b>ip nbar resources system</b>	Sets the expiration time and memory requirements for NBAR flow-link tables on a systemwide basis.
<b>show ip nbar pdlm</b>	Displays the PDLM in use by NBAR.
<b>show ip nbar port-map</b>	Displays the current protocol-to-port mappings in use by NBAR.
<b>show ip nbar protocol-discovery</b>	Displays the statistics gathered by the NBAR Protocol Discovery feature.
<b>show ip nbar version</b>	Displays information about the version of the NBAR software in your Cisco IOS release or the version of an NBAR PDLM on your Cisco IOS router.

# show ip nbar version

To display information about the version of the network-based application recognition (NBAR) software in your Cisco IOS release or the version of an NBAR Packet Description Language Module (PDLM) on your Cisco IOS router, use the **show ip nbar version** command in **privileged EXEC** mode.

```
show ip nbar version [ PDLM-name ]
```

## Syntax Description

<i>PDLM-name</i>	(Optional) Specifies the name of a specific PDLM whose information will be displayed.
------------------	---

## Command Modes

Privileged EXEC

## Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

## Usage Guidelines

The **show ip nbar version** command treats all protocols that were added to NBAR after the initial NBAR release as PDLMs, including protocols that were added into the Cisco IOS software without a user having to download a PDLM from Cisco.com. PDLMs downloaded from Cisco.com and incorporated into NBAR by the user also appear when the **show ip nbar version** command is entered.

When using NBAR, various elements within NBAR are assigned versioning numbers. These versioning numbers become significant when you want to download a PDLM. PDLMs, which are also versioned, can be downloaded only to NBAR on a particular Cisco IOS release if the PDLM versioning numbers are compatible with the NBAR version numbers in the Cisco IOS software.

The following NBAR-related version information is available:

- NBAR Software Version--Version of NBAR software running on the current version of Cisco IOS software.
- Resident Module Version--Version of the NBAR-supported PDLM protocol.

The following version number is kept by the PDLM:

- NBAR Software Version--Minimum version of the NBAR software that is required to load this PDLM.

The **show ip nbar version** command provides version information for PDLMs already loaded onto the Cisco IOS software.

## Examples

The following is sample output from the show ip nbar version command:

```
Router# show ip nbar version
NBAR software version: 3
1 base Mv: 2
2 ftp Mv: 2
3 http Mv: 7, Nv: 3; slot1:http_vers.pdlm
4 static-port Mv: 6
5 tftp Mv: 1
6 exchange Mv: 1
7 vdolive Mv: 1
8 sqlnet Mv: 1
9 rcmd Mv: 1
10 netshow Mv: 1
11 sunrpc Mv: 2
12 streamwork Mv: 1
13 citrix Mv: 5
14 fasttrack Mv: 2
15 gnutella Mv: 1
16 kazaa Mv: 6, Nv: 3; slot1:kazaa2_vers.pdlm
17 custom-protocols Mv: 1
18 rtsp Mv: 1
19 rtp Mv: 2
20 mgcp Mv: 1
21 skinny Mv: 1
22 h323 Mv: 1
23 sip Mv: 1
24 rtcp Mv: 1
```

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

**Table 32: show ip nbar version Command Field Descriptions**

Field	Description
NBAR Software Version	NBAR software version running in the current Cisco IOS software. In this particular example, version 3 is the NBAR software running on the current version of the Cisco IOS software.
Mv	Resident Module Version. The Resident Module Version is the version of the NBAR-supported PDLM protocol and, therefore, varies by protocol. The Resident Module Version of TFTP, for example, is 1.
Nv	Minimum version of the NBAR software that is required to load a nonnative PDLM. This number is available only for nonnative PDLMs that were loaded onto the router such as the Kazaa PDLM (protocol 17); in that case, the Nv version is 3.

For the same network setup, the following example shows the output if a specific protocol with a PDLM is specified in the `show ip nbar version` CLI:

```
Router# show ip nbar version http
http                               Mv: 7, Nv: 3; slot1:http_vers.pdlm
```

#### Related Commands

Command	Description
<code>ip nbar pdlm</code>	Downloads a PDLM onto a router to add support for additional protocols in NBAR.

# show ip rsvp

To display information about the Resource Reservation Protocol (RSVP), use the **show ip rsvp** command in user EXEC or privileged EXEC mode.

## show ip rsvp

### Syntax Description

This command has no arguments or keywords.

### Command Modes

User EXEC (>) Privileged EXEC (#)

### Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(13)T	This command was modified. The <b>listeners</b> and <b>policy</b> keywords were added, and this command was modified to display RSVP global settings when no keywords or arguments are entered.
12.2(33)SRB	This command was modified. The command output was modified to display fast local repair (FLR) information.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was modified. The command output was modified to display the following: <ul style="list-style-type: none"> <li>• RSVP quality of service (QoS) and Multiprotocol Label Switching (MPLS) traffic engineering (TE) information.</li> <li>• RSVP aggregation information.</li> </ul>
15.0(1)M	This command was modified.  The [ <b>atm-peak-rate-limit</b>   <b>counters</b>   <b>host</b>   <b>installed</b>   <b>interface</b>   <b>listeners</b>   <b>neighbor</b>   <b>policy</b>   <b>precedence</b>   <b>request</b>   <b>reservation</b>   <b>sbm</b>   <b>sender</b>   <b>signalling</b>   <b>tos</b> ] syntax was removed from the command. The keyword options are represented in the following individual command files: show ip rsvp <b>atm-peak-rate-limit</b> , show ip rsvp <b>counters</b> , show ip rsvp <b>host</b> , show ip rsvp <b>installed</b> , show ip rsvp <b>interface</b> , show ip rsvp <b>listeners</b> , show ip rsvp <b>neighbor</b> , show ip rsvp <b>policy</b> , show ip rsvp <b>precedence</b> , show ip rsvp <b>request</b> , show ip rsvp <b>reservation</b> , show ip rsvp <b>sbm</b> , show ip rsvp <b>sender</b> , show ip rsvp <b>signalling</b> , and show ip rsvp <b>tos</b> commands.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

**Examples**

The following is sample output from the **showiprsvp** command:

```

Router# show ip rsvp
RSVP: enabled (on 1 interface(s))
  RSVP QoS signalling enabled
  MPLS/TE signalling enabled
Signalling:
  Refresh interval (msec): 30000
  Refresh misses: 4
Rate Limiting: enabled
  Burst: 8
  Limit: 37
  Maxsize: 2000
  Period (msec): 20
  Max rate (msgs/sec): 400
Refresh Reduction: disabled
  ACK delay (msec): 250
  Initial retransmit delay (msec): 1000
  Local epoch: 0xCE969E
  Message IDs: in use 0, total allocated 0, total freed 0
Neighbors: 0
  Raw IP encap: 0  UDP encap: 0  Raw IP, UDP encap: 0
RFC 3175 Aggregation: Enabled
  Level: 1
  Default QoS service: Controlled-Load
  Router ID: 10.22.22.22
  Number of signaled aggregate reservations:      0
  Number of signaled E2E reservation:            0
  Number of configured map commands:             0
  Number of configured reservation commands:     0
Hello:
  RSVP Hello for Fast-Reroute/Reroute: Disabled
  Statistics: Disabled
  BFD for Fast-Reroute/Reroute: Disabled
  RSVP Hello for Graceful Restart: Disabled
Graceful Restart: Disabled
  Refresh interval: 10000 msec
  Refresh misses: 4
  DSCP: 0x30
  Advertised restart time: 5 msec
  Advertised recovery time: 0 msec
  Maximum wait for recovery: 3600000 msec
Fast-Reroute:
  PSBs w/ Local protection desired
  Yes: 0
  No: 0
Fast Local Repair: enabled
  Max repair rate (paths/sec): 400
  Max processed (paths/run): 1000
Local policy:
COPS:
Generic policy settings:
  Default policy: Accept all
  Preemption: Disabled

```

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

**Table 33: show ip rsvp Field Descriptions**

Field	Description
RSVP	<p>The state of RSVP, QoS, and MPLS TE signaling; values are enabled (activated) or disabled (deactivated).</p> <p><b>Note</b> This field is disabled only if an internal error occurred when registering with RIB.</p>
Signalling	<p>The RSVP signaling parameters in effect are as follows:</p> <ul style="list-style-type: none"> <li>• Refresh interval--Time, in milliseconds (ms), between sending refreshes for each RSVP state.</li> <li>• Refresh misses--Number of successive refresh messages that can be missed before RSVP considers the state expired and tears it down.</li> </ul>
Rate Limiting: enabled or disabled	<p>The RSVP rate-limiting parameters in effect are as follows:</p> <ul style="list-style-type: none"> <li>• Burst--Maximum number of RSVP messages allowed to be sent to a neighboring router during an interval.</li> <li>• Limit--Maximum number of RSVP messages to send per queue interval.</li> <li>• Maxsize--Maximum size of the message queue, in bytes.</li> <li>• Period--Length of an interval (time frame), in milliseconds (ms).</li> <li>• Max rate--Maximum number of messages allowed to be sent per second.</li> </ul>

Field	Description
Refresh Reduction: enabled or disabled	<p>The RSVP refresh-reduction parameters in effect are as follows:</p> <ul style="list-style-type: none"> <li>• ACK delay (msec)--How long, in milliseconds, before the receiving router sends an acknowledgment (ACK).</li> <li>• Initial retransmit delay (msec)--How long, in milliseconds, before the router retransmits a message.</li> <li>• Local epoch--The RSVP message identifier (ID); randomly generated each time a node reboots or the RSVP process restarts.</li> <li>• Message IDs--The number of message IDs in use, the total number allocated, and the total number available (freed).</li> </ul>
Neighbors	<p>The total number of neighbors and the types of encapsulation in use including RSVP and User Datagram Protocol (UDP).</p>
RFC 3175 Aggregation	<p>The state of aggregation as defined in RFC 3175, <i>Aggregation of RSVP for IPv4 and IPv6 Reservations</i>; values are the following:</p> <ul style="list-style-type: none"> <li>• Enabled--Active.</li> <li>• Disabled--Inactive.</li> </ul>
Level	<p>Aggregation level of the reservations; common values are the following:</p> <ul style="list-style-type: none"> <li>• 0 = End-to-end (E2E) reservations.</li> <li>• 1 = Aggregated reservations.</li> </ul> <p>Level <math>x</math> reservations can be aggregated to form reservations at level <math>x + 1</math>.</p>

Field	Description
Default QoS service	Type of QoS configured; values are the following: <ul style="list-style-type: none"> <li>• Controlled-Load--Allows applications to reserve bandwidth to meet their requirements. For example, RSVP with Weighted Random Early Detection (WRED) provides this kind of service.</li> <li>• Guaranteed-Rate--Allows applications to have low delay and high throughput even during times of congestion. For example, weighted fair queueing (WFQ) with RSVP provides this kind of service.</li> </ul>
Number of signaled aggregate reservations	Cumulative number of signaled aggregate reservations.
Number of signaled E2E reservations	Cumulative number of signaled E2E reservations.
Number of configured map commands	Cumulative number of configured map commands.
Number of configured reservation commands	Cumulative number of configured reservation commands.
Hello	Subsequent fields describe the processes for which hello is enabled or disabled. Choices are Fast Reroute, reroute (hello for state timer), bidirectional forwarding detection (BFD), and Graceful Restart for a node with restart capability.
Statistics	Status of hello statistics. Valid values are as follows: <ul style="list-style-type: none"> <li>• Enabled--Statistics are configured. Hello packets are time-stamped when they arrive in the hello input queue for the purpose of recording the time it takes until they are processed.</li> <li>• Disabled--Hello statistics are not configured.</li> <li>• Shutdown--Hello statistics are configured, but not operational. The input queue is too long (that is, more than 10,000 packets are queued).</li> </ul>

Field	Description
Graceful Restart: Enabled or Disabled	<p>The RSVP Graceful Restart parameters in effect are as follows:</p> <ul style="list-style-type: none"> <li>• Refresh interval--Frequency, in milliseconds (ms), with which a node sends a hello message to its neighbor.</li> <li>• Refresh misses--Number of missed hello messages that trigger a neighbor-down event upon which stateful switchover (SSO) procedures are started.</li> <li>• DSCP--Differentiated services code point (DSCP) value in the IP header of a hello message.</li> <li>• Advertised restart time--Time, in milliseconds, required for the sender to restart the RSVP-traffic engineering component and exchange hello messages after a failure.</li> <li>• Advertised recovery time--Time, in milliseconds, within which a recovering node wants its neighbor router to resynchronize the RSVP or MPLS forwarding state after SSO. A zero value indicates that the RSVP or MPLS forwarding state is not preserved after SSO.</li> <li>• Maximum wait for recovery--Maximum amount of time, in milliseconds, that a router waits for a neighbor to recover.</li> </ul>
Fast-Reroute	<p>The Fast Reroute parameters in effect are as follows:</p> <ul style="list-style-type: none"> <li>• PSBs w/ Local protection desired--Yes means that path state blocks (PSBs) are rerouted when a tunnel goes down and packet flow is not interrupted; No means that PSBs are not rerouted.</li> </ul>
Fast Local Repair: enabled or disabled	<p>The Fast Local Repair parameters in effect are as follows:</p> <ul style="list-style-type: none"> <li>• Max repair rate (paths/sec)--Maximum repair rate, in paths per second.</li> <li>• Max processed (paths/run)--Maximum notification elements processed, in paths per run.</li> </ul>
Local policy	The local policy currently configured.

Field	Description
COPS	The Common Open Policy Service (COPS) currently in effect.
Generic policy settings	<p>Policy settings that are not specific to COPS or the local policy.</p> <ul style="list-style-type: none"> <li>• Default policy: 'Accept all' means that all RSVP messages are accepted and forwarded. 'Reject all' means all RSVP messages are rejected.</li> <li>• Preemption: 'Disabled' means that RSVP is not prioritizing reservations and allocating bandwidth accordingly. 'Enabled' means that RSVP is prioritizing reservations and allocating more bandwidth to those with the highest priority.</li> </ul>

**Related Commands**

Command	Description
<b>debug ip rsvp</b>	Displays debug messages for RSVP categories.
<b>show ip rsvpatm-peak-rate-limit</b>	Displays the current peak rate limit set for an interface or for all interfaces.
<b>show ip rsvpcounters</b>	Displays the number of RSVP messages sent and received on each interface.
<b>show ip rsvp host</b>	Displays specific information for an RSVP host.
<b>show ip rsvp installed</b>	Displays RSVP related installed filters and corresponding bandwidth information.
<b>show ip rsvp interface</b>	Displays information about interfaces on which RSVP is enabled.
<b>show ip rsvp listeners</b>	Displays the RSVP listeners for a specified port or protocol.
<b>show ip rsvp neighbor</b>	Displays information about the current RSVP neighbors.
<b>show ip rsvp policy</b>	Displays information about the currently configured RSVP policies.
<b>show ip rsvp precedence</b>	Displays IP precedence information about the interfaces on which RSVP is enabled.

<b>Command</b>	<b>Description</b>
<b>show ip rsvp request</b>	Displays current RSVP-related request information.
<b>show ip rsvp reservation</b>	Displays current RSVP-related receiver information.
<b>show ip rsvp sbm</b>	Displays SBM configuration information about RSVP-enabled interfaces.
<b>show ip rsvp sender</b>	Displays the RSVP PATH-related sender information
<b>show ip rsvp signalling</b>	Displays RSVP signaling information.
<b>show ip rsvp tos</b>	Displays IP ToS information about the interfaces on which RSVP is enabled.

## show ip rsvp aggregation ip

To display Resource Reservation Protocol (RSVP) summary aggregation information, use the **show ip rsvp aggregation ip** command in user EXEC or privileged EXEC mode.

```
show ip rsvp aggregation ip [endpoints [detail] [dscp value] [remote ip-address] [role {aggregator|deaggregator}]] interface [if-name] map [dscp value] reservation [dscp value [aggregator ip-address]]
```

### Syntax Description

<b>endpoints</b>	(Optional) Specifies the aggregator and deaggregator nodes for the aggregation region.
<b>interface</b> <i>if-name</i>	(Optional) Specifies the interface name.
<b>map</b>	(Optional) Displays the map configuration rules.
<b>dscp</b> <i>value</i>	(Optional) Specifies the differentiated services code point (DSCP) for the <b>map</b> keyword. Values can be the following: <ul style="list-style-type: none"> <li>• 0 to 63--Numerical DSCP values. The default value is 0.</li> <li>• af11 to af43--Assured forwarding (AF) DSCP values.</li> <li>• cs1 to cs7--Type of service (ToS) precedence values.</li> <li>• default--Default DSCP value.</li> <li>• ef--Expedited forwarding (EF) DSCP values.</li> </ul>
<b>reservation</b>	(Optional) Displays the reservation configuration.
<b>dscp</b> <i>value</i>	(Optional) Specifies the differentiated services code point (DSCP) for the <b>reservation</b> keyword. Values can be the following: <ul style="list-style-type: none"> <li>• 0 to 63--Numerical DSCP values. The default value is 0.</li> <li>• af11 to af43--Assured forwarding (AF) DSCP values.</li> <li>• cs1 to cs7--Type of service (ToS) precedence values.</li> <li>• default--Default DSCP value.</li> <li>• ef--Expedited forwarding (EF) DSCP values.</li> </ul>

<b>aggregator</b> <i>ip-address</i>	(Optional) Specifies the IP address of the aggregator.
-------------------------------------	--

**Command Default** If you enter the **show ip rsvp aggregation ip** command without an optional keyword, the command displays summary information for all aggregate reservations.

**Command Modes** User EXEC (>) Privileged EXEC (#)

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	12.2(33)SRC	This command was introduced.
	Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

**Usage Guidelines** Use the **show ip rsvp aggregation ip** command to display summary information for aggregation, including the number of aggregate, map, and reservation configurations.

### Examples

#### Examples

The following is sample output from the **show ip rsvp aggregation ip** command:

```
Router# show ip rsvp aggregation ip
RFC 3175 Aggregation: Enabled
  Level: 1
  Default QoS service: Controlled-Load
  Number of signaled aggregate reservations: 2
  Number of signaled E2E reservations:      8
  Number of configured map commands:       4
  Number of configured reservation commands: 1
```

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

**Table 34: show ip rsvp aggregation ip Field Descriptions**

<b>Field</b>	<b>Description</b>
RFC 3175 Aggregation	The state of aggregation as defined in RFC 3175, <i>Aggregation of RSVP for IPv4 and IPv6 Reservations</i> ; values are the following: <ul style="list-style-type: none"> <li>• Enabled--Active.</li> <li>• Disabled--Inactive.</li> </ul>

Field	Description
Level	<p>Aggregation level of the reservations; common values are the following:</p> <ul style="list-style-type: none"> <li>• 0 = End-to-end (E2E) reservations.</li> <li>• 1 = Aggregated reservations.</li> </ul> <p><b>Note</b> Level x reservations can be aggregated to form reservations at the next higher level; for example, level x+1.</p>
Default QoS service	<p>Type of quality of service (QoS) configured; values are the following:</p> <ul style="list-style-type: none"> <li>• <b>Controlled-Load</b>--Allows applications to reserve bandwidth to meet their requirements. For example, RSVP with Weighted Random Early Detection (WRED) provides this kind of service.</li> <li>• <b>Guaranteed-Rate</b>--Allows applications to have low delay and high throughput even during times of congestion. For example, Weighted Fair Queueing (WFQ) with RSVP provides this kind of service.</li> </ul>
Number of signaled aggregate reservations	Cumulative number of signaled aggregate reservations.
Number of signaled E2E reservations	Cumulative number of signaled E2E reservations.
Number of configured map commands	Cumulative number of configured map commands.
Number of configured reservation commands	Cumulative number of configured reservation commands.

## Examples

The following is sample output from the **show ip rsvp aggregation ip interface** command:

```
Router# show ip rsvp aggregation ip interface
Interface Name      Role
-----
Ethernet0/0        interior
Serial2/0           exterior
Serial3/0           exterior
```

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

**Table 35: show ip rsvp aggregation ip interface Field Descriptions**

Field	Description
Interface Name	Name and number of the interface.
Role	Configuration of a router's interfaces; values are interior and exterior.

The following is sample output from the **show ip rsvp aggregation ip interface** command with a specified interface:

```
Router# show ip rsvp aggregation ip interface Ethernet0/0
Interface Name      Role
-----
Ethernet0/0        interior
```

**Related Commands**

Command	Description
<b>ip rsvp aggregation ip</b>	Enables RSVP aggregation on a router.

## show ip rsvp aggregation ip endpoints

To display Resource Reservation Protocol (RSVP) information about aggregator and deaggregator routers, use the **show ip rsvp aggregation ip endpoints** command in user EXEC or privileged EXEC mode.

```
show ip rsvp aggregation ip endpoints [detail] [dscp value] [remote ip-address] [role {aggregator|deaggregator}]
```

### Syntax Description

<b>detail</b>	(Optional) Displays additional information about the aggregators and deaggregators.
<b>dscp</b> <i>value</i>	(Optional) Specifies the differentiated services code point (DSCP) for the aggregator and deaggregator routers. Values can be the following: <ul style="list-style-type: none"> <li>• 0 to 63--Numerical DSCP values. The default value is 0.</li> <li>• af11 to af43--Assured forwarding (AF) DSCP values.</li> <li>• cs1 to cs7--Type of service (ToS) precedence values.</li> <li>• default--Default DSCP value.</li> <li>• ef--Expedited forwarding (EF) DSCP values.</li> </ul>
<b>remote</b>	(Optional) Specifies the remote deaggregator.
<i>ip-address</i>	IP address of the remote deaggregator.
<b>role</b>	(Optional) Specifies a router's position in the aggregation region.
<b>aggregator</b>	(Optional) Specifies the router at the beginning of the aggregation region.
<b>deaggregator</b>	(Optional) Specifies the router at the end of the aggregation region.

### Command Default

If you enter the **show ip rsvp aggregation ip endpoints** command without an optional keyword, the command displays information for all aggregate reservations.

### Command Modes

User EXEC (>) Privileged EXEC (#)

**Command History**

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

**Usage Guidelines**

Use the **showiprsvpaggregationipendpoints** command to display any of the following output at aggregator and deaggregator routers:

- All aggregate reservations.
- All aggregate reservations for which a node is the aggregator.
- All aggregate reservations for which a node is the deaggregator.
- All aggregate reservations for which the remote node is identified with an IP address.
- All aggregate reservations for a given DSCP.
- Any combination of the preceding options; for example, all aggregates with a given DSCP for which a node is an aggregator and the remote node as specified in the IP address.
- Any of the preceding options with detailed information.

**Examples**

The following is sample output from the **showiprsvpaggregationipendpointsdetail** command:

```
Router# show ip rsvp aggregation ip endpoints detail
Role DSCP Aggregator Deaggregator State Rate Used QBM PoolID
-----
Agg 46 10.3.3.3 10.4.4.4 ESTABL 100K 100K 0x00000003
Aggregate Reservation for the following E2E Flows (PSBs):
To From Pro DPort Sport Prev Hop I/F BPS
10.4.4.4 10.1.1.1 UDP 1 1 10.23.20.3 Et1/0 100K
Aggregate Reservation for the following E2E Flows (RSBs):
To From Pro DPort Sport Next Hop I/F Fi Serv BPS
10.4.4.4 10.1.1.1 UDP 1 1 10.4.4.4 Se2/0 FF RATE 100K
Aggregate Reservation for the following E2E Flows (Reqs):
To From Pro DPort Sport Next Hop I/F Fi Serv BPS
10.4.4.4 10.1.1.1 UDP 1 1 10.23.20.3 Et1/0 FF RATE 100K
```

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

**Table 36: show ip rsvp aggregation ip endpoints detail Field Descriptions**

Field	Description
Role	The router's function; values are aggregator or deaggregator.
DSCP	DSCP value.
Aggregator	IP address of the aggregator.

Field	Description
Deaggregator	IP address of the deaggregator.
State	<p>Status of the reservation. Each aggregate reservation can be in one of the following states:</p> <ul style="list-style-type: none"> <li>• <b>PATH_WAIT</b>--Valid at the deaggregator only. The aggregate reservation at the deaggregator enters this state after the deaggregator has sent a <b>PATHERROR</b> message requesting a new aggregate needed.</li> <li>• <b>RESV_WAIT</b>--Valid at the aggregator only. The aggregate reservation at the aggregator enters this state after the aggregator has sent a <b>PATH</b> message for the aggregate reservation.</li> <li>• <b>RESVCONF_WAIT</b>--Valid at the deaggregator only. The aggregate reservation at the deaggregator enters this state after the deaggregator has sent a <b>RESV</b> message for the aggregate reservation.</li> <li>• <b>ESTABLISHED</b>--Valid at both the aggregator and the deaggregator. The aggregator enters this state after a <b>RESVCONF</b> message has been sent. The deaggregator enters this state after it receives a <b>RESVCONF</b> message for the aggregate reservation.</li> <li>• <b>SHUT_DELAY</b>--Valid at both the aggregator and the deaggregator. The aggregator and the deaggregator enter this state after the last end-to-end (E2E) reservation has been removed.</li> </ul>
Rate	Allocated bandwidth in bits per second (BPS).
Used	Amount of bandwidth used in bits per second (BPS).
QBM Pool ID	The quality of service (QoS) bandwidth manager (QBM) ID for the reservation.
Aggregate Reservation for the following E2E Flows	<p>Information for the reservation:</p> <p><b>PSB</b>--path state block. Contains data used for forwarding <b>PATH</b> messages downstream;</p> <p><b>RSB</b>--reservation state block. Contains data for the incoming <b>RESV</b> message.</p> <p><b>Reqs</b>--requests. Contain data required to forward a <b>RESV</b> message upstream to the node that sent the <b>PATH</b> message.</p>

Field	Description
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. Code indicates IP protocol such as TCP or User Datagram Protocol (UDP).
DPort	Destination port number.
Sport	Source port number.
Prev Hop or Next Hop	IP address of the previous or next hop.
I/F	Interface of the previous or next hop.
Fi	Filter (Wildcard Filter, Shared-Explicit, or Fixed-Filter).
Serv	Service (RATE or LOAD).
BPS	Bandwidth used by the aggregate reservation in bits per second (BPS).

**Related Commands**

Command	Description
<b>ip rsvp aggregation ip</b>	Enables RSVP aggregation on a router.

# show ip rsvp atm-peak-rate-limit

To display the current peak rate limit set for an interface or for all interfaces, if any, use the **showiprsvpatm-peak-rate-limit** command in EXEC mode.

**show ip rsvp atm-peak-rate-limit** [*interface-type interface-number*]

## Syntax Description

<i>interface-type interface-number</i>	(Optional) Interface type and interface number.
--	---

## Command Modes

EXEC

## Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

## Usage Guidelines

The **showiprsvpatm-peak-rate-limit** command displays the configured peak rate using the following notations for brevity:

- Kilobytes is shown as K bytes; for example, 1200 kilobytes is displayed as 1200K bytes.
- 1000 kilobytes is displayed as 1M bytes.

If no interface name is specified, configured peak rates for all Resource Reservation Protocol (RSVP)-enabled interfaces are displayed.

## Examples

The following example depicts results of the **showiprsvpatm-peak-rate-limit** command, presuming that the ATM subinterface 2/0/0.1 was configured with a reservation peak rate limit of 100 KB using the **iprsvpatm-peak-rate-limit** command.

The following is sample output from the **showiprsvpatm-peak-rate-limit** command using the *interface-type interface-number* arguments:

```
Router# show ip rsvp atm-peak-rate-limit atm2/0/0.1
RSVP: Peak rate limit for ATM2/0/0.1 is 100K bytes
```

The following samples show output from the **showiprsvpatm-peak-rate-limit** command when no interface name is given:

```
Router# show ip rsvp atm-peak-rate-limit
```

```
Interface name      Peak rate limit
Ethernet0/1/1      not set
ATM2/0/0           not set
```

```
ATM2/0/0.1          100K
Router# show ip rsvp atm-peak-rate-limit
Interface name      Peak rate limit
Ethernet0/1         not set
ATM2/1/0            1M
ATM2/1/0.10         not set
ATM2/1/0.11         not set
ATM2/1/0.12         not set
```

**Related Commands**

Command	Description
<b>ip rsvp atm-peak-rate-limit</b>	Sets a limit on the peak cell rate of reservations for all newly created RSVP SVCs established on the current interface or any of its subinterfaces.

# show ip rsvp authentication

To display the security associations that Resource Reservation Protocol (RSVP) has established with other RSVP neighbors, use the show **iprsvpauthentication** command in user EXEC or privileged EXEC mode.

**show ip rsvp authentication** [**detail**] [**from** {*ip-address*| *hostname*}] [**to** {*ip-address*| *hostname*}]

## Syntax Description

<b>detail</b>	(Optional) Displays additional information about RSVP security associations.
<b>from</b>	(Optional) Specifies the starting point of the security associations.
<b>to</b>	(Optional) Specifies the ending point of the security associations.
<b>ip-address</b>	(Optional) Information about a neighbor with a specified IP address.
<b>hostname</b>	(Optional) Information about a particular host.

## Command Modes

User EXEC (<) Privileged EXEC (#)

## Command History

Release	Modification
12.2(15)T	This command was introduced.
12.0(29)S	The optional <b>from</b> and <b>to</b> keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

## Usage Guidelines

Use the show ip rsvp authentication command to display the security associations that RSVP has established with other RSVP neighbors. You can display all security associations or specify an IP address or hostname of a particular RSVP neighbor, which restricts the size of the display.

The difference between the *ip-address* and *hostname* arguments is whether you specify the neighbor by its IP address or by its name.

**Examples**

The following is sample output from the **show ip rsvp authentication** command:

```
Router# show ip rsvp authentication
Codes: S - static, D - dynamic, N - neighbor, I -interface, C - chain
From      To      I/F      Mode   Key-Source Key-ID      Code
192.168.102.1 192.168.104.3 Et2/2    Send   RSVPKey    1          DNC
192.168.104.1 192.168.104.3 Et2/2    Send   RSVPKey    1          DNC
192.168.104.1 192.168.104.3 AT1/0.1  Send   RSVPKey    1          DNC
192.168.106.1 192.168.104.3 AT1/0.1  Send   RSVPKey    1          DNC
192.168.106.1 192.168.106.2 AT1/0.1  Send   RSVPKey    1          DNC
192.168.106.2 192.168.104.1 AT1/0.1  Receive RSVPKey    1          DNC
192.168.106.2 192.168.106.1 AT1/0.1  Receive RSVPKey    1          DNC
```

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

**Table 37: show ip rsvp authentication Field Descriptions**

Field	Description
Codes	Keys can be either static (manually configured) or dynamic (created from a per-ACL key or obtained from a key management server such as Kerberos). Cisco IOS software does not currently support dynamic keys from key management servers. If the field contains the string per-neighbor, it means the security association is using a per-neighbor key; if the field contains the string per-interface, it means the security association is using a per-interface key. If the field contains the string chain, it means the key for the security association comes from the key chain specified in the Key Source.
From	Starting point of the security association.
To	Ending point of the security association.
I/F	Name and number of the interface over which the security association is being maintained.
Mode	Separate associations maintained for sending and receiving RSVP messages for a specific RSVP neighbor. Possible values are <b>Send</b> or <b>Receive</b> .
Key-Source	Indicates where the key was configured.

Field	Description
Key-ID	<p>A string which, along with the IP address, uniquely identifies a security association. The key ID is automatically generated in Cisco IOS software by using the per-interface <b>iprsvpauthenticationkey</b> command, but it is configured in Cisco IOS software when using key chains for per-neighbor or per-interface RSVP keys. The key ID may be configurable on other RSVP platforms. A key ID is provided in every RSVP authenticated message initiated by a sender and is stored by every RSVP receiver.</p> <p><b>Note</b> <b>Key Expired</b> in this field means that all possible keys used for this neighbor have expired.</p>
Code	Indicates the type of key ID used.

The following is sample output from the **showiprsvpauthentication** detail command:

```

Router# show ip rsvp authentication detail
From:                192.168.102.1
To:                  192.168.104.3
Neighbor:            192.168.102.2
Interface:           Ethernet2/2
Mode:                Send
Key ID:              1
Key ACL:             R2 (populated)
Key Source:          RSVPKey (enabled)
Key Type:            Dynamic per-neighbor chain
Handle:              01000411
Hash Type:           MD5
Lifetime:            00:30:00
Expires:             00:17:08
Challenge:           Supported
Window size:        1
Last seq # sent:    14167519095569779135
From:                192.168.104.1
To:                  192.168.104.3
Neighbor:            192.168.102.2
Interface:           Ethernet2/2
Mode:                Send
Key ID:              1
Key ACL:             R2 (populated)
Key Source:          RSVPKey (enabled)
Key Type:            Dynamic per-neighbor chain
Handle:              0400040F
Hash Type:           MD5
Lifetime:            00:30:00
Expires:             00:22:06
Challenge:           Supported
Window size:        1
Last seq # sent:    14167520384059965440
From:                192.168.104.1
To:                  192.168.104.3
Neighbor:            192.168.106.2
Interface:           ATM1/0.1
Mode:                Send
Key ID:              1
Key ACL:             R3 (populated)
Key Source:          RSVPKey (enabled)

```

```

Key Type:                Dynamic per-neighbor chain
Handle:                  02000404
Hash Type:               MD5
Lifetime:                00:30:00
Expires:                 00:16:37
Challenge:               Supported
Window size:             1
Last seq # sent:        14167518979605659648
From:                    192.168.106.1
To:                      192.168.104.3
Neighbor:                192.168.106.2
Interface:               ATM1/0.1
Mode:                    Send
Key ID:                  1
Key ACL:                 R3 (populated)
Key Source:              RSVPKey (enabled)
Key Type:                Dynamic per-neighbor chain
Handle:                  01000408
Hash Type:               MD5
Lifetime:                00:30:00
Expires:                 00:11:37
Challenge:               Supported
Window size:             1
Last seq # sent:        14167517691115473376
From:                    192.168.106.1
To:                      192.168.106.2
Neighbor:                192.168.106.2
Interface:               ATM1/0.1
Mode:                    Send
Key ID:                  1
Key ACL:                 R3 (populated)
Key Source:              RSVPKey (enabled)
Key Type:                Dynamic per-neighbor chain
Handle:                  8D00040E
Hash Type:               MD5
Lifetime:                00:30:00
Expires:                 00:29:29
Challenge:               Supported
Window size:             1
Last seq # sent:        14167808344437293057
From:                    192.168.106.2
To:                      192.168.104.1
Neighbor:                192.168.106.2
Interface:               ATM1/0.1
Mode:                    Receive
Key ID:                  1
Key ACL:                 R3 (populated)
Key Source:              RSVPKey (enabled)
Key Type:                Dynamic per-neighbor chain
Handle:                  CD00040A
Hash Type:               MD5
Lifetime:                00:30:00
Expires:                 00:29:33
Challenge:               Not configured
Window size:             1
Last seq # rcvd:        14167808280012783626
From:                    192.168.106.2
To:                      192.168.106.1
Neighbor:                192.168.106.2
Interface:               ATM1/0.1
Mode:                    Receive
Key ID:                  1
Key ACL:                 R3 (populated)
Key Source:              RSVPKey (enabled)
Key Type:                Dynamic per-neighbor chain
Handle:                  C0000412
Hash Type:               MD5
Lifetime:                00:30:00
Expires:                 00:29:33
Challenge:               Not configured
Window size:             1
Last seq # rcvd:        14167808280012783619

```

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

**Table 38: show ip rsvp authentication detail Field Descriptions**

Field	Description
From	Starting point of the security association.
To	Ending point of the security association.
Neighbor	IP address of the RSVP neighbor with which the security association is being maintained.
Interface	Name and number of the interface over which the security association is being maintained.
Mode	Separate associations maintained for sending and receiving RSVP messages for a specific RSVP neighbor. Possible values are Send or Receive.
Key ID	<p>A string which, along with the IP address, uniquely identifies a security association. The key ID is automatically generated in Cisco IOS software by using the per-interface <b>iprsvpauthenticationkey</b> command, but it is configured in Cisco IOS software when using key chains for per-neighbor or per-interface RSVP keys. The key ID may be configurable on other RSVP platforms. A key ID is provided in every RSVP authenticated message initiated by a sender and is stored by every RSVP receiver.</p> <p><b>Note</b> <b>Key Expired</b> in this field means that all possible keys used for this neighbor have expired.</p>
Key ACL	<p>For key types that say dynamic and chain, this field indicates which ACL matched that neighbor, and therefore, which key chain to use. Possible values include:</p> <ul style="list-style-type: none"> <li>• <b>populated</b> = ACL has entries in it.</li> <li>• <b>removed</b> = ACL has been removed from the configuration.</li> </ul>
Key Source	Indicates where the key was configured and whether it is enabled or disabled. For key chains, this indicates the name of the key chain; the Key ID field indicates which key in the chain is currently being used. For per-interface keys, this field contains the name of the interface that was configured with the key.

Field	Description
Key Type	<p>Static (manually configured) or dynamic (created from a per-ACL key or obtained from a key management server such as Kerberos).</p> <p><b>Note</b> Cisco IOS software does not currently support dynamic keys from key management servers.</p>
Handle	Internal database ID assigned to the security association by RSVP for bookkeeping purposes.
Hash Type	Type of secure hash algorithm being used with that neighbor.
Lifetime	<p>Maximum amount of time (in hours, minutes, and seconds) that can elapse before a security association is expired.</p> <p><b>Note</b> This is not how long a key is valid; to obtain duration times for keys, use the <b>showkeychain</b> command.</p>
Expires	<p>Amount of time remaining (in days, hours, minutes, and seconds) before the security association expires.</p> <p><b>Note</b> This is not when the current key expires; to obtain expiration times for keys, use the <b>showkeychain</b> command.</p>
Challenge	For receive-type security associations, possible values are <b>NotConfigured</b> , <b>Completed</b> , <b>InProgress</b> , and <b>Failed</b> . For send-type security associations, the value is <b>Supported</b> . Cisco IOS software can always respond to challenges; however, there may be non-Cisco neighbors that do not implement challenges.
Window size	Indicates the size of the window for receive-type security associations and the maximum number of authenticated RSVP messages that can be received out-of-order before a replay attack is to be suspected.
Last seq # sent	Displayed only for send-type security associations. It indicates the sequence number used to send the last authenticated message to the RSVP neighbor. Use this information to troubleshoot certain types of authentication problems.

Field	Description
Last valid seq # rcvd	Displayed only for receive-type security associations. It indicates the authentication sequence number of the last valid RSVP message received from the neighbor. By default, it shows only one sequence number. However, if you use the ip rsvp authentication window-size command to increase the authentication window size to n, then the last n valid received sequence numbers are displayed. Use this information to troubleshoot certain types of authentication problems.

**Related Commands**

Command	Description
<b>clear ip rsvp authentication</b>	Eliminates RSVP security associations before their lifetimes expire.

# show ip rsvp counters

To display the number of Resource Reservation Protocol (RSVP) messages that were sent and received on each interface, use the **showiprsvpcounters** command in user EXEC or privileged EXEC mode.

```
show ip rsvp counters [authentication] [interface type number | neighbor [vrf {*| vrf-name}] | state teardown]
summary]
```

## Syntax Description

<b>authentication</b>	(Optional) Displays a list of RSVP authentication counters.
<b>interface</b> <i>type number</i>	(Optional) Displays the number of RSVP messages sent and received for the specified interface name.
<b>neighbor</b>	(Optional) Displays the number of RSVP messages sent and received by the specified neighbor.
vrf *	(Optional) Displays all the configured virtual routing and forwarding (VRF) instances.
<b>vrf</b> <i>vrf-name</i>	(Optional) Displays the name of a specified VRF.
<b>state teardown</b>	(Optional) Displays the number of RSVP message states and the reasons for teardown.
<b>summary</b>	(Optional) Displays the cumulative number of RSVP messages sent and received by the router over all interfaces.

## Command Default

If you enter the **showiprsvpcounters** command without an optional keyword, the command displays the number of RSVP messages that were sent and received for each interface on which RSVP is configured.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(13)T	The <b>neighbor</b> keyword was added, and the command was integrated into Cisco IOS Release 12.2(13)T.

Release	Modification
12.2(15)T	The command output was modified to show the errors counter incrementing whenever an RSVP message is received on an interface with RSVP authentication enabled, but the authentication checks failed on that message.
12.2(11)S	This command was integrated into Cisco IOS Release 12.2(11)S.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(29)S	The <b>authentication</b> keyword was added, and the command output was modified to include hello and message queues information.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
15.0(1)M	This command was modified. The <b>vrf</b> and <b>*keywords</b> and the <i>vrf-name</i> argument were added.

## Examples

### Examples

The following example shows the values for the number of RSVP messages of each type that were sent and received by the router over all interfaces, including the hello and message queues information:

```
Router# show ip rsvp counters summary
All Interfaces          Recv      Xmit
  Path                 110       15    Resv                50       28
  PathError            0         0    ResvError           0         0
  PathTear             0         0    ResvTear            0         0
  ResvConf             0         0    RTearConf           0         0
  Ack                  0         0    Srefresh            0         0
  Hello                5555      5554  IntegrityChalle     0         0
  IntegrityRespon      0         0    DSBM_WILLING        0         0
  I_AM_DSBM            0         0
  Unknown              0         0    Errors              0         0
Recv Msg Queues        Current   Max
  RSVP                  0         2
  Hello (per-I/F)      0         1
  Awaiting Authentication 0         0
```

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

**Table 39: show ip rsvp counters summary Field Descriptions**

Field	Description
All Interfaces	Types of messages displayed for all interfaces. <b>Note</b> Hello is a summary of graceful restart, reroute (hello state timer), and Fast Reroute messages.
Recv	Number of messages received on the specified interface or on all interfaces.
Xmit	Number of messages transmitted from the specified interface or from all interfaces.
Recv Msg Queues	Queues for received messages for RSVP, hello per interface, and awaiting authentication. <ul style="list-style-type: none"> <li>• Current--Number of messages queued.</li> <li>• Max--Maximum number of messages ever queued.</li> </ul>

**Examples**

The following example shows the values for the number of RSVP messages for a specified neighbor with a VRF named myvrf:

```
Router# show ip rsvp counters neighbor vrf myvrf
VRF: myvrf
Neighbor: 10.10.15.13
  Rate-Limiting:
    Output queue overflow, number of dropped RSVP messages: 0
  Refresh-Reduction:
    Number of RSVP messages received out of order: 0
    Number of retransmitted RSVP messages: 0
```

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

**Table 40: show ip rsvp counters neighbor vrf Field Descriptions**

Field	Description
VRF	Name of the VRF.
Neighbor	IP address of the neighbor.
Rate-Limiting	The rate-limiting parameters in effect are as follows: <ul style="list-style-type: none"> <li>• Output queue overflow, number of dropped RVSP messages--Number of messages dropped by the neighbor when the queue overflowed.</li> </ul>

Field	Description
Refresh-Reduction	<p>The refresh-reduction parameters in effect are as follows:</p> <ul style="list-style-type: none"><li>• Number of RSVP messages received out of order--Messages that were dropped because they were out of sequential order.</li><li>• Number of retransmitted RSVP messages--Number of messages retransmitted to the neighbor.</li></ul>

**Related Commands**

Command	Description
<code>clear ip rsvp counters</code>	Clears (sets to zero) all IP RSVP counters that are being maintained.

## show ip rsvp counters state teardown

To display counters for Resource Reservation Protocol (RSVP) events that caused a state to be torn down, use the **showiprsvpcountersstateteardown** command in user EXEC or privileged EXEC mode.

**show ip rsvp counters state teardown**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC Privileged EXEC

Command History	Release	Modification
	12.0(29)S	This command was introduced.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
	12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

**Usage Guidelines** Use the **showiprsvpcountersstateteardown** command when a label-switched path (LSP) is down. If graceful restart triggered the state teardown, the numbers in the Path, Resv-In, and Resv-Out columns in the “Examples” section are greater than 0.

**Examples** The following is sample output from the **showiprsvpcountersstateteardown** command:

```
Router# show ip rsvp counters state teardown
States
Reason for Teardown                               State torn down
                                                    Path   Resv-In  Resv-Out
PathTear arrival                                 0       0       0
ResvTear arrival                                 0       0       0
Local application requested tear                 0       0       0
Output or Input I/F went down                   0       0       0
Missed refreshes                                0       0       0
Preemption                                       0       0       0
Backup tunnel failed for FRR Active LSP          0       0       0
Reroutability changed for FRR Active LSP         0       0       0
Hello RR Client (HST) requested tear             0       0       0
Graceful Restart (GR) requested tear             0       0       0
Downstream neighbor SSO-restarting               0       0       0
Resource unavailable                             0       0       0
Policy rejection                                 0       0       0
Policy server sync failed                        0       0       0
Traffic control error                            0       0       0
Error in received message                        0       0       0
Non RSVP HOP upstream, TE LSP                    0       0       0
Other                                             0       0       0
```

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

**Table 41: show ip rsvp counters state teardown Field Descriptions**

Field	Description
States	RSVP state, including path state block (PSB) and reservation state block (RSB) information.
Reason for Teardown	Event triggering the teardown.

**Related Commands**

Command	Description
<b>clear ip rsvp counters</b>	Clears (sets to zero) the IP RSVP counters that are being maintained.

## show ip rsvp fast bw-protect

To display information about whether backup bandwidth protection is enabled and the status of backup tunnels that may be used to provide that protection, use the **show ip rsvp fast bw-protect** command in user EXEC or privileged EXEC mode.

```
show ip rsvp fast bw-protect [detail] [filter [destination ip-address| hostname] [dst-port port-number]
[source ip-address| hostname] [src-port port-number]]
```

### Syntax Description

<b>detail</b>	(Optional) Specifies additional receiver information.
<b>filter</b>	(Optional) Specifies a subset of the receivers to display .
<b>destination</b> <i>ip-address</i>	(Optional) Specifies the destination IP address of the receiver.
<i>hostname</i>	(Optional) Specifies the hostname of the receiver.
<b>dst-port</b> <i>port-number</i>	(Optional) Specifies the destination port number. Valid destination port numbers must be in the range from 0 to 65535.
<b>source</b> <i>ip-address</i>	(Optional) Specifies the source IP address of the receiver.
<b>src-port</b> <i>port-number</i>	(Optional) Specifies the source port number. Valid source port numbers must be in the range from 0 to 65535.

### Command Default

The backup bandwidth protection and backup tunnel status information is not displayed.

### Command Modes

User EXEC (>) Privileged EXEC (#)

### Command History

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T

## Examples

The following is sample output from the **showiprsvpfastbw-protect** command:

```
Router# show ip rsvp fast bw-protect
```

```

Primary      Protect  BW      Backup
Tunnel       I/F      BPS:Type Tunnel:Label  State  BW-P  Type
-----
PRAB-72-5_t500 PO2/0    500K:S   Tu501:19    Ready  ON    Nhop
PRAB-72-5_t601 PO2/0    103K:S   Tu501:20    Ready  OFF   Nhop
PRAB-72-5_t602 PO2/0    70K:S    Tu501:21    Ready  ON    Nhop
PRAB-72-5_t603 PO2/0    99K:S    Tu501:22    Ready  ON    Nhop
PRAB-72-5_t604 PO2/0    100K:S   Tu501:23    Ready  OFF   Nhop
PRAB-72-5_t605 PO2/0    101K:S   Tu501:24    Ready  OFF   Nhop

```

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

**Table 42: show ip rsvp fast bw-protect Field Descriptions**

Field	Description
Primary Tunnel	Identification of the tunnel being protected.
Protect I/F	Interface name.
BW BPS:Type	Bandwidth, in bits per second, and type of bandwidth. Possible values are the following: <ul style="list-style-type: none"> <li>• S--Subpool</li> <li>• G--Global pool</li> </ul>
Backup Tunnel:Label	Identification of the backup tunnel.
State	Status of backup tunnel. Valid values are the following: <ul style="list-style-type: none"> <li>• Ready--Data is passing through the primary tunnel, but the backup tunnel is ready to take over if the primary tunnel goes down.</li> <li>• Active--The primary tunnel is down, so the backup tunnel is used for traffic.</li> <li>• None--There is no backup tunnel.</li> </ul>
BW-P	Status of backup bandwidth protection. Possible values are ON and OFF.

Field	Description
Type	Type of backup tunnel. Possible values are the following: <ul style="list-style-type: none"><li>• Nhop--Next hop</li><li>• NNHOP--Next-next hop</li></ul>

**Related Commands**

Command	Description
<b>tunnel mpls traffic-eng fast-reroute bw-protect</b>	Enables an MPLS TE tunnel to use an established backup tunnel in the event of a link or node failure.

# show ip rsvp fast detail

To display specific information for Resource Reservation Protocol (RSVP) categories, use the **show ip rsvp fast detail** command in user EXEC or privileged EXEC mode.

**show ip rsvp fast detail** [**filter** [**destination** *ip-address*| *hostname*]] [**dst-port** *port-number*] [**source** *ip-address*| *hostname*] [**src-port** *port-number*]

## Syntax Description

<b>filter</b>	(Optional) Specifies a subset of the receivers to display .
<b>destination</b> <i>ip-address</i>	(Optional) Specifies the destination IP address of the receiver.
<i>hostname</i>	(Optional) Specifies the hostname of the receiver.
<b>dst-port</b> <i>port-number</i>	(Optional) Specifies the destination port number. Valid destination port numbers must be in the range from 0 to 65535.
<b>source</b> <i>ip-address</i>	(Optional) Specifies the source IP address of the receiver.
<b>src-port</b> <i>port-number</i>	(Optional) Specifies the source port number. Valid source port numbers must be in the range from 0 to 65535.

## Command Default

Specific information for RSVP categories is not displayed.

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

Release	Modification
12.0(24)S	This command was introduced.
12.0(29)S	Bandwidth Prot desired was added in the Flag field of the command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

**Examples**

The following is sample output from the **show ip rsvp fast detail** command:

```
Router# show ip rsvp fast detail

PATH:
Tun Dest: 10.0.0.7 Tun ID: 500 Ext Tun ID: 10.0.0.5
Tun Sender: 10.0.0.5 LSP ID: 8
Path refreshes:
  sent: to NHOP 10.5.6.6 on POS2/0
Session Attr:
  Setup Prio: 7, Holding Prio: 7
  Flags: Local Prot desired, Label Recording, SE Style, Bandwidth Prot desired
  Session Name: PRAB-72-5_t500
ERO: (incoming)
  10.0.0.5 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.5.6 (Strict IPv4 Prefix, 8 bytes, /32)
  10.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
ERO: (outgoing)
  10.5.6.6 (Strict IPv4 Prefix, 8 bytes, /32)
  10.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
Traffic params - Rate: 500K bits/sec, Max. burst: 1K bytes
Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
Fast-Reroute Backup info:
  Inbound FRR: Not active
  Outbound FRR: Ready -- backup tunnel selected
  Backup Tunnel: Tu501 (label 19)
  Bkup Sender Template:
    Tun Sender: 10.5.6.5 LSP ID: 8
  Bkup FilerSpec:
    Tun Sender: 10.5.6.5, LSP ID: 8
Path ID handle: 04000405.
Incoming policy: Accepted. Policy source(s): MPLS/TE
Status: Proxied
Output on POS2/0. Policy status: Forwarding. Handle: 02000406
```

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

**Table 43: show ip rsvp fast detail Field Descriptions**

Field	Description
Tun Dest	IP address of the receiver.
Tun ID	Tunnel identification number.
Ext Tun ID	Extended tunnel identification number.
Tun Sender	IP address of the sender.
LSP ID	Label-switched path identification number.
Setup Prio	Setup priority.
Holding Prio	Holding priority.
Flags	Backup bandwidth protection has been configured for the label-switched path (LSP).

Field	Description
Session Name	Name of the session.
ERO (incoming)	EXPLICIT_ROUTE object of incoming path messages.
ERO (outgoing)	EXPLICIT_ROUTE object of outgoing path messages.
Traffic params Rate	Average rate, in bits per second.
Max. burst	Maximum burst size, in bytes.
Min Policed Unit	Minimum policed units, in bytes.
Max Pkt Size	Maximum packet size, in bytes.
Inbound FRR	Status of inbound Fast Reroute (FRR) backup tunnel. If this node is downstream from a rerouted LSP (for example, at a merge point for this LSP), the state is Active.
Outbound FRR	Status of outbound FRR backup tunnel. If this node is a point of local repair (PLR) for an LSP, there are three possible states: <ul style="list-style-type: none"> <li>• Active--This LSP is actively using its backup tunnel, presumably because there has been a downstream failure.</li> <li>• No Backup--This LSP does not have local (Fast Reroute) protection. No backup tunnel has been selected for it to use in case of a failure.</li> <li>• Ready--This LSP is ready to use a backup tunnel in case of a downstream link or node failure. A backup tunnel has been selected for it to use.</li> </ul>
Backup Tunnel	If the Outbound FRR state is Ready or Active, this field indicates the following: <ul style="list-style-type: none"> <li>• Which backup tunnel has been selected for this LSP to use in case of a failure.</li> <li>• The inbound label that will be prepended to the LSP's data packets for acceptance at the backup tunnel tail (the merge point).</li> </ul>

Field	Description
Bkup Sender Template	If the Outbound FRR state is Ready or Active, SENDER_TEMPLATE and FILTERSPEC objects are shown. These objects will be used in RSVP messages sent by the backup tunnel if or when the LSP starts actively using the backup tunnel. They differ from the original (prefailure) objects only in that the node (the PLR) substitutes its own IP address for that of the original sender. For example, path and pathTear messages will contain the new SENDER_TEMPLATE. Resv and resvTear messages will contain the new FILTERSPEC object. If this LSP begins actively using the backup tunnel, the display changes.
Bkup FilerSpec	If the Outbound FRR state is Ready or Active, SENDER_TEMPLATE and FILTERSPEC objects are shown. These objects will be used in RSVP messages sent by the backup tunnel if or when the LSP starts actively using the backup tunnel. They differ from the original (prefailure) objects only in that the node (the PLR) substitutes its own IP address for that of the original sender. For example, path and pathTear messages will contain the new SENDER_TEMPLATE. Resv and resvTear messages will contain the new FILTERSPEC object. If this LSP begins actively using the backup tunnel, the display changes.
Path ID handle	Protection Switch Byte (PSB) identifier.
Incoming policy	Policy decision of the LSP. If RSVP policy was not granted for the incoming path message for the tunnel, the LSP does not come up. Accepted is displayed.
Policy source(s)	For FRR LSPs, this value always is MPLS/TE for the policy source.
Status	<p>For FRR LSPs, valid values are as follows:</p> <ul style="list-style-type: none"> <li>• Proxied--Headend routers.</li> <li>• Proxied Terminated--Tailend routers.</li> </ul> <p>For midpoint routers, the field always is blank.</p>

**Related Commands**

Command	Description
<b>mpls traffic-eng fast-reroute backup-prot-preemption</b>	Changes the backup protection preemption algorithm to minimize the amount of bandwidth that is wasted.

## show ip rsvp fast-reroute

To display information about fast reroutable primary tunnels and their corresponding backup tunnels that provide protection, use the **show ip rsvp fast-reroute** command in user EXEC or privileged EXEC mode.

```
show ip rsvp fast-reroute [filter [session-type {session-type-number} all]]
```

### Syntax Description

<b>filter</b>	(Optional) Specifies a subset of the tunnel to display.
<b>session-type</b> <i>session-type-number</i>	(Optional) Specifies the type of tunnels to display. Valid values are: <ul style="list-style-type: none"> <li>• <b>7</b> for IPv4 point-to-point (P2P) traffic engineering (TE) label switched path (LSP) tunnel sessions.</li> <li>• <b>13</b> for IPv4 point-to-multipoint (P2MP) TE LSP tunnel sessions.</li> </ul>
<b>session-type all</b>	(Optional) Specifies all types of tunnel sessions.

### Command Default

If no arguments are specified, the display information about all fast reroutable primary tunnels is displayed.

### Command Modes

User EXEC (>) Privileged EXEC (#)

### Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SRE	This command was modified. The <b>filter</b> keyword was added to display tunnel information categorized by point-to-point and point-to-multipoint. The output was updated to display Multiprotocol Label Switching (MPLS) TE P2MP information.
15.0(1)M	This command was modified. Support for classic IP RSVP (session type 1) was removed.

**Examples**

The following is sample output of fast reroutable primary tunnels and their corresponding backup tunnels that provide protection:

```
Router# show ip rsvp fast-reroute
Primary          Protect BW      Backup
Tunnel          I/F      BPS:Type      Tunnel:Label  State  Level  Type
-----
GSR1---R2---_t65336  PO1/0   0:G          Tu1002:0     Ready any-unl Nhop
GSR1---R2---_t65338  PO4/0   0:G          Tu1004:0     Ready any-unl Nhop
```

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

**Table 44: show ip rsvp fast-reroute Field Descriptions**

Field	Description
Primary Tunnel	Hostname and tunnel ID.
Protect I/F	Interface that is being protected.
BW BPS:Type	Bandwidth, in bits per second, and the pool from which the bandwidth comes. Valid values are G, global pool, S, and subpool.
Backup Tunnel:Label	Backup tunnel ID and label.
State	Status of protection. Valid values are Ready, Active, and None.
Level	Level of bandwidth. Valid values are any and unl (unlimited).
Type	Type of backup tunnel: Nhop (next hop) or NNhop (next-next hop).

The following example shows fast reroutable primary tunnels and their corresponding backup tunnels. The information is organized by P2P LSPs and P2MP sub-LSPs. The following example shows that Tunnel 22 has six sub-LSPs, three that are protected on Ethernet interface 0/0, and three that are not protected on Ethernet interface 0/1:

```
Router# show ip rsvp fast-reroute
P2P
Protected LSP      Protect BW      Backup
                  I/F      BPS:Type      Tunnel:Label  State  Level  Type
-----
R201_t1           Et0/1   500K:G        Tu777:16     Ready any-lim Nhop
P2MP
Protected Sub-LSP      Protect BW      Backup
src_lspid[subid]->dst_tunid  I/F      BPS:Type      Tunnel:Label  State
-----
10.1.1.201_1[1]->10.1.1.203_22  Et0/0   500K:G        Tu666:20     Ready
10.1.1.201_1[2]->10.1.1.206_22  Et0/0   500K:G        Tu666:20     Ready
10.1.1.201_1[3]->10.1.1.213_22  Et0/0   500K:G        Tu666:20     Ready
10.1.1.201_1[4]->10.1.1.214_22  Et0/1   500K:G        None          None
10.1.1.201_1[5]->10.1.1.216_22  Et0/1   500K:G        None          None
10.1.1.201_1[6]->10.1.1.217_22  Et0/1   500K:G        None          None
```

The following example displays information about fast reroutable primary tunnels and their corresponding backup tunnels for Cisco IOS Release 12.4(24)T and earlier releases. The output is organized by session type.

```
Router# show ip rsvp fast-reroute filter session-type all

Session Type 1 (rsvp)
P2P
Protected LSP          Protect BW      Backup
I/F      BPS:Type  Tunnel:Label  State  Level  Type
-----
Session Type 7 (te-p2p-lsp)
P2P
Protected LSP          Protect BW      Backup
I/F      BPS:Type  Tunnel:Label  State  Level  Type
-----
R201_t1                Et0/1   500K:G      Tu777:16   Ready  any-lim Nhop
Session Type 13 (te-p2mp-lsp)
P2MP
Protected Sub-LSP
src_lspid[subid]->dst_tunid          Protect BW      Backup
I/F      BPS:Type  Tunnel:Label  State
-----
10.1.1.201_1[1]->10.1.1.203_22      Et0/0   500K:G      Tu666:20   Ready
10.1.1.201_1[2]->10.1.1.206_22      Et0/0   500K:G      Tu666:20   Ready
10.1.1.201_1[3]->10.1.1.213_22      Et0/0   500K:G      Tu666:20   Ready
10.1.1.201_1[4]->10.1.1.214_22      Et0/1   500K:G      None       None
10.1.1.201_1[5]->10.1.1.216_22      Et0/1   500K:G      None       None
10.1.1.201_1[6]->10.1.1.217_22      Et0/1   500K:G      None       None
```

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

**Table 45: show ip rsvp fast-reroute Point-to-Multipoint Field Descriptions**

Field	Description
Protected LSP	LSP being protected and the tunnel ID.
Protected Sub-LSP src_lspid[subid]->dst_tunid	The source and destination address of the sub-LSP being protected. The P2MP ID is appended to the source address. The tunnel ID is appended to the destination address.

The following example displays information about fast reroutable primary tunnels and their corresponding backup tunnels that provide protection for Cisco IOS Release 15.0(1)M and later releases.

```
Router# show ip rsvp fast-reroute filter session-type all

Session Type 7 (te-p2p-lsp)
P2P
Protected LSP          Protect BW      Backup
I/F      BPS:Type  Tunnel:Label  State  Level  Type
-----
p2mp-2_t12            Se3/0   500K:G      Tu700:0    Ready  any-unl Nhop
p2mp-2_t13            Se3/0   500K:G      Tu700:0    Ready  any-unl Nhop
Session Type 13 (te-p2mp-lsp)
P2MP
*Protected Sub-LSP
src_lspid[subid]->dst_tunid          Protect BW      Backup
I/F      BPS:Type  Tunnel:Label  State
-----
10.2.0.1_12[1]->10.1.0.1_1          Se5/0   1M:G        None       None
10.2.0.1_12[3]->10.2.3.3_1          Se3/0   1M:G        Tu700:16   Ready
10.2.0.1_12[5]->10.3.0.1_1          Se3/0   1M:G        Tu700:16   Ready
10.2.0.1_12[6]->10.3.4.3_1          Se3/0   1M:G        Tu700:16   Ready
10.2.0.1_12[8]->10.2.5.3_1          Se6/0   1M:G        Tu100:17   Ready
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>mpls traffic-eng auto-tunnel primary config</b>	Enables IP processing without an explicit address.
<b>mpls traffic-eng auto-tunnel primary config mpls ip</b>	Enables LDP on primary autotunnels.
<b>mpls traffic-eng auto-tunnel primary onehop</b>	Automatically creates primary tunnels to all next hops.
<b>mpls traffic-eng auto-tunnel primary timers</b>	Configures how many seconds after a failure primary autotunnels are removed.
<b>mpls traffic-eng auto-tunnel primary tunnel-num</b>	Configures the range of tunnel interface numbers for primary autotunnels.

## show ip rsvp fast-reroute bw-protect

To display information about whether backup bandwidth protection is enabled and the status of backup tunnels that may be used to provide that protection, use the **show ip rsvp fast-reroute bw-protect** command in user EXEC or privileged EXEC mode.

**show ip rsvp fast-reroute bw-protect** [**detail**] [**filter** [**session-type** {*session-type-number*| **all**}] [**destination** *ip-address*| *hostname*] [**dst-port** *port-number*] [**source** *ip-address*| *hostname*] [**src-port** *port-number*]]

### Syntax Description

<b>detail</b>	(Optional) Specifies additional receiver information.
<b>filter</b>	(Optional) Specifies a subset of the receivers to display .
<b>session-type</b> <i>session-type-number</i>	(Optional) Specifies the type of Resource Reservation Protocol (RSVP) sessions to display. Valid values are: <ul style="list-style-type: none"> <li>• <b>1</b> for IPv4 sessions</li> <li>• <b>7</b> for IPv4 point-to-point traffic engineering (TE) label switched path (LSP) tunnel sessions</li> <li>• <b>13</b> for IPv4 point-to-multipoint TE LSP tunnel sessions</li> </ul>
<b>all</b>	(Optional) Specifies all types of RSVP sessions.
<b>destination</b> <i>ip-address</i>	(Optional) Specifies the destination IP address of the receiver.
<i>hostname</i>	(Optional) Specifies the hostname of the receiver.
<b>dst-port</b> <i>port-number</i>	(Optional) Specifies the destination port number. Valid destination port numbers must be in the range from 0 to 65535.
<b>source</b> <i>ip-address</i>	(Optional) Specifies the source IP address of the receiver.
<b>src-port</b> <i>port-number</i>	(Optional) Specifies the source port number. Valid source port numbers must be in the range from 0 to 65535.

### Command Default

The backup bandwidth protection and backup tunnel status information is not displayed.

**Command Modes**

User EXEC (&gt;) Privileged EXEC (#)

**Command History**

Release	Modification
12.0(29)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SRE	This command was modified. The <b>session-type</b> keyword was added to display specific types of tunnels. The output was modified to display Multiprotocol Label Switching (MPLS) traffic engineering (TE) point-to-multipoint (P2MP) information.

**Examples**

The following is sample output from the **show ip rsvp fast-reroute bw-protect** command:

```
Router# show ip rsvp fast-reroute bw-protect
```

```

Primary      Protect  BW      Backup
Tunnel       I/F      BPS:Type Tunnel:Label  State  BW-P  Type
-----
PRAB-72-5_t500 PO2/0    500K:S  Tu501:19    Ready  ON   Nhop
PRAB-72-5_t601 PO2/0    103K:S  Tu501:20    Ready  OFF  Nhop
PRAB-72-5_t602 PO2/0    70K:S   Tu501:21    Ready  ON   Nhop
PRAB-72-5_t603 PO2/0    99K:S   Tu501:22    Ready  ON   Nhop
PRAB-72-5_t604 PO2/0    100K:S  Tu501:23    Ready  OFF  Nhop
PRAB-72-5_t605 PO2/0    101K:S  Tu501:24    Ready  OFF  Nhop

```

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

**Table 46: show ip rsvp fast-reroute bw-protect Field Descriptions**

Field	Description
Primary Tunnel	Identification of the tunnel being protected.
Protect I/F	Interface name.
BW BPS:Type	Bandwidth, in bits per second, and type of bandwidth. Possible values are the following: <ul style="list-style-type: none"> <li>• S--Subpool</li> <li>• G--Global pool</li> </ul>
Backup Tunnel:Label	Identification of the backup tunnel.

Field	Description
State	Status of backup tunnel. Valid values are the following: <ul style="list-style-type: none"> <li>• Ready--Data is passing through the primary tunnel, but the backup tunnel is ready to take over if the primary tunnel goes down.</li> <li>• Active--The primary tunnel is down, so the backup tunnel is used for traffic.</li> <li>• None--There is no backup tunnel.</li> </ul>
BW-P	Status of backup bandwidth protection. Possible values are ON and OFF.
Type	Type of backup tunnel. Possible values are the following: <ul style="list-style-type: none"> <li>• Nhop--Next hop</li> <li>• NNHOP--Next-next hop</li> </ul>

The following example shows fast reroutable primary tunnels and their corresponding backup tunnels that provide protection. The information is organized by point-to-point (P2P) label switched paths (LSPs) and P2MP sub-LSPs. The following example shows that Tunnel 22 has six sub-LSPs, three that are protected on Ethernet interface 0/0, and three that are not protected on Ethernet interface 0/1:

```
Router# show ip rsvp fast-reroute bw-protect
```

```

P2P
Protected LSP
-----
R201_t1          Et0/1   500K:G   Tu777:16   Ready  ON      Nhop
P2MP
Protected Sub-LSP
src_lspid[subid]->dst_tunid
-----
10.1.1.201_1[1]->10.1.1.203_22      Et0/0   500K:G   Tu666:20   ON
10.1.1.201_1[2]->10.1.1.206_22      Et0/0   500K:G   Tu666:20   ON
10.1.1.201_1[3]->10.1.1.213_22      Et0/0   500K:G   Tu666:20   ON
10.1.1.201_1[4]->10.1.1.214_22      Et0/1   500K:G   None        None
10.1.1.201_1[5]->10.1.1.216_22      Et0/1   500K:G   None        None
10.1.1.201_1[6]->10.1.1.217_22      Et0/1   500K:G   None        None

```

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

**Table 47: show ip rsvp fast-reroute bw-protect Point-to-Multipoint Field Descriptions**

Field	Description
Protected LSP	LSP being protected and the tunnel ID.

Field	Description
Protected Sub-LSP src_lspid[subid]->dst_tunid	The source and destination address of the sub-LSP being protected. The P2MP ID is appended to the source address. The tunnel ID is appended to the destination address.

**Related Commands**

Command	Description
<b>tunnel mpls traffic-eng fast-reroute bw-protect</b>	Enables an MPLS TE tunnel to use an established backup tunnel in the event of a link or node failure.

## show ip rsvp fast-reroute detail

To display specific information for Resource Reservation Protocol (RSVP) categories, use the **show ip rsvp fast-reroute detail** command in user EXEC or privileged EXEC mode.

```
show ip rsvp fast-reroute detail [filter [session-type {session-type-number| all}] [destination ip-address|
hostname] [dst-port port-number] [source ip-address| hostname] [src-port port-number]]
```

### Syntax Description

<b>filter</b>	(Optional) Specifies a subset of the receivers to display .
<b>session-type</b> <i>session-type-number</i>	(Optional) Specifies the type of RSVP sessions to display. Valid values are: <ul style="list-style-type: none"> <li>• <b>1</b> for IPv4 sessions</li> <li>• <b>7</b> for IPv4 point-to-point (P2P) traffic engineering (TE) label switched path (LSP) tunnel sessions</li> <li>• <b>13</b> for IPv4 point-to-multipoint (P2MP) TE LSP tunnel sessions.</li> </ul>
<b>all</b>	(Optional) Specifies all types of RSVP sessions.
<b>destination</b> <i>ip-address</i>	(Optional) Specifies the destination IP address of the receiver.
<i>hostname</i>	(Optional) Specifies the hostname of the receiver.
<b>dst-port</b> <i>port-number</i>	(Optional) Specifies the destination port number. Valid destination port numbers must be in the range from 0 to 65535.
<b>source</b> <i>ip-address</i>	(Optional) Specifies the source IP address of the receiver.
<b>src-port</b> <i>port-number</i>	(Optional) Specifies the source port number. Valid source port numbers must be in the range from 0 to 65535.

### Command Modes

User EXEC (>) Privileged EXEC (#)

**Command History**

Release	Modification
12.0(24)S	This command was introduced.
12.0(29)S	Bandwidth Prot desired was added in the Flag field of the command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SRE	This command was modified. The <b>session-type</b> keyword was added to display specific types of tunnels. The output was modified to display MPLS TE P2MP information.

**Examples**

The following is sample output from the **show ip rsvp fast-reroute detail** command:

```
Router# show ip rsvp fast-reroute detail

PATH:
Tun Dest: 10.0.0.7 Tun ID: 500 Ext Tun ID: 10.0.0.5
Tun Sender: 10.0.0.5 LSP ID: 8
Path refreshes:
  sent: to NHOP 10.5.6.6 on POS2/0
Session Attr:
  Setup Prio: 7, Holding Prio: 7
  Flags: Local Prot desired, Label Recording, SE Style, Bandwidth Prot desired
  Session Name: PRAB-72-5_t500
ERO: (incoming)
  10.0.0.5 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.5.6 (Strict IPv4 Prefix, 8 bytes, /32)
  10.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
ERO: (outgoing)
  10.5.6.6 (Strict IPv4 Prefix, 8 bytes, /32)
  10.6.7.7 (Strict IPv4 Prefix, 8 bytes, /32)
  10.0.0.7 (Strict IPv4 Prefix, 8 bytes, /32)
Traffic params - Rate: 500K bits/sec, Max. burst: 1K bytes
Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
Fast-Reroute Backup info:
  Inbound FRR: Not active
  Outbound FRR: Ready -- backup tunnel selected
  Backup Tunnel: Tu501 (label 19)
  Bkup Sender Template:
  Tun Sender: 10.5.6.5 LSP ID: 8
  Bkup FilerSpec:
  Tun Sender: 10.5.6.5, LSP ID: 8
Path ID handle: 04000405.
Incoming policy: Accepted. Policy source(s): MPLS/TE
Status: Proxied
Output on POS2/0. Policy status: Forwarding. Handle: 02000406
```

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

**Table 48: show ip rsvp fast-reroute detail Field Descriptions**

Field	Description
Tun Dest	IP address of the receiver.

Field	Description
Tun ID	Tunnel identification number.
Ext Tun ID	Extended tunnel identification number.
Tun Sender	IP address of the sender.
LSP ID	Label switched path identification number.
Setup Prio	Setup priority.
Holding Prio	Holding priority.
Flags	Backup bandwidth protection has been configured for the label switched path.
Session Name	Name of the session.
ERO (incoming)	EXPLICIT_ROUTE object of incoming path messages.
ERO (outgoing)	EXPLICIT_ROUTE object of outgoing path messages.
Traffic params Rate	Average rate, in bits per second.
Max. burst	Maximum burst size, in bytes.
Min Policed Unit	Minimum policed units, in bytes.
Max Pkt Size	Maximum packet size, in bytes.
Inbound FRR	Status of inbound Fast Reroute (FRR) backup tunnel. If this node is downstream from a rerouted LSP (for example, at a merge point for this LSP), the state is Active.

Field	Description
Outbound FRR	<p>Status of outbound FRR backup tunnel. If this node is a point of local repair (PLR) for an LSP, there are three possible states:</p> <ul style="list-style-type: none"> <li>• Active--This LSP is actively using its backup tunnel, presumably because there has been a downstream failure.</li> <li>• No Backup--This LSP does not have local (Fast Reroute) protection. No backup tunnel has been selected for it to use in case of a failure.</li> <li>• Ready--This LSP is ready to use a backup tunnel in case of a downstream link or node failure. A backup tunnel has been selected for it to use.</li> </ul>
Backup Tunnel	<p>If the Outbound FRR state is Ready or Active, this field indicates the following:</p> <ul style="list-style-type: none"> <li>• Which backup tunnel has been selected for this LSP to use in case of a failure.</li> <li>• The inbound label that will be prepended to the LSP's data packets for acceptance at the backup tunnel tail (the merge point).</li> </ul>
Bkup Sender Template	<p>If the Outbound FRR state is Ready or Active, SENDER_TEMPLATE and FILTERSPEC objects are shown. These objects will be used in RSVP messages sent by the backup tunnel if or when the LSP starts actively using the backup tunnel. They differ from the original (prefailure) objects only in that the node (the PLR) substitutes its own IP address for that of the original sender. For example, path and pathTear messages will contain the new SENDER_TEMPLATE. Resv and resvTear messages will contain the new FILTERSPEC object. If this LSP begins actively using the backup tunnel, the display changes.</p>

Field	Description
Bkup FilerSpec	If the Outbound FRR state is Ready or Active, SENDER_TEMPLATE and FILTERSPEC objects are shown. These objects will be used in RSVP messages sent by the backup tunnel if or when the LSP starts actively using the backup tunnel. They differ from the original (prefailure) objects only in that the node (the PLR) substitutes its own IP address for that of the original sender. For example, path and pathTear messages will contain the new SENDER_TEMPLATE. Resv and resvTear messages will contain the new FILTERSPEC object. If this LSP begins actively using the backup tunnel, the display changes.
Path ID handle	Protection Switch Byte (PSB) identifier.
Incoming policy	Policy decision of the LSP. If RSVP policy was not granted for the incoming path message for the tunnel, the LSP does not come up. Accepted is displayed.
Policy source(s)	For FRR LSPs, this value always is MPLS/TE for the policy source.
Status	For FRR LSPs, valid values are as follows: <ul style="list-style-type: none"> <li>• Proxied--Headend routers.</li> <li>• Proxied Terminated--Tailend routers.</li> </ul> For midpoint routers, the field always is blank.

The following example shows P2MP data:

```
Router# show ip rsvp fast-reroute detail
```

```
PATH:
P2MP ID: 22 Tun ID: 22 Ext Tun ID: 10.1.1.201
Tun Sender: 10.1.1.201 LSP ID: 1 SubGroup Orig: 10.1.1.201
SubGroup ID: 2
S2L Destination : 10.1.1.206
Path refreshes:
sent: to NHOP 10.0.0.205 on Ethernet0/0
Session Attr:
Setup Prio: 7, Holding Prio: 7
Flags: (0xF) Local Prot desired, Label Recording, SE Style, Bandwidth Prot desired
Session Name: R201_t22
ERO: (incoming)
10.1.1.201 (Strict IPv4 Prefix, 8 bytes, /32)
10.0.0.201 (Strict IPv4 Prefix, 8 bytes, /32)
10.0.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
10.1.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
10.1.0.206 (Strict IPv4 Prefix, 8 bytes, /32)
10.1.1.206 (Strict IPv4 Prefix, 8 bytes, /32)
ERO: (outgoing)
10.0.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
```

```

10.1.0.205 (Strict IPv4 Prefix, 8 bytes, /32)
10.1.0.206 (Strict IPv4 Prefix, 8 bytes, /32)
10.1.1.206 (Strict IPv4 Prefix, 8 bytes, /32)
Traffic params - Rate: 500K bits/sec, Max. burst: 1K bytes
Min Policed Unit: 1 bytes, Max Pkt Size 2147483647 bytes
Fast-Reroute Backup info:
Inbound FRR: Not active
Outbound FRR: Ready -- backup tunnel selected
Backup Tunnel: Tu666 (label 20)
Bkup Sender Template:
  Tun Sender: 10.0.2.201 LSP ID: 1 SubGroup Orig: 10.1.1.201
  SubGroup ID: 2
Bkup FilerSpec:
  Tun Sender: 10.0.2.201, LSP ID: 1, SubGroup Orig: 10.1.1.201
  SubGroup ID: 2
Path ID handle: 01000417.
Incoming policy: Accepted. Policy source(s): MPLS/TE
Status: Proxied

```

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

**Table 49: show ip rsvp fast-reroute detail P2MP Field Descriptions**

Field	Description
P2MP ID	A 32-bit number that identifies the set of destinations of the P2MP tunnel.
Tun ID	Tunnel identification number.
Ext Tun ID	Extended tunnel identification number.
Tun Sender	IP address of the sender.
LSP ID	Label switched path identification number.
SubGroup Orig	LSP headend router ID address.
SubGroup ID	An incremental number assigned to each sub-LSP signaled from the headend router.
S2L Destination	LSP tailend router ID address.

#### Related Commands

Command	Description
<b>mpls traffic-eng fast-reroute backup-prot-preemption</b>	Changes the backup protection preemption algorithm to minimize the amount of bandwidth that is wasted.

## show ip rsvp hello

To display hello status and statistics for Fast Reroute, reroute (hello state timer), and graceful restart, use the **showiprsvphello** command in user EXEC or privileged EXEC mode.

**show ip rsvp hello**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** User EXEC (>) Privileged EXEC (#)

Command History	Release	Modification
	12.0(22)S	This command was introduced.
	12.0(29)S	The command output was modified to include graceful restart, reroute (hello state timer), and Fast Reroute information.
	12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
	12.2(33)SRA	The command output was modified to show whether graceful restart is configured and full mode was added.
	12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
	12.2(33)SRC	The command output was modified to include Bidirectional Forwarding Detection (BFD) protocol information.
	12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
	15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

**Examples** The following is sample output from the **showiprsvphello** command:

```
Router# show ip rsvp hello
Hello:
  RSVP Hello for Fast-Reroute/Reroute: Enabled
  Statistics: Disabled
  BFD for Fast-Reroute/Reroute: Enabled
  RSVP Hello for Graceful Restart: Disabled
```

The table below describes the significant fields shown in the display. The fields describe the processes for which hello is enabled or disabled.

**Table 50: show ip rsvp hello Field Descriptions**

Field	Description
RSVP Hello for Fast-Reroute/Reroute	Status of Fast-Reroute/Reroute: <ul style="list-style-type: none"> <li>• Disabled--Fast reroute and reroute (hello for state timer) are not activated (disabled).</li> <li>• Enabled--Fast reroute and reroute (hello for state timer) are activated (enabled).</li> </ul>
Statistics	Status of hello statistics: <ul style="list-style-type: none"> <li>• Disabled--Hello statistics are not configured.</li> <li>• Enabled--Statistics are configured. Hello packets are time-stamped when they arrive in the hello input queue for the purpose of recording the time required until they are processed.</li> <li>• Shutdown--Hello statistics are configured but not operational. The input queue is too long (that is, more than 10,000 packets are queued).</li> </ul>
BFD for Fast-Reroute/Reroute	Status of BFD for Fast-Reroute/Reroute: <ul style="list-style-type: none"> <li>• Disabled--BFD is not configured.</li> <li>• Enabled--BFD is configured.</li> </ul>
Graceful Restart	Restart capability: <ul style="list-style-type: none"> <li>• Disabled--Restart capability is not activated.</li> <li>• Enabled--Restart capability is activated for a router (full mode) or its neighbor (help-neighbor).</li> </ul>

**Related Commands**

Command	Description
<b>ip rsvp signalling hello (configuration)</b>	Enables hello globally on the router.
<b>ip rsvp signalling hello statistics</b>	Enables hello statistics on the router.
<b>show ip rsvp hello statistics</b>	Displays how long hello packets have been in the hello input queue.

# show ip rsvp hello client lsp detail

To display detailed information about Resource Reservation Protocol (RSVP) traffic engineering (TE) client hellos for label-switched paths (LSPs), use the **show ip rsvp hello client lsp detail** command in user EXEC or privileged EXEC mode.

**show ip rsvp hello client lsp detail** [*filter* [*destination* *hostname*]]

## Syntax Description

<b>filter</b>	(Optional) Specifies filters to limit the display of output.
<b>destination</b>	(Optional) Displays the filters configured on the destination (tunnel tail).
<i>hostname</i>	(Optional) IP address or name of destination (tunnel tail).

## Command Modes

User EXEC (>) Privileged EXEC (#)

## Command History

Release	Modification
12.0(33)S	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

## Usage Guidelines

Use the **show ip rsvp hello client lsp detail** command to display information about the LSPs, including IP addresses and their types.

## Examples

The following is sample output from the **show ip rsvp hello client lsp detail** command:

```
Router# show ip rsvp hello client lsp detail
Hello Client LSPs (all lsp tree)
  Tun Dest: 10.0.1.1  Tun ID: 14  Ext Tun ID: 172.16.1.1
  Tun Sender: 172.16.1.1  LSP ID: 31
    Lsp flags: 0x32
    Lsp GR DN nbr: 192.168.1.1
    Lsp RR DN nbr: 10.0.0.3 HST
```

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

**Table 51: show ip rsvp hello client lsp detail Field Descriptions**

Field	Description
Hello Client LSPs	Current clients include graceful restart (GR), reroute (RR) (hello state timer), and fast reroute (FRR).
Tun Dest	IP address of the destination tunnel.
Tun ID	Identification number of the tunnel.
Ext Tun ID	Extended identification number of the tunnel. Usually, this is the same as the source address.
Tun Sender	IP address of the tunnel sender.
LSP ID	Identification number of the LSP.
Lsp flags	LSP database information.
Lsp GR DN nbr	IP address of the LSP graceful restart downstream neighbor.
Lsp RR DN nbr	IP address of the LSP reroute downstream neighbor; HST--hello state timer.

**Related Commands**

Command	Description
<b>show ip rsvp hello</b>	Displays hello status and statistics for fast reroute, reroute (hello state timer), and graceful restart.