

show ip nbar port-map

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

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

Syntax Description	<i>protocol-name</i> (Optional) Limits the command display to the specified protocol.
---------------------------	---

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.

Usage Guidelines	<p>The show ip nbar port-map command displays port assignments for NBAR protocols.</p> <p>This command is used to display the current protocol-to-port mappings in use by NBAR. When the ip nbar port-map command has been used, the show ip nbar port-map command displays the ports assigned by the user to the protocol. If no ip nbar port-map command has been used, the show ip nbar port-map command displays the default ports. The <i>protocol-name</i> argument can also be used to limit the display to a specific protocol.</p>
-------------------------	--

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

```
Router# show ip nbar port-map

port-map bgp      udp 179
port-map bgp      tcp 179
port-map cuseeme  udp 7648 7649
port-map cuseeme  tcp 7648 7649
port-map dhcp     udp 67 68
port-map dhcp     tcp 67 68
```

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

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 interface-spec] [stats {byte-count | bit-rate
| packet-count}] [{protocol protocol-name | top-n number}]
```

Syntax Description

interface	(Optional) Specifies that Protocol Discovery statistics for the interface are to be displayed.
<i>interface-spec</i>	(Optional) Specifies an interface to display.
stats	(Optional) Specifies that the byte count, byte rate, or packet count is to be displayed.
byte-count	(Optional) Specifies that the byte count is to be displayed.
bit-rate	(Optional) Specifies that the bit rate is to be displayed.
packet-count	(Optional) Specifies that the packet count is to be displayed.
protocol	(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.
top-n	(Optional) Specifies that a top-n is to be displayed. A top-n is the number of most active NBAR-supported protocols, where n is the number of protocols to be displayed. For instance, if top-n 3 is entered, the three most active NBAR-supported protocols will be displayed.
<i>number</i>	(Optional) Specifies the number of most active NBAR-supported protocols to be displayed.

Defaults

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.

Usage Guidelines

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

Use the **show ip nbar protocol-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.

Examples

The following example displays partial output of the **show ip nbar protocol-discovery** command for an Ethernet interface:

```
Router# show ip nbar protocol-discovery interface FastEthernet 6/0
```

```
FastEthernet6/0

Protocol                Input                Output
                        Packet Count         Packet Count
                        Byte Count           Byte Count
                        5 minute bit rate (bps) 5 minute bit rate (bps)
-----
igrp                    316773              0
                        26340105            0
                        3000                0
streamwork             4437                7367
                        2301891             339213
                        3000                0
rsvp                   279538             14644
                        319106191           673624
                        0                   0
ntp                    8979               7714
                        906550             694260
                        0                   0
.
.
.
Total                  17203819           151684936
                        19161397327        50967034611
                        4179000            6620000
```

Related Commands

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

show ip rsvp

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

show ip rsvp [**atm-peak-rate-limit** | **counters** | **host** | **installed** | **interface** | **listeners** | **neighbor** | **policy** | **precedence** | **request** | **reservation** | **sbm** | **sender** | **signalling** | **tos**]

Syntax Description	
atm-peak-rate-limit	(Optional) RSVP peak rate limit.
counters	(Optional) RSVP statistics.
host	(Optional) RSVP endpoint senders and receivers.
installed	(Optional) RSVP installed reservations.
interface	(Optional) RSVP interface information.
listeners	(Optional) RSVP listeners.
neighbor	(Optional) RSVP neighbor information.
policy	(Optional) RSVP policy information.
precedence	(Optional) RSVP precedence settings.
request	(Optional) RSVP reservations upstream.
reservation	(Optional) RSVP reservation requests from downstream.
sender	(Optional) RSVP path state information.
sbm	(Optional) RSVP subnet bandwidth manager (SBM) information.
signalling	(Optional) RSVP signalling information.
tos	(Optional) RSVP type of service (TOS) settings.

Command Modes EXEC

Command History	Release	Modification
	12.0(3)T	This command was introduced.
	12.2(13)T	The listeners and policy keywords were added, and this command was modified to display RSVP global settings when no keywords or arguments are entered.

Examples The following command shows RSVP rate-limiting, refresh-reduction, and neighbor information:

```
Router# show ip rsvp

Rate Limiting:enabled
  Max msgs per interval:4
  Interval length (msec):20
  Max queue size:500
  Max msgs per second:200

Refresh Reduction:enabled
  ACK delay (msec):250
```

```

Initial retransmit delay (msec):1000
Local epoch:0x16528C
Message IDs:in use 580, total allocated 3018, total freed 2438

Neighbors:1
  RSVP encap:1 UDP encap:0 RSVP and UDP encap:0

Local policy:
COPS:

Generic policy settings:
  Default policy:Accept all
  Preemption:    Disabled

```

Table 26 describes the fields shown in the display.

Table 26 *show ip rsvp Command Field Descriptions*

Field	Description
Rate Limiting: enabled (active) or disabled (not active)	<p>The RSVP rate-limiting parameters in effect including the following:</p> <ul style="list-style-type: none"> • Max msgs per interval = number of messages allowed to be sent per interval (timeframe). • Interval length (msecs) = interval (timeframe) length in milliseconds. • Max queue size = maximum size of the message queue in bytes. • Max msgs per second = maximum number of messages allowed to be sent per second.
Refresh Reduction: enabled (active) or disabled (not active)	<p>The RSVP refresh-reduction parameters in effect including the following:</p> <ul style="list-style-type: none"> • ACK delay (msec) = how long in milliseconds before the receiving router sends an acknowledgment (ACK). • Initial retransmit delay (msec) = how long in milliseconds before the router retransmits a message. • Local epoch = the RSVP message identifier (ID) number space identifier; randomly generated each time a node reboots or the RSVP process restarts. • Message IDs = the number of message IDs in use, the total number allocated, and the total number available (freed).
Neighbors	The total number of neighbors and the types of encapsulation in use including RSVP and User Datagram Protocol (UDP).
Local policy	The local policy currently configured.

Table 26 *show ip rsvp Command Field Descriptions (continued)*

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> <p>Default policy: Accept all means all RSVP messages are accepted and forwarded. Reject all means all RSVP messages are rejected.</p> <p>Preemption: Disabled means RSVP is not prioritizing reservations and allocating bandwidth accordingly. Enabled means RSVP is prioritizing reservations and allocating more bandwidth to those with the highest priority.</p>

Related Commands

Command	Description
debug ip rsvp	Displays debug messages for RSVP categories.

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 **show ip rsvp atm-peak-rate-limit** command in EXEC mode.

```
show ip rsvp atm-peak-rate-limit [interface-id]
```

Syntax Description	<i>interface-id</i>	(Optional) Specifies the interface for which current peak rate limit statistics should be displayed.
---------------------------	---------------------	--

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	12.0(3)T	This command was introduced.

Usage Guidelines The **show ip rsvp atm-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 **show ip rsvp atm-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 **ip rsvp atm-peak-rate-limit** command.

The following is sample output from the **show ip rsvp atm-peak-rate-limit** command using the *interface-id* argument:

```
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 **show ip rsvp atm-peak-rate-limit** command when no interface name is given:

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

```
Interface name      Peak rate limit
Ethernet0/1/1      not set
ATM2/0/0           not set
ATM2/0/0.1        100K
```

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

```
Interface name      Peak rate limit
Ethernet0/1         not set
ATM2/1/0            1M
ATM2/1/0.10         not set
ATM2/1/0.11         not set
ATM2/1/0.12         not set
```

Related Commands

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

show ip rsvp counters

To display the number of Resource Reservation Protocol (RSVP) messages that were sent and received on each interface, use the **show ip rsvp counters** command in EXEC mode.

show ip rsvp counters [**interface** *interface_unit* | **summary** | **neighbor**]

Syntax Description

interface <i>interface_unit</i>	(Optional) Number of RSVP messages sent and received for the specified interface name.
summary	(Optional) Cumulative number of RSVP messages sent and received by the router over all interfaces.
neighbor	(Optional) Number of RSVP messages sent and received by the specified neighbor.

Command Modes

EXEC

Command History

Release	Modification
12.0(14)ST	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T, and the neighbor keyword was added.
12.2(15)T	The following modifications were made to this command: <ul style="list-style-type: none"> The neighbor keyword was added. The output was modified to show the errors counter incrementing. This occurs whenever an RSVP message, on which the authentication checks have failed, is received on an interface that has RSVP authentication enabled.

Usage Guidelines

Use the **show ip rsvp counters** command to display the number of RSVP messages that were sent and received for each interface on which RSVP is configured.

If you enter the **show ip rsvp counters** command without a keyword, the command displays the number of RSVP messages that were sent and received for each interface on which RSVP is configured.

Examples

The following command shows the values for the number of RSVP messages of each type that were sent and received by the router over all interfaces:

```
Router# show ip rsvp counters summary
```

```
All Interfaces          Recv      Xmit
Path                    23284     0      Resv          0      23258
PathError               0         0      ResvError     0         0
PathTear                6         0      ResvTear     0         6
ResvConf                0         0      RTearConf    0         0
Ack                     186       86     Srefresh     85        93
DSBM_WILLING            0         0      I_AM_DSBM    0         0
Unknown                 0         0      Errors       0         0
```

Table 27 describes the fields shown in the display.

Table 27 show ip rsvp counters summary Command Field Descriptions

Field	Description
All Interfaces	Types of messages displayed for all interfaces.
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.

Related Commands

Command	Description
clear ip rsvp counters	Clears (sets to zero) all IP RSVP counters that are being maintained by the router.

show ip rsvp installed

To display Resource Reservation Protocol (RSVP)-related installed filters and corresponding bandwidth information, use the **show ip rsvp installed** command in EXEC mode.

show ip rsvp installed [*interface-type interface-number*] [**detail**]

Syntax Description	detail	(Optional) Specifies additional information about interfaces and their reservations.
	<i>interface-type</i>	(Optional) Specifies the type of the interface.
	<i>interface-number</i>	(Optional) Specifies the number of the interface.

Command Modes EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	12.2(15)T	The command output was modified to display the resources required for a traffic control state block (TCSB) after compression has been taken into account.

Usage Guidelines The **show ip rsvp installed** command displays information about interfaces and their reservations. Enter the optional **detail** keyword for additional information, including the reservation's traffic parameters, downstream hop, compression, and resources used by RSVP to ensure quality of service (QoS) for this reservation.

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

```
Router# show ip rsvp installed

RSVP:
RSVP: Ethernet1: has no installed reservations
RSVP: Serial0:
  kbps  To          From          Protocol DPort Sport Weight Conversation
  0     224.250.250.1  132.240.2.28  UDP 20   30   128   270
  150   224.250.250.1  132.240.2.1   UDP 20   30   128   268
  100   224.250.250.1  132.240.1.1   UDP 20   30   128   267
  200   224.250.250.1  132.240.1.25  UDP 20   30   256   265
  200   224.250.250.2  132.240.1.25  UDP 20   30   128   271
  0     224.250.250.2  132.240.2.28  UDP 20   30   128   269
  150   224.250.250.2  132.240.2.1   UDP 20   30   128   266
  350   224.250.250.3  0.0.0.0       UDP 20   0    128   26
```

Table 28 describes the significant fields shown in the display.

Table 28 *show ip rsvp installed Field Descriptions*

Field	Description
kbps	Reserved rate.
To	IP address of the source device.
From	IP address of the destination device.
Protocol	Protocol User Datagram Protocol (UDP)/TCP type.
DPort	Destination UDP/TCP port
Sport	Source UDP/TCP port.
Weight	Weight used in weighted fair queueing (WFQ).
Conversation	WFQ conversation number. If the WFQ is not configured on the interface, weight and conversation will be zero.

RSVP Compression Method Prediction Example

The following example of the **show ip rsvp installed detail** command shows the compression parameters, including the compression method, the compression context ID, and the bytes saved per packet, on the serial3/0 interface in effect:

```
Router# show ip rsvp installed detail

RSVP:Ethernet2/1 has no installed reservations

RSVP:Serial3/0 has the following installed reservations
RSVP Reservation. Destination is 10.1.1.2. Source is 10.1.1.1,
  Protocol is UDP, Destination port is 18054, Source port is 19156
  Compression:(method rtp, context ID = 1, 37.98 bytes-saved/pkt avg)
  Admitted flowspec:
    Reserved bandwidth:65600 bits/sec, Maximum burst:328 bytes, Peak rate:80K bits/sec
    Min Policed Unit:164 bytes, Max Pkt Size:164 bytes
  Admitted flowspec (as required if compression were not applied):
    Reserved bandwidth:80K bits/sec, Maximum burst:400 bytes, Peak rate:80K bits/sec
    Min Policed Unit:200 bytes, Max Pkt Size:200 bytes
  Resource provider for this flow:
    WFQ on FR PVC dlc1 101 on Se3/0: PRIORITY queue 24. Weight:0, BW 66 kbps
  Conversation supports 1 reservations [0x1000405]
  Data given reserved service:3963 packets (642085 bytes)
  Data given best-effort service:0 packets (0 bytes)
  Reserved traffic classified for 80 seconds
  Long-term average bitrate (bits/sec):64901 reserved, 0 best-effort
  Policy:INSTALL. Policy source(s):Default
```

The following example of the **show ip rsvp installed detail** command shows that compression is not predicted on the serial3/0 interface because no compression context IDs are available:

```
Router# show ip rsvp installed detail

RSVP:Ethernet2/1 has no installed reservations

RSVP:Serial3/0 has the following installed reservations
RSVP Reservation. Destination is 10.1.1.2. Source is 10.1.1.1,
  Protocol is UDP, Destination port is 18116, Source port is 16594
  Compression:(rtp compression not predicted:no contexts available)
```

```

Admitted flowspec:
  Reserved bandwidth:80K bits/sec, Maximum burst:400 bytes, Peak rate:80K bits/sec
  Min Policed Unit:200 bytes, Max Pkt Size:200 bytes
Resource provider for this flow:
  WFQ on FR PVC dlc1 101 on Se3/0: PRIORITY queue 24. Weight:0, BW 80 kbps
Conversation supports 1 reservations [0x2000420]
Data given reserved service:11306 packets (2261200 bytes)
Data given best-effort service:0 packets (0 bytes)
Reserved traffic classified for 226 seconds
Long-term average bitrate (bits/sec):79951 reserved, 0 best-effort
Policy:INSTALL. Policy source(s):Default

```

**Note**

When no compression context IDs are available, use the **ip rtp compression-connections** *number* command to increase the pool of compression context IDs.

Related Commands

Command	Description
ip rtp compression-connections	Specifies the total number of RTP header compression connections that can exist on an interface.
show ip rsvp interface	Displays RSVP-related information.

show ip rsvp interface

To display Resource Reservation Protocol (RSVP)-related information, use the **show ip rsvp interface** command in EXEC mode.

show ip rsvp interface [*interface-type interface-number*] [**detail**]

Syntax Description		
	<i>interface-type</i>	(Optional) Type of the interface.
	<i>interface-number</i>	(Optional) Number of the interface.
	detail	(Optional) Additional information about interfaces.

Command Modes EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	12.2(2)T	The detail keyword was added.
	12.2(4)T	This command was implemented on the Cisco 7500 series and the ATM-permanent virtual circuit (PVC) interface.
	12.2(13)T	The following modifications were made to this command: <ul style="list-style-type: none"> • Rate-limiting and refresh-reduction information were added to the output display. • This command was modified to display RSVP global settings when no keywords or arguments are entered.
	12.2(15)T	The following modifications were made to this command: <ul style="list-style-type: none"> • The command output was modified to display the effects of compression on admission control and the RSVP bandwidth limit counter. • Cryptographic authentication parameters were added to the display.

Usage Guidelines

Use the **show ip rsvp interface** command to display information about interfaces on which RSVP is enabled, including the current allocation budget and maximum available bandwidth. Enter the optional **detail** keyword for additional information, including bandwidth and signaling parameters and blockade state.

Use the **show ip rsvp interface detail** command to display information about the RSVP parameters associated with an interface. These parameters include the following:

- Total RSVP bandwidth
- RSVP bandwidth allocated to existing flows
- Maximum RSVP bandwidth that can be allocated to a single flow
- The type of admission control supported (header compression methods)
- The compression methods supported by RSVP compression prediction

Examples

The following command shows information for each interface on which RSVP is enabled:

```
Router# show ip rsvp interface

interface    allocated  i/f max  flow max  sub max
PO0/0        0          200M    200M     0
PO1/0        0          50M     50M      0
PO1/1        0          50M     50M      0
PO1/2        0          50M     50M      0
PO1/3        0          50M     50M      0
Lo0          0          200M    200M     0
```

Table 29 describes the fields shown in the display.

Table 29 show ip rsvp interface Field Descriptions

Field	Description
interface	Interface name.
allocated	Current allocation budget.
i/f max	Maximum allocatable bandwidth.
flow max	Largest single flow allocatable on this interface.
sub max	Largest sub-pool value allowed on this interface.

Detailed RSVP Information Example

The following command shows detailed RSVP information for each interface on which RSVP is enabled:

```
Router# show ip rsvp interface detail

PO0/0:
  Bandwidth:
    Curr allocated:0 bits/sec
    Max. allowed (total):200M bits/sec
    Max. allowed (per flow):200M bits/sec
    Max. allowed for LSP tunnels using sub-pools:0 bits/sec
    Set aside by policy (total):0 bits/sec
  Signalling:
    DSCP value used in RSVP msgs:0x3F
    Number of refresh intervals to enforce blockade state:4
    Number of missed refresh messages:4
    Refresh interval:30

PO1/0:
  Bandwidth:
    Curr allocated:0 bits/sec
    Max. allowed (total):50M bits/sec
    Max. allowed (per flow):50M bits/sec
    Max. allowed for LSP tunnels using sub-pools:0 bits/sec
    Set aside by policy (total):0 bits/sec
  Signalling:
    DSCP value used in RSVP msgs:0x3F
    Number of refresh intervals to enforce blockade state:4
    Number of missed refresh messages:4
    Refresh interval:30

PO1/1:
  Bandwidth:
    Curr allocated:0 bits/sec
```

```

Max. allowed (total):50M bits/sec
Max. allowed (per flow):50M bits/sec
Max. allowed for LSP tunnels using sub-pools:0 bits/sec
Set aside by policy (total):0 bits/sec
Signalling:
  DSCP value used in RSVP msgs:0x3F
  Number of refresh intervals to enforce blockade state:4
  Number of missed refresh messages:4
  Refresh interval:30

PO1/2:
  Bandwidth:
    Curr allocated:0 bits/sec
    Max. allowed (total):50M bits/sec
    Max. allowed (per flow):50M bits/secMax. allowed for LSP tunnels using sub-pools:0
bits/sec
    Set aside by policy (total):0 bits/sec
  Signalling:
    DSCP value used in RSVP msgs:0x3F
    Number of refresh intervals to enforce blockade state:4
    Number of missed refresh messages:4
    Refresh interval:30

PO1/3:
  Bandwidth:
    Curr allocated:0 bits/sec
    Max. allowed (total):50M bits/sec
    Max. allowed (per flow):50M bits/sec
    Max. allowed for LSP tunnels using sub-pools:0 bits/sec
    Set aside by policy (total):0 bits/sec
  Signalling:
    DSCP value used in RSVP msgs:0x3F
    Number of refresh intervals to enforce blockade state:4
    Number of missed refresh messages:4
    Refresh interval:30

Lo0:
  Bandwidth:
    Curr allocated:0 bits/sec
    Max. allowed (total):200M bits/sec
    Max. allowed (per flow):200M bits/sec
    Max. allowed for LSP tunnels using sub-pools:0 bits/sec
    Set aside by policy (total):0 bits/sec
  Signalling:
    DSCP value used in RSVP msgs:0x3F
    Number of refresh intervals to enforce blockade state:4
    Number of missed refresh messages:4
    Refresh interval:30

```

Table 30 describes the significant fields shown in the detailed display for interface PO0/0. The fields for the other interfaces are similar.

Table 30 *show ip rsvp interface detail Field Descriptions –Detailed RSVP Information Example*

Field	Description
PO0/0	Interface name.
Bandwidth	<p>The RSVP bandwidth parameters in effect including the following:</p> <ul style="list-style-type: none"> • Curr allocated = amount of bandwidth currently allocated in bits per second. • Max. allowed (total) = maximum amount of bandwidth allowed in bits per second. • Max. allowed (per flow) = maximum amount of bandwidth allowed per flow in bits per second. • Max. allowed for LSP tunnels using sub-pools = maximum amount of bandwidth allowed for label switched path (LSP) tunnels in bits per second. • Set aside by policy (total) = the amount of bandwidth set aside by the local policy in bits per second.
Signalling	<p>The RSVP signalling parameters in effect including the following:</p> <ul style="list-style-type: none"> • DSCP value used in RSVP msgs = differentiated services code point (DSCP) used in RSVP messages. • Number of refresh intervals to enforce blockade state = how long in milliseconds before the blockade takes effect. • Number of missed refresh messages = how many refresh messages until the router state expires. • Refresh interval = how long in milliseconds until a refresh message is sent.

RSVP Compression Method Prediction Example

The following example from the **show ip rsvp interface detail** command shows the RSVP compression method prediction configuration for each interface on which RSVP is configured:

```
Router# show ip rsvp interface detail

Et2/1:
  Bandwidth:
    Curr allocated:0 bits/sec
    Max. allowed (total):1158K bits/sec
    Max. allowed (per flow):128K bits/sec
    Max. allowed for LSP tunnels using sub-pools:0 bits/sec
    Set aside by policy (total):0 bits/sec
  Admission Control:
    Header Compression methods supported:
      rtp (36 bytes-saved), udp (20 bytes-saved)
  Neighbors:
    Using IP encap:0. Using UDP encap:0
  Signalling:
    Refresh reduction:disabled
    Authentication:disabled
```

```

Se3/0:
  Bandwidth:
    Curr allocated:0 bits/sec
    Max. allowed (total):1158K bits/sec
    Max. allowed (per flow):128K bits/sec
    Max. allowed for LSP tunnels using sub-pools:0 bits/sec
    Set aside by policy (total):0 bits/sec
  Admission Control:
    Header Compression methods supported:
      rtp (36 bytes-saved), udp (20 bytes-saved)
  Neighbors:
    Using IP encap:1. Using UDP encap:0
  Signalling:
    Refresh reduction:disabled
  Authentication:disabled
  
```

Table 31 describes the significant fields shown in the display for interface Ethernet2/1. The fields for interface Serial3/0 are similar.

Table 31 *show ip rsvp interface detail* Field Descriptions—RSVP Compression Method Prediction Example

Field	Description
Et2/1: Se3/0	Interface name.
Bandwidth	The RSVP bandwidth parameters in effect including the following: <ul style="list-style-type: none"> • Curr allocated = amount of bandwidth currently allocated in bits per second. • Max. allowed (total) = maximum amount of bandwidth allowed in bits per second. • Max. allowed (per flow) = maximum amount of bandwidth allowed per flow in bits per second. • Max. allowed for LSP tunnels using sub-pools = maximum amount of bandwidth allowed for LSP tunnels in bits per second. • Set aside by policy (total) = the amount of bandwidth set aside by the local policy in bits per second.
Admission Control	The type of admission control in effect including the following: <ul style="list-style-type: none"> • Header Compression methods supported: <ul style="list-style-type: none"> – Real-Time Transport Protocol (RTP) or User Data Protocol (UDP) compression schemes and the number of bytes saved per packet.
Neighbors	The number of neighbors using IP and UDP encapsulation.
Signalling	The type of signaling in effect; Refresh reduction is either enabled (active) or disabled (inactive).
Authentication	Authentication is either enabled (active) or disabled (inactive).

Cryptographic Authentication Example

The following example of the **show ip rsvp interface detail** command displays detailed information, including the cryptographic authentication parameters, for all RSVP-configured interfaces on the router:

```
Router# show ip rsvp interface detail
```

```
Et0/0:
  Bandwidth:
    Curr allocated: 0 bits/sec
    Max. allowed (total): 7500K bits/sec
    Max. allowed (per flow): 7500K bits/sec
    Max. allowed for LSP tunnels using sub-pools: 0 bits/sec
    Set aside by policy (total):0 bits/sec
  Neighbors:
    Using IP encap: 0. Using UDP encap: 0
  Signalling:
    Refresh reduction: disabled
  Authentication: enabled
    Key: 11223344
    Type: sha-1
    Window size: 2
    Challenge: enabled
```

Table 32 describes the significant fields shown in the display.

Table 32 *show ip rsvp interface detail Field Descriptions—Cryptographic Authentication Example*

Field	Description
Et0/0	Interface name.
Bandwidth	The RSVP bandwidth parameters in effect including the following: <ul style="list-style-type: none"> • Curr allocated = amount of bandwidth currently allocated in bits per second. • Max. allowed (total) = maximum amount of bandwidth allowed in bits per second. • Max. allowed (per flow) = maximum amount of bandwidth allowed per flow in bits per second. • Max. allowed for LSP tunnels using sub-pools = maximum amount of bandwidth allowed for LSP tunnels in bits per second. • Set aside by policy (total) = the amount of bandwidth set aside by the local policy in bits per second.
Neighbors	The number of neighbors using IP and UDP encapsulation.
Signalling	The type of signaling in effect; Refresh reduction is either enabled (active) or disabled (inactive).

Table 32 *show ip rsvp interface detail Field Descriptions—Cryptographic Authentication Example (continued)*

Field	Description
Authentication	<p>Authentication is either enabled (active) or disabled (inactive). The parameters include the following:</p> <ul style="list-style-type: none"> • Key = The key (string) for the RSVP authentication algorithm displayed in clear text (for example, 11223344) or encrypted <encrypted>. • Type = The algorithm to generate cryptographic signatures in RSVP messages; possible values are md5 and sha-1. • Window size = Maximum number of RSVP authenticated messages that can be received out of order. • Challenge = The challenge-response handshake performed with any new RSVP neighbors that are discovered on a network; possible values are enabled (active) or disabled (inactive).

Related Commands

Command	Description
show ip rsvp installed	Displays RSVP-related installed filters and corresponding bandwidth information.
show ip rsvp neighbor	Displays current RSVP neighbors.

show ip rsvp listeners

To display the Resource Reservation Protocol (RSVP) listeners for a specified port or protocol, use the **show ip rsvp listeners** command in EXEC mode.

```
show ip rsvp listeners [dst | any] [udp | tcp | any | protocol] [dst-port | any]
```

Syntax Description	<i>dst</i> any	(Optional) A particular destination or any destination for an RSVP message.
	udp tcp any <i>protocol</i>	(Optional) User Datagram Protocol (UDP), TCP, or any protocol to be used on the receiving interface and the UDP or TCP source port number. Note If you select <i>protocol</i> , the range is 0 to 255 and the protocol is IP.
	<i>dst-port</i> any	(Optional) A particular destination port from 0 to 65535 or any destination for an RSVP message.

Defaults If you enter **show ip rsvp listeners** command without a keyword or an argument, the command displays all the listeners that were sent and received for each interface on which RSVP is configured.

Command Modes EXEC

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines Use the **show ip rsvp listeners** command to display the number of listeners that were sent and received for each interface on which RSVP is configured.

Examples The following command shows the current listeners:

```
Router# show ip rsvp listeners
```

```
To          Protocol  DPort  Description  Action
145.10.2.1  any       any    RSVP Proxy   reply
```

Table 33 describes the fields shown in the display.

Table 33 *show ip rsvp listeners Command Field Descriptions*

Field	Description
To	IP address of the receiving interface.
Protocol	Protocol used.
DPort	Destination port on the receiving router.
Description	Cisco IOS component that requested RSVP to do the listening; for example, RSVP proxy and label-switched path (LSP) tunnel signaling.
Action	Action taken when a flow arrives at its destination. The choices include: <ul style="list-style-type: none"> • Announce—The arrival of the flow is announced. • Reply—After the flow arrives at its destination, the sender receives a reply.

Related Commands

Command	Description
ip rsvp listener	Configures an RSVP router to listen for Path messages.

show ip rsvp neighbor

To display current Resource Reservation Protocol (RSVP) neighbors, use the **show ip rsvp neighbor** command in EXEC mode.

show ip rsvp neighbor [detail]

Syntax Description	detail	(Optional) Additional information about RSVP neighbors.
---------------------------	---------------	---

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	11.2	This command was introduced.
12.2(13)T	The <i>interface-type interface-number</i> arguments were deleted. The detail keyword was added to the command, and rate-limiting and refresh-reduction information was added to the output.	

Usage Guidelines Use the **show ip rsvp neighbor** command to show the IP addresses for the current RSVP neighbors. Enter the **detail** keyword to display rate-limiting and refresh-reduction parameters for the RSVP neighbors.

Examples The following command shows the current RSVP neighbors:

```
Router# show ip rsvp neighbor

21.0.0.1      RSVP
22.0.0.2      RSVP
```

[Table 34](#) describes the fields shown in the display.

Table 34 show ip rsvp neighbor Command Field Descriptions

Field	Description
21.0.0.1	IP address of neighboring router.
RSVP	Type of encapsulation being used.

The following command shows the rate-limiting and refresh-reduction parameters for the current RSVP neighbors:

```
Router# show ip rsvp neighbor detail

Neighbor:21.0.0.1
  Encapsulation:RSVP
  Rate-Limiting:
    Dropped messages:0
```

```

Refresh Reduction:
  Remote epoch:0x1BFEA5
  Out of order messages:0
  Retransmitted messages:0
  Highest rcvd message id:1059
  Last rcvd message:00:00:04

Neighbor:22.0.0.2
  Encapsulation:RSVP
  Rate-Limiting:
    Dropped messages:0
  Refresh Reduction:
    Remote epoch:0xB26B1
    Out of order messages:0
    Retransmitted messages:0
    Highest rcvd message id:945
    Last rcvd message:00:00:05
    
```

Table 35 describes the fields shown in the display.

Table 35 show ip rsvp neighbor detail Command Field Descriptions

Field	Description
Neighbor	IP address of the neighboring router.
Encapsulation	Type of encapsulation being used.
Rate-Limiting	The rate-limiting parameters in effect including: <ul style="list-style-type: none"> Dropped messages = number of messages dropped by the neighbor.
Refresh Reduction	The refresh-reduction parameters in effect including: <ul style="list-style-type: none"> Remote epoch = the RSVP message number space identifier (ID); randomly generated whenever the node reboots or the RSVP process restarts. Out of order messages = messages that were dropped because they are out of sequential order. Retransmitted messages = number of messages retransmitted to the neighbor. Highest rcvd message id = highest message ID number sent by the neighbor. Last rcvd message= time delta in hours, minutes, and seconds when last message was received by the neighbor.

Related Commands

Command	Description
show ip rsvp interface	Displays RSVP-related interface information.

show ip rsvp policy

To display the policies currently configured, use the **show ip rsvp policy** command in EXEC mode.

```
show ip rsvp policy [cops | local [acl]]
```

Syntax Description	Parameter	Description
	cops local	(Optional) Displays either the configured Common Open Policy Service (COPS) servers or the local policies.
	<i>acl</i>	(Optional) Displays the access control lists (ACLs) whose sessions are governed by COPS servers or the local policies.

Command Modes EXEC

Command History	Release	Modification
	12.1(1)T	This command was introduced as show ip rsvp policy cops .
	12.2(13)T	This command was modified to include the local keyword. This command replaces the show ip rsvp policy cops command.

Usage Guidelines Use the **show ip rsvp policy** command to display current local policies, configured COPS servers, default policies, and the preemption parameter (disabled or enabled).

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

```
Router# show ip rsvp policy

Local policy:

    A=Accept    F=Forward

    Path:-- Resv:-- PathErr:-- ResvErr:-- ACL:104
    Path:-- Resv:-- PathErr:-- ResvErr:-- ACL:None [Default policy]

COPS:

Generic policy settings:
  Default policy: Accept all
  Preemption:     Disabled
```

Table 36 describes the fields shown in the display.

Table 36 *show ip rsvp policy Command Field Descriptions*

Field	Description
Local policy	The local policy currently configured. A = Accept the message. F = Forward the message. Blank (--) means messages of the specified type are neither accepted or forwarded.
COPS	The COPS servers currently in effect.
Generic policy settings	Policy settings that are not specific to COPS or the local policy. Default policy: Accept all means all RSVP messages are accepted and forwarded. Reject all means all RSVP messages are rejected. Preemption: Disabled means that RSVP should not implement any preemption decisions required by a particular local or remote policy. Enabled means that RSVP should implement any preemption decisions required by a particular local or remote policy.

Related Commands

Command	Description
ip rsvp signalling	Creates a local procedure that determines the use of RSVP resources in a network.
initial-retransmit-delay	

show ip rsvp policy cops

The **show ip rsvp policy cops** command is replaced by the **show ip rsvp policy** command. See the **show ip rsvp policy** command for more information.

show ip rsvp policy local

To display the local policies currently configured, use the **show ip rsvp policy local** command in EXEC mode.

show ip rsvp policy local [**detail**] [**default** | **acl** *acl-list-number*]

Syntax Description	detail	(Optional) Additional information about the configured local policies including preempt-priority and local-override.
	default	(Optional) Information about the default policy.
	acl <i>acl-list-number</i>	(Optional) Used when an access control list (ACL) is specified. Values are numbers from 1 to 199.

Command Modes EXEC

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines Use the **show ip rsvp policy local** command to display information about the (selected) local policies currently configured.

If you use the ACL option, you can specify only one ACL. However, that parameter can be any ACL of any local policy that you have created. If you have multiple local policies with a common ACL, then using the ACL option displays all local policies with that ACL. On the other hand, if you have created local policies each with multiple ACLs, you cannot use the ACL option to show only a specific policy. You must omit the ACL option and show all the local policies.

Examples The following is sample output from the **show ip rsvp policy local detail** command after you enter the **ip rsvp policy local acl 104** command:

```
Router# show ip rsvp policy local detail

Local policy for ACL(s): 104
  Preemption Priority: Start at 0, Hold at 0.
  Local Override: Disabled.

          Accept  Forward
Path:      No     No
Resv:      No     No
PathError: No     No
ResvError: No     No

Default local policy:
  Preemption Priority: Start at 0, Hold at 0.
  Local Override: Disabled.
Accept  Forward
Path:    No     No
Resv:    No     No
```

```

PathError: No      No
ResvError: No     No

```

```

Generic policy settings:
  Default policy: Accept all
  Preemption:     Disabled

```

Table 37 describes the fields shown in the display.

Table 37 *show ip rsvp policy local detail Command Field Descriptions*

Field	Description
Local policy for ACL(s)	The local policy currently configured for a specified ACL.
Preemption Priority	Start at 0, Hold at 0 indicates the priorities for resource requests contained in Resv messages that match the ACL(s) of this policy. Values are 0 to 65,535. <ul style="list-style-type: none"> Start at 0 indicates the priority of the reservation when it was installed. Hold at 0 indicates the priority of the reservation after it was installed.
Local Override	Overrides any remote Common Open Policy Service (COPS) policy by enforcing the local policy in effect. <ul style="list-style-type: none"> Disabled = not active. Enabled = active.
Path, Resv, PathError, ResvError	Types of RSVP messages being accepted and forwarded. <ul style="list-style-type: none"> No = message not being accepted or forwarded. Yes = message being accepted and forwarded.
Default local policy	The default local policy currently configured.
Preemption Priority	Start at 0, Hold at 0 indicates the priorities for resource requests contained in Resv messages that match the ACL(s) of this policy. Values are 0 to 65,535. <ul style="list-style-type: none"> Start at 0 indicates the priority of the reservation when it was installed. Hold at 0 indicates the priority of the reservation after it was installed.
Local Override	Overrides any remote (COPS) policy by enforcing the local policy in effect. <ul style="list-style-type: none"> Disabled = not active. Enabled = active.

Related Commands

Command	Description
ip rsvp signalling initial-retransmit-delay	Creates a local procedure that determines the use of RSVP resources in a network.

show ip rsvp request

To display Resource Reservation Protocol (RSVP)-related request information being requested upstream, use the **show ip rsvp request** command in EXEC mode.

show ip rsvp request [*ip-address*] [**detail**]

Syntax Description

<i>ip-address</i>	(Optional) IP or group address of the requestor.
detail	(Optional) Specifies additional request information.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to show the RSVP reservations currently being requested upstream for a specified interface or all interfaces. The received reservations may differ from requests because of aggregated or refused reservations.

Examples

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

```
Router# show ip rsvp request
```

```
To          From          Pro DPort Sport Next Hop      I/F  Fi Serv
132.240.1.49 132.240.4.53  1  0    0    132.240.3.53 Et1  FF LOAD
```

[Table 38](#) describes the significant fields shown in the display.

Table 38 *show ip rsvp request Field Descriptions*

Field	Description
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. Code 1 indicates Internet Control Message Protocol (ICMP).
DPort	Destination port number.
Sport	Source port number.
Next Hop	IP address of the next hop.
I/F	Interface of the next hop.
Fi	Filter (Wild Card Filter, Shared Explicit, or Fixed Filter).
Serv	Service (value can be rate or load).

show ip rsvp reservation

To display Resource Reservation Protocol (RSVP)-related receiver information currently in the database, use the **show ip rsvp reservation** command in EXEC mode.

show ip rsvp reservation [*ip-address*] [**detail**]

Syntax Description	
<i>ip-address</i>	(Optional) IP or group address of the receiver.
detail	(Optional) Specifies additional reservation information.

Command Modes EXEC

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines Use this command to show the current receiver (RESV) information in the database for a specified interface or all interfaces. This information includes reservations aggregated and forwarded from other RSVP routers.

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

```
Router# show ip rsvp reservation

To          From          Pro DPort Sport Next Hop      I/F  Fi Serv
132.240.1.49 132.240.4.53 1 0 0 132.240.1.49 Se1  FF LOAD
```

[Table 39](#) describes the significant fields shown in the display.

Table 39 *show ip rsvp reservation Field Descriptions*

Field	Descriptions
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. Code 1 indicates Internet Control Message Protocol (ICMP).
DPort	Destination port number.
Sport	Source port number.
Next Hop	IP address of the next hop.
I/F	Interface of the next hop.
Fi	Filter (Wild Card Filter, Shared Explicit, or Fixed Filter).
Serv	Service (value can be rate or load).

show ip rsvp sbm

To display information about a Subnetwork Bandwidth Manager (SBM) configured for a specific Resource Reservation Protocol (RSVP)-enabled interface or for all RSVP-enabled interfaces on the router, use the **show ip rsvp sbm** command in EXEC mode.

show ip rsvp sbm [**detail**] [*interface-name*]

Syntax Description	detail	(Optional) Detailed SBM configuration information, including values for the NonResvSendLimit object.
	<i>interface-name</i>	(Optional) Name of the interface for which you want to display SBM configuration information.

Command Modes EXEC

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.1(1)T	The detail keyword was added.

Usage Guidelines

To obtain SBM configuration information about a specific interface configured to use RSVP, specify the interface name with the **show ip rsvp sbm** command. To obtain information about all interfaces enabled for RSVP on the router, use the **show ip rsvp sbm** command without specifying an interface name.

To view the values for the NonResvSendLimit object, use the **detail** keyword.

Examples

The following example displays information for the RSVP-enabled Ethernet interfaces 1 and 2 on router1:

```
Router# show ip rsvp sbm

Interface DSBM Addr      DSBM Priority   DSBM Candidate  My Priority
Et1      1.1.1.1          70              yes              70
Et2      10.2.2.150       100             yes              100
```

The following example displays information about the RSVP-enabled Ethernet interface e2 on router1:

```
Router# show ip rsvp sbm e2

Interface DSBM Addr      DSBM Priority   DSBM candidate  My Priority
e2       10.2.2.150       100             yes              100
```

Table 40 describes the significant fields shown in the display.

Table 40 show ip rsvp sbm Field Descriptions

Field	Description
Interface	Name of the Designated Subnetwork Bandwidth Manager (DSBM) candidate interface on the router.
DSBM Addr	IP address of the DSBM.
DSBM Priority	Priority of the DSBM.
DSBM Candidate	Yes if the ip rsvp dsbm candidate command was issued for this SBM to configure it as a DSBM candidate. No if it was not so configured.
My Priority	Priority configured for this interface.

The following example displays information about the RSVP-enabled Ethernet interface 2 on router1. In the left column, the local SBM configuration is shown; in the right column, the corresponding information for the current DSBM is shown. In this example, the information is the same because the DSBM won election.

```
Router# show ip rsvp sbm detail
```

```
Interface:Ethernet2
Local Configuration          Current DSBM
IP Address:10.2.2.150       IP Address:10.2.2.150
DSBM candidate:yes         I Am DSBM:yes
Priority:100                 Priority:100
Non Resv Send Limit        Non Resv Send Limit
Rate:500 Kbytes/sec         Rate:500 Kbytes/sec
Burst:1000 Kbytes           Burst:1000 Kbytes
Peak:500 Kbytes/sec         Peak:500 Kbytes/sec
Min Unit:unlimited           Min Unit:unlimited
Max Unit:unlimited           Max Unit:unlimited
```

Table 41 describes the significant fields shown in the display.

Table 41 show ip rsvp sbm detail Field Descriptions

Field	Description
Local Configuration	The local DSBM candidate configuration.
Current DSBM	The current DSBM configuration.
Interface	Name of the DSBM candidate interface on the router.
IP Address	IP address of the local DSBM candidate or the current DSBM.
DSBM candidate	Yes if the ip rsvp dsbm candidate command was issued for this SBM to configure it as a DSBM candidate. No if it was not so configured.
I am DSBM	Yes if the local candidate is the DSBM. No if the local candidate is not the DSBM.
Priority	Priority configured for the local DSBM candidate or the current SBM.
Rate	The average rate, in kbps, for the DSBM candidate.
Burst	The maximum burst size, in KB, for the DSBM candidate.

Table 41 *show ip rsvp sbm detail Field Descriptions (continued)*

Field	Description
Peak	The peak rate, in kbps, for the DSBM candidate.
Min Unit	The minimum policed unit, in bytes, for the DSBM candidate.
Max Unit	The maximum packet size, in bytes, for the DSBM candidate.

Related Commands

Command	Description
debug ip rsvp	Displays information about SBM message processing, the DSBM election process, and standard RSVP enabled message processing information.
debug ip rsvp detail	Displays detailed information about RSVP and SBM.
debug ip rsvp detail sbm	Displays detailed information about SBM messages only, and SBM and DSBM state transitions.
ip rsvp dsbm candidate	Configures an interface as a DSBM candidate.
ip rsvp dsbm non-resv-send-limit	Configures the NonResvSendLimit object parameters.

show ip rsvp sender

To display Resource Reservation Protocol (RSVP) PATH-related sender information currently in the database, use the **show ip rsvp sender** command in EXEC mode.

show ip rsvp sender [*ip-address*] [**detail**]

Syntax Description

<i>ip-address</i>	(Optional) IP or group address of the sender.
detail	(Optional) Specifies additional sender information.

Command Modes

EXEC

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to show the RSVP sender (PATH) information currently in the database for a specified interface or all interfaces.

Examples

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

```
Router# show ip rsvp sender
```

```
To          From          Pro DPort Sport Prev Hop      I/F
132.240.1.49 132.240.4.53  1  0    0    132.240.3.53  Et1
132.240.2.51 132.240.5.54  1  0    0    132.240.3.54  Et1
```

[Table 42](#) describes the significant fields shown in this display.

Table 42 show ip rsvp sender Field Descriptions

Field	Description
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. Code 1 indicates Internet Control Message Protocol (ICMP).
DPort	Destination port number.
Sport	Source port number.
Prev Hop	IP address of the previous hop.
I/F	Interface of the previous hop.

show ip rsvp signalling

To display Resource Reservation Protocol (RSVP) signaling information that optionally includes rate-limiting and refresh-reduction parameters for RSVP messages, use the **show ip rsvp signalling** command in EXEC mode.

```
show ip rsvp signalling [rate-limit | refresh reduction]
```

Syntax Description

rate-limit	(Optional) Rate-limiting parameters for signalling messages.
refresh reduction	(Optional) Refresh-reduction parameters and settings.

Command Modes

EXEC

Command History

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

Usage Guidelines

Use the **show ip rsvp signalling** command with either the **rate-limit** or the **refresh reduction** keyword to display rate-limiting parameters or refresh-reduction parameters, respectively.

Examples

The following command shows rate-limiting parameters:

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

```
Rate Limiting:enabled
  Max msgs per interval:4
  Interval length (msec):20
  Max queue size:500
  Max msgs per second:200
  Max msgs allowed to be sent:37
```

[Table 43](#) describes the fields shown in the display.

Table 43 show ip rsvp signalling rate-limit Command Field Descriptions

Field	Description
Rate Limiting: enabled (active) or disabled (not active)	<p>The RSVP rate-limiting parameters in effect including the following:</p> <ul style="list-style-type: none"> • Max msgs per interval = number of messages allowed to be sent per interval (timeframe). • Interval length (msecs) = interval (timeframe) length in milliseconds. • Max queue size = maximum size of the message queue in bytes. • Max msgs per second = maximum number of messages allowed to be sent per second.

The following command shows refresh-reduction parameters:

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

```
Refresh Reduction:enabled
  ACK delay (msec):250
  Initial retransmit delay (msec):1000
  Local epoch:0x74D040
  Message IDs:in use 600, total allocated 3732, total freed 3132
```

[Table 44](#) describes the fields shown in the display.

Table 44 show ip rsvp signalling refresh reduction Command Field Descriptions

Field	Description
Refresh Reduction: enabled (active) or disabled (not active)	<p>The RSVP refresh-reduction parameters in effect including the following:</p> <ul style="list-style-type: none"> • ACK delay (msec) = how long in milliseconds before the receiving router sends an acknowledgment (ACK). • Initial retransmit delay (msec) = how long in milliseconds before the sending router retransmits a message. • Local epoch = the RSVP process identifier that defines a local router for refresh reduction and reliable messaging; randomly generated each time a node reboots or the RSVP process restarts. • Message IDs = the number of message identifiers (IDs) in use, the total number allocated, and the total number available (freed).

Related Commands

Command	Description
clear ip rsvp signalling rate-limit	Clears the counters recording dropped messages.
clear ip rsvp signalling refresh reduction	Clears the counters recording retransmissions and out-of-order messages.
debug ip rsvp rate-limit	Displays debug messages for RSVP rate-limiting events.
ip rsvp signalling rate-limit	Controls the transmission rate for RSVP messages sent to a neighboring router during a specified amount of time.
ip rsvp signalling refresh reduction	Enables refresh reduction.

show ip rsvp signalling blockade

To display the Resource Reservation Protocol (RSVP) sessions that are currently blocked, use the **show ip rsvp signalling blockade** command in EXEC mode.

```
show ip rsvp signalling blockade [detail] [name | address]
```

Syntax Description	detail	(Optional) Additional blockade information.
	<i>name</i>	(Optional) Name of the router being blocked.
	<i>address</i>	(Optional) IP address of the destination of a reservation.

Defaults If you enter the **show ip rsvp signalling blockade** command without a keyword or an argument, the command displays all the blocked sessions on the router.

Command Modes EXEC

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Usage Guidelines Use the **show ip rsvp signalling blockade** command to display the RSVP sessions that are currently blocked.

An RSVP sender becomes blocked when the corresponding receiver sends a Resv message that fails admission control on a router that has RSVP configured. A ResvError message with an admission control error is sent in reply to the Resv message, causing all routers downstream of the failure to mark the associated sender as blocked. As a result, those routers do not include that contribution to subsequent Resv refreshes for that session until the blockade state times out.

Blockading solves a denial-of-service problem on shared reservations where one receiver can request so much bandwidth as to cause an admission control failure for all the receivers sharing that reservation, even though the other receivers are making requests that are within the limit.

Examples The following example shows all the sessions currently blocked:

```
Router# show ip rsvp signalling blockade

To          From          Pro DPort Sport Time Left Rate
192.168.101.2 192.168.101.1 UDP 1000 1000 27      5K
192.168.101.2 192.168.101.1 UDP 1001 1001 79      5K
192.168.101.2 192.168.101.1 UDP 1002 1002 17      5K
225.1.1.1     192.168.104.1 UDP 2222 2222 48      5K
```

[Table 45](#) describes the fields shown in the display.

Table 45 show ip rsvp signalling blockade Command Field Descriptions

Field	Description
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol used.
DPort	Destination port number.
Sport	Source port number.
Time Left	Amount of time, in seconds, before the blockade expires.
Rate	The average rate, in bits per second, for the data.

The following example shows more detail about the sessions currently blocked:

```
Router# show ip rsvp signalling blockade detail

Session address: 192.168.101.2, port: 1000. Protocol: UDP
Sender address: 192.168.101.1, port: 1000
Admission control error location: 192.168.101.1
Flowspec that caused blockade:
  Average bitrate:      5K bits/second
  Maximum burst:       5K bytes
  Peak bitrate:        5K bits/second
  Minimum policed unit: 0 bytes
  Maximum packet size: 0 bytes
  Requested bitrate:   5K bits/second
  Slack:               0 milliseconds
  Blockade ends in:    99 seconds

Session address: 192.168.101.2, port: 1001. Protocol: UDP
Sender address: 192.168.101.1, port: 1001
Admission control error location: 192.168.101.1
Flowspec that caused blockade:
  Average bitrate:      5K bits/second
  Maximum burst:       5K bytes
  Peak bitrate:        5K bits/second
  Minimum policed unit: 0 bytes
  Maximum packet size: 0 bytes
  Requested bitrate:   5K bits/second
  Slack:               0 milliseconds
  Blockade ends in:    16 seconds

Session address: 192.168.101.2, port: 1002. Protocol: UDP
Sender address: 192.168.101.1, port: 1002
Admission control error location: 192.168.101.1
Flowspec that caused blockade:
  Average bitrate:      5K bits/second
  Maximum burst:       5K bytes
  Peak bitrate:        5K bits/second
  Minimum policed unit: 0 bytes
  Maximum packet size: 0 bytes
  Requested bitrate:   5K bits/second
  Slack:               0 milliseconds
  Blockade ends in:    47 seconds
```

```

Session address: 225.1.1.1, port: 2222. Protocol: UDP
Sender address: 192.168.104.1, port: 2222
Admission control error location: 192.168.101.1
Flowspec that caused blockade:
  Average bitrate:      5K bits/second
  Maximum burst:       5K bytes
  Peak bitrate:        5K bits/second
  Minimum policed unit: 0 bytes
  Maximum packet size: 0 bytes
  Requested bitrate:   5K bits/second
  Slack:               0 milliseconds
Blockade ends in:     124 seconds

```

Table 46 describes the fields shown in the display.

Table 46 *show ip rsvp signalling blockade detail Command Field Descriptions*

Field	Description
Session address	Destination IP address of the reservation affected by the blockade.
port	Destination port number of the reservation affected by the blockade.
Protocol	Protocol used by the reservation affected by the blockade; choices include User Datagram Protocol (UDP) and TCP.
Sender address	Source IP address of the reservation affected by the blockade.
port	Source port number of the reservation affected by the blockade.
Admission control error location	IP address of the router where the admission control error occurred.
Flowspec that caused blockade	Parameters for the flowspec that caused the blockade.
Average bitrate	The average rate, in bits per second, for the flowspec.
Maximum burst	The maximum burst size, in bytes, for the flowspec.
Peak bitrate	The peak rate, in bps, for the flowspec.
Minimum policed unit	The minimum policed unit, in bytes, for the flowspec.
Maximum packet size	The maximum packet size, in bytes, for the flowspec.
Requested bitrate	The requested rate, in bits per second, for the flowspec.
Slack	Time, in milliseconds, allocated to a router for scheduling delivery of packets.
Blockade ends in	Time, in seconds, until the blockade expires.

show ip rsvp signalling rate-limit

To display the Resource Reservation Protocol (RSVP) rate-limiting parameters, use the **show ip rsvp signalling rate-limit** command in EXEC mode.

show ip rsvp signalling rate-limit

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Examples The following command shows the rate-limiting parameters:

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

```
Rate Limiting:
  Max msgs per interval: 4
  Interval length (msec): 20
  Max queue size: 500
  Max msgs per second: 200
```

Table 47 describes the fields shown in the display.

Table 47 *show ip rsvp signalling rate-limit Command Field Descriptions*

Field	Description
Rate Limiting	The RSVP rate-limiting parameters in effect including the following: <ul style="list-style-type: none"> • Max msgs per interval = number of messages allowed to be sent per interval (timeframe). • Interval length (msecs) = interval (timeframe) length in milliseconds. • Max queue size = maximum size of the message queue in bytes. • Max msgs per second = maximum number of messages allowed to be sent per second.

Related Commands

Command	Description
clear ip rsvp signalling rate-limit	Clears (sets to zero) the number of messages that were dropped because of a full queue.
debug ip rsvp rate-limit	Displays debug messages for RSVP rate-limiting events.
ip rsvp signalling rate-limit	Controls the transmission rate for RSVP messages sent to a neighboring router during a specified amount of time.

show ip rsvp signalling refresh reduction

To display the Resource Reservation Protocol (RSVP) refresh-reduction parameters, use the **show ip rsvp signalling refresh reduction** command in EXEC mode.

show ip rsvp signalling refresh reduction

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	12.2(13)T	This command was introduced.

Examples The following command shows the refresh-reduction parameters:

```
Router# show ip rsvp signalling refresh reduction

Refresh Reduction:
  ACK delay (msec): 250
  Initial retransmit delay (msec): 1000
  Local epoch: 0xF2F6BC
  Message IDs: in use 1, total allocated 4, total freed 3
```

[Table 48](#) describes the fields shown in the display.

Table 48 *show ip rsvp signalling refresh reduction Command Field Descriptions*

Field	Description
Refresh Reduction	<p>The RSVP refresh-reduction parameters in effect including the following:</p> <ul style="list-style-type: none"> • ACK delay (msec) = how long in milliseconds before the receiving router sends an acknowledgment (ACK). • Initial retransmit delay (msec) = how long in milliseconds before the sending router retransmits a message. • Local epoch = the RSVP message number space ID (identifier); randomly generated each time a node reboots or the RSVP process restarts. • Message IDs = the number of message IDs in use, the total number allocated, and the total number available (freed).

Related Commands

Command	Description
clear ip rsvp signalling refresh reduction	Clears (sets to zero) the counters recording retransmissions and out-of-order messages.
ip rsvp signalling refresh reduction	Enables refresh reduction.

show ip rtp header-compression

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

show ip rtp header-compression [*interface-type interface-number*] [**detail**]

Syntax Description	<i>interface-type</i>	(Optional) The interface type and number.
	<i>interface-number</i>	
	detail	(Optional) Displays details of each connection.

Command Modes	User EXEC
	Privileged EXEC

Command History	Release	Modification
	11.3	This command was introduced.
	12.1(5)T	The command output was modified to include information related to the Distributed Compressed Real-Time Transport Protocol (dCRTP) feature.

Usage Guidelines The **detail** keyword is not available with the **show ip rtp header-compression** command on a Route Switch Processor (RSP). However, the **detail** keyword is available with the **show ip rtp header-compression** command on a Versatile Interface Processor (VIP). Enter the **show ip rtp header-compression interface-type interface-number detail** command on a VIP to retrieve detailed information regarding RTP header compression on a specific interface.

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

```
Router# show ip rtp header-compression

RTP/UDP/IP header compression statistics:
Interface Serial1:
  Rcvd: 0 total, 0 compressed, 0 errors
        0 dropped, 0 buffer copies, 0 buffer failures
  Sent: 430 total 429 compressed,
        15122 bytes saved, 139318 bytes sent
        1.10 efficiency improvement factor
  Connect: 16 rx slots, 16 tx slots, 1 long searches, 1 misses
           99% hit ratio, five minute miss rate 0 misses/sec, 0 max.
```

Table 49 describes the significant fields shown in the display.

Table 49 *show ip rtp header-compression Field Descriptions*

Field	Description
Interface Serial1	Type and number of interface.
Rcvd: total	Number of packets received on the interface.
compressed	Number of packets with compressed header.
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: total	Total number of packets sent.
compressed	Number of packets sent with compressed header.
bytes saved	Total savings in bytes due to compression.
bytes sent	Total bytes sent after compression.
efficiency improvement factor	Compression efficiency.
Connect: 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 existing states were revised.
five minute miss rate	Average miss rate.
max.	Maximum miss rate.

Related Commands

Command	Description
ip rtp compression-connections	Specifies the total number of RTP header compression connections supported on the interface.
ip rtp header-compression	Enables RTP header compression.

show policy-map

To display the configuration of all classes for a specified service policy map or all classes for all existing policy maps, use the **show policy-map** command in EXEC mode.

```
show policy-map [policy-map]
```

Syntax Description

<i>policy-map</i>	(Optional) The name of the service policy map whose complete configuration is to be displayed. The name can be a maximum of 40 characters.
-------------------	--

Defaults

All existing policy map configurations are displayed.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was incorporated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was incorporated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was incorporated into Cisco IOS Release 12.1(1)E.
12.2(4)T	This command was modified for two-rate traffic policing to display burst parameters and associated actions.
12.2(8)T	The command was modified for the Policer Enhancement—Multiple Actions feature and the WRED—Explicit Congestion Notification (ECN) feature.
12.2(13)T	The following modifications were made: <ul style="list-style-type: none"> The output was modified for the Percentage-Based Policing and Shaping feature. This command was modified as part of the Modular QoS CLI (MQC) Unconditional Packet Discard feature. Traffic classes can now be configured to discard packets belonging to a specified class. This command was modified for the Enhanced Packet Marking feature. A mapping table (table map) can now be used to convert and propagate packet-marking values.
12.2(15)T	This command was modified to support display of Frame Relay voice-adaptive traffic-shaping information.

Usage Guidelines

The **show policy-map** command displays the configuration of a policy map created using the **policy-map** command. You can use the **show policy-map** command to display all class configurations comprising any existing service policy map, whether or not that policy map has been attached to an interface.

The **show policy-map** command will display ECN marking information only if ECN is enabled on the interface.

Examples

The following example displays the contents of the service policy map called po1:

```
Router# show policy-map po1

Policy Map po1
  Weighted Fair Queueing
    Class class1
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class2
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class3
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class4
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class5
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class6
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class7
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class8
      Bandwidth 937 (kbps) Max thresh 64 (packets)
```

The following example displays the contents of all policy maps on the router:

```
Router# show policy-map

Policy Map poH1
  Weighted Fair Queueing
    Class class1
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class2
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class3
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class4
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class5
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class6
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class7
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class8
      Bandwidth 937 (kbps) Max thresh 64 (packets)
Policy Map policy2
  Weighted Fair Queueing
    Class class1
      Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class2
      Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class3
      Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class4
      Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class5
      Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class6
      Bandwidth 300 (kbps) Max thresh 64 (packets)
```

Table 50 describes the significant fields shown in the display.

Table 50 *show policy-map Field Descriptions*

Field	Description
Policy Map	Policy map name.
Class	Class name.
Bandwidth	Amount of bandwidth in kbps allocated to class.
Max thresh	Maximum threshold. Maximum Weighted Random Early Detection (WRED) threshold in number of packets.

Frame Relay Voice-Adaptive Traffic-Shaping Example

The following sample output for the **show-policy map** command indicates that Frame Relay voice-adaptive traffic-shaping is configured in the class-default class in the policy map “MQC-SHAPE-LLQ1” and that the deactivation timer is set to 30 seconds.

```
Router# show policy-map

  Policy Map VSD1
    Class VOICE1
      Strict Priority
      Bandwidth 10 (kbps) Burst 250 (Bytes)
    Class SIGNALS1
      Bandwidth 8 (kbps) Max Threshold 64 (packets)
    Class DATA1
      Bandwidth 15 (kbps) Max Threshold 64 (packets)

  Policy Map MQC-SHAPE-LLQ1
    Class class-default
      Traffic Shaping
        Average Rate Traffic Shaping
          CIR 63000 (bps) Max. Buffers Limit 1000 (Packets)
          Adapt to 8000 (bps)
          Voice Adapt Deactivation Timer 30 Sec
      service-policy VSD1
```

Table 51 describes the significant fields shown in the display.

Table 51 *show policy-map Field Descriptions—Configured for Frame Relay Voice-Adaptive Traffic-Shaping*

Field	Description
Strict Priority	Indicates the queueing priority assigned to the traffic in this class.
Burst	Specifies the traffic burst size in bytes.
Traffic Shaping	Indicates that Traffic Shaping is enabled.
Average Rate Traffic Shaping	Indicates the type of Traffic Shaping enabled. Choices are Peak Rate Traffic Shaping or Average Rate Traffic Shaping.
CIR	Committed Information Rate (CIR) in bps.
Max. Buffers Limit	Maximum memory buffer size in packets.

Table 51 *show policy-map Field Descriptions—Configured for Frame Relay Voice-Adaptive Traffic-Shaping (continued)*

Field	Description
Adapt to	Traffic rate when shaping is active.
Voice Adapt Deactivation Timer	Indicates that Frame Relay voice-adaptive traffic-shaping is configured, and that the deactivation timer is set to 30 seconds.
service-policy	Name of the service policy configured in the policy map “MQC-SHAPE-LLQ1”.

Two-Rate Traffic Policing show policy-map Command Example

The following is sample output from the **show policy-map** command when two-rate traffic policing has been configured. As shown below, two-rate traffic policing has been configured for a class called “police.” In turn, the class called police has been configured in a policy map called “policy1.” Two-rate traffic policing has been configured to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps.

```
Router(config)# class-map police
Router(config-cmap)# match access-group 101
Router(config-cmap)# policy-map policy1
Router(config-pmap)# class police
Router(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Router(config-pmap-c)# interface serial3/0
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial3/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
```

The following sample output shows the contents of the policy map called “policy1”:

```
Router# show policy-map policy1

Policy Map policy1
Class police
  police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
```

Traffic marked as conforming to the average committed rate (500 kbps) will be sent as is. Traffic marked as exceeding 500 kbps, but not exceeding 1 Mbps, will be marked with IP Precedence 2 and then sent. All traffic exceeding 1 Mbps will be dropped. The burst parameters are set to 10000 bytes.

[Table 52](#) describes the significant fields shown in the display.

Table 52 show policy-map Field Descriptions—Configured for Two-Rate Traffic Policing

Field	Description
police	Indicates that the police command has been configured to enable traffic policing. Also, displays the specified CIR, conform burst size (bc), peak information rate (PIR), and peak burst (BE) size used for marking packets.
conform-action	Displays the action to be taken on packets conforming to a specified rate.
exceed-action	Displays the action to be taken on packets exceeding a specified rate.
violate-action	Displays the action to be taken on packets violating a specified rate.

Multiple Traffic Policing Actions show policy-map Command Example

The following is sample output from the **show policy-map** command when the Policer Enhancement — Multiple Actions feature has been configured. The following sample output of the **show policy-map** command displays the configuration for a service policy called “police.” In this service policy, traffic policing has been configured to allow multiple actions for packets marked as conforming to, exceeding, or violating the CIR or the PIR shown in the example.

```
Router# show policy-map police

Policy Map police
Class class-default
  police cir 1000000 bc 31250 pir 2000000 be 31250
    conform-action transmit
    exceed-action set-prec-transmit 4
    exceed-action set-frde-transmit

    violate-action set-prec-transmit 2
    violate-action set-frde-transmit
```

Packets conforming to the specified CIR (1000000 bps) are marked as conforming packets. These are transmitted unaltered.

Packets exceeding the specified CIR (but not the specified PIR, 2000000 bps) are marked as exceeding packets. For these packets, the IP Precedence level is set to 4, the discard eligibility (DE) bit is set to 1, and the packet is transmitted.

Packets exceeding the specified PIR are marked as violating packets. For these packets, the IP Precedence level is set to 2, the DE bit is set to 1, and the packet is transmitted.

**Note**

Actions are specified by using the *action* argument of the **police** command. For more information about the available actions, see the [police](#) command reference page.

[Table 53](#) describes the significant fields shown in the display.

Table 53 show policy-map Field Descriptions—Configured for Multiple Traffic Policing Actions

Field	Description
police	Indicates that the police command has been configured to enable traffic policing. Also, displays the specified CIR, BC, PIR, and BE used for marking packets.
conform-action	Displays the one or more actions to be taken on packets conforming to a specified rate.
exceed-action	Displays the one or more actions to be taken on packets exceeding a specified rate.
violate-action	Displays the one or more actions to be taken on packets violating a specified rate.

Explicit Congestion Notification show policy-map Command Example

The following is sample output from the **show policy-map** command when the WRED — Explicit Congestion Notification (ECN) feature has been configured. The words “explicit congestion notification” (along with the ECN marking information) included in the output indicate that ECN has been enabled.

```
Router# show policy-map

Policy Map poll
  Class class-default
    Weighted Fair Queueing
      Bandwidth 70 (%)
      exponential weight 9
      explicit congestion notification
      class      min-threshold  max-threshold  mark-probability
      -----
      -----
      0          -              -              1/10
      1          -              -              1/10
      2          -              -              1/10
      3          -              -              1/10
      4          -              -              1/10
      5          -              -              1/10
      6          -              -              1/10
      7          -              -              1/10
      rsvp      -              -              1/10
```

Table 54 describes the significant fields shown in the display.

Table 54 show policy-map Field Descriptions—Configured for ECN

Field	Description
explicit congestion notification	Indication that Explicit Congestion Notification is enabled.
class	IP precedence value.

Table 54 show policy-map Field Descriptions—Configured for ECN (continued)

Field	Description
min-threshold	Minimum threshold. Minimum WRED threshold in number of packets.
max-threshold	Maximum threshold. Maximum WRED threshold in number of packets.
mark-probability	Fraction of packets dropped when the average queue depth is at the maximum threshold.

Modular QoS CLI (MQC) Unconditional Packet Discard show policy-map Command Example

The following example displays the contents of the policy map called “policy1.” All the packets belonging to the class called “c1” are discarded.

```
Router# show policy-map policy1

Policy Map policy1
  Class c1
    drop
```

Table 55 describes the significant fields shown in the display.

Table 55 show policy-map Field Descriptions—Configured for MQC Unconditional Packet Discard

Field	Description
Policy Map	Name of the policy map being displayed.
Class	Name of the class in the policy map being displayed.
drop	Indicates that the packet discarding action for all the packets belonging to the specified class has been configured.

Percentage-Based Policing and Shaping show policy-map Command Example

The following example displays the contents of two service policy maps—one called “policy1” and one called “policy2.” In policy1, traffic policing based on a CIR of 50 percent has been configured. In policy 2, traffic shaping based on an average rate of 35 percent has been configured.

```
Router# show policy-map policy1

Policy Map policy1
  class class1
    police cir percent 50

Router# show policy-map policy2

Policy Map policy2
  class class2
    shape average percent 35
```

The following example displays the contents of the service policy map called “po1”:

```
Router# show policy-map po1

Policy Map po1
  Weighted Fair Queueing
  Class class1
```

```

Bandwidth 937 (kbps) Max thresh 64 (packets)
  Class class2
    Bandwidth 937 (kbps) Max thresh 64 (packets)
  Class class3
    Bandwidth 937 (kbps) Max thresh 64 (packets)
  Class class4
    Bandwidth 937 (kbps) Max thresh 64 (packets)

```

The following example displays the contents of all policy maps on the router:

```

Router# show policy-map

Policy Map poH1
  Weighted Fair Queueing
    Class class1
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class2
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class3
      Bandwidth 937 (kbps) Max thresh 64 (packets)
    Class class4
      Bandwidth 937 (kbps) Max thresh 64 (packets)
Policy Map policy2
  Weighted Fair Queueing
    Class class1
      Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class2
      Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class3
      Bandwidth 300 (kbps) Max thresh 64 (packets)
    Class class4
      Bandwidth 300 (kbps) Max thresh 64 (packets)

```

Table 56 describes the significant fields shown in the display.

Table 56 *show policy-map Field Descriptions—Configured for Percentage-Based Policing and Shaping*

Field	Description
Policy Map	Name of policy map displayed.
Weighted Fair Queueing	Indicates that weighted fair queueing (WFQ) has been enabled.
Class	Name of class configured in policy map displayed.
Bandwidth	Bandwidth, in kbps, configured for this class.
Max threshold	Maximum threshold. Maximum WRED threshold in number of packets.

Enhanced Packet Marking show policy-map Command Example

The following sample output of the **show policy-map** command displays the configuration for policy maps called “policy1” and “policy2”.

In “policy1”, a table map called “table-map-cos1” has been configured to determine the precedence based on the class of service (CoS) value. Policy map “policy 1” converts and propagates the packet markings defined in the table map called “table-map-cos1”.

The following sample output of the **show policy-map** command displays the configuration for service polices called “policy1” and “policy2”. In “policy1”, a table map called “table-map1” has been configured to determine the precedence according to the CoS value. In “policy2”, a table map called “table-map2” has been configured to determine the CoS value according to the precedence value.

```

Router# show policy-map policy1

Policy Map policy1
  Class class-default
    set precedence cos table table-map1

Router# show policy-map policy2

Policy Map policy2
  Class class-default
    set cos precedence table table-map2
    
```

Table 57 describes the fields shown in the display.

Table 57 show policy-map Field Descriptions—Configured for Enhanced Packet Marking

Field	Description
Policy Map	Name of the policy map being displayed.
Class	Name of the class in the policy map being displayed.
set precedence cos table table-map1 or set cos precedence table table-map2	Name of the set command used to set the specified value. For instance, set precedence cos table-map1 indicates that a table map called “table-map1” has been configured to set the precedence value on the basis of the values defined in the table map. Alternately, set cos table table-map2 indicates that a table map called “table-map2” has been configured to set the CoS value on the basis of the values defined in the table map.

Related Commands

Command	Description
drop	Configures a traffic class to discard packets belonging to a specific class.
police	Configures traffic policing.
police (two rates)	Configures traffic policing using two rates, the CIR and the PIR.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
random-detect ecn	Enables ECN.
show policy-map class	Displays the configuration for the specified class of the specified policy map.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.
show table-map	Displays the configuration of a specified table map or of all table maps.
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

show policy-map class

To display the configuration for the specified class of the specified policy map, use the **show policy-map class** command in EXEC mode.

show policy-map *policy-map* **class** *class-name*

Syntax Description

<i>policy-map</i>	The name of a policy map that contains the class configuration to be displayed.
<i>class-name</i>	The name of the class whose configuration is to be displayed.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.

Usage Guidelines

You can use the **show policy-map class** command to display any single class configuration for any service policy map, whether or not the specified service policy map has been attached to an interface.

Examples

The following example displays configurations for the class called class7 that belongs to the policy map called po1:

```
Router# show policy-map po1 class class7

Class class7
  Bandwidth 937 (kbps) Max Thresh 64 (packets)
```

Related Commands

Command	Description
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the configuration of all classes configured for all service policies on the specified interface or displays the classes for the service policy for a specific PVC on the interface.

show policy-map interface

To display the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific permanent virtual circuit (PVC) on the interface, use the **show policy-map interface** command in EXEC mode.

```
show policy-map interface interface-name [vc [vpi] vci] [dlci dlci] [input | output]
```

Syntax Description

<i>interface-name</i>	Name of the interface or subinterface whose policy configuration is to be displayed.
vc	(Optional) For ATM interfaces only, shows the policy configuration for a specified PVC. The name can be up to 16 characters long.
<i>vpi</i>	(Optional) ATM network virtual path identifier (VPI) for this PVC. On the Cisco 7200 and 7500 series routers, this value ranges from 0 to 255. The <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.
<i>vci</i>	(Optional) ATM network virtual channel identifier (VCI) for this PVC. This value ranges from 0 to 1 less than the maximum value set for this interface by the atm vc-per-vc command. Typically, the lower values 0 to 31 are reserved for specific traffic (F4 Operation, Administration, and Maintenance (OAM), switched virtual circuit (SVC) signaling, Integrated Local Management Interface (ILMI), and so on) and should not be used. The VCI is a 16-bit field in the header of the ATM cell. The VCI value is unique only on a single link, not throughout the ATM network, because it has local significance only. The <i>vpi</i> and <i>vci</i> arguments cannot both be set to 0; if one is 0, the other cannot be 0.
dlci	(Optional) Indicates that a specific PVC for which policy configuration will be displayed.
<i>dlci</i>	(Optional) A specific data-link connection identifier (DLCI) number used on the interface. Policy configuration for the corresponding PVC will be displayed when a DLCI is specified.
input	(Optional) Indicates that the statistics for the attached input policy will be displayed.
output	(Optional) Indicates that the statistics for the attached output policy will be displayed.

Defaults

The absence of both the forward slash (/) and a *vpi* value defaults the *vpi* value to 0. If this value is omitted, information for all virtual circuits (VCs) on the specified ATM interface or subinterface is displayed.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was incorporated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was incorporated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was incorporated into Cisco IOS Release 12.1(1)E.
12.1(2)T	This command was modified to display information about the policy for all Frame Relay PVCs on the interface, or, if a DLCI is specified, the policy for that specific PVC. This command was also modified to display the total number of packets marked by the quality of service (QoS) set action.
12.1(3)T	This command was modified to display per-class accounting statistics.
12.2(4)T	This command was modified for two-rate traffic policing. It now can display burst parameters and associated actions.
12.2(8)T	The command was modified for the Policer Enhancement — Multiple Actions feature and the WRED — Explicit Congestion Notification (ECN) feature.
12.2(13)T	The following modifications were made: <ul style="list-style-type: none"> • The output was modified for the Percentage-Based Policing and Shaping feature. • This command was modified for the Class-Based RTP and TCP Header Compression feature. • This command was modified as part of the Modular QoS CLI (MQC) Unconditional Packet Discard feature. Traffic classes in policy maps can now be configured to discard packets belonging to a specified class. • This command was modified to display the Frame Relay DLCI number as a criterion for matching traffic inside a class map. • This command was modified to display Layer 3 packet length as a criterion for matching traffic inside a class map. • This command was modified for the Enhanced Packet Marking feature. A mapping table (table map) can now be used to convert and propagate packet-marking values.
12.2(15)T	This command was modified to support display of Frame Relay voice-adaptive traffic-shaping information.

Usage Guidelines

The **show policy-map interface** command displays the packet statistics for classes on the specified interface or the specified PVC only if a service policy has been attached to the interface or the PVC.

You can use the *interface-name* argument to display output for a PVC only for enhanced ATM port adapters (PA-A3) that support per-VC queueing.

The counters displayed after the **show policy-map interface** command is entered are updated only if congestion is present on the interface.

The **show policy-map interface** command will display policy information about Frame Relay PVCs only if Frame Relay Traffic Shaping (FRTS) is enabled on the interface.

The **show policy-map interface** command displays ECN marking information only if ECN is enabled on the interface.

Examples

This section provides sample output of a typical **show policy-map interface** command. Depending upon the interface in use and the options enabled, the output you see may vary slightly from the ones shown below. See [Table 58](#) for an explanation of the significant fields that commonly appear in the command output.

The following sample output of the **show policy-map interface** command displays the statistics for the serial 3/1 interface, to which a service policy called “mypolicy” (configured as shown below) is attached.

```
policy-map mypolicy
  class voice
    priority 128
  class gold
    bandwidth 100
  class silver
    bandwidth 80
    random-detect
```

```
Router# show policy-map output interface serial3/1
```

```
Serial3/1
```

```
Service-policy output: mypolicy
```

```
Class-map: voice (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: ip precedence 5
  Weighted Fair Queueing
    Strict Priority
    Output Queue: Conversation 264
    Bandwidth 128 (kbps) Burst 3200 (Bytes)
    (pkts matched/bytes matched) 0/0
    (total drops/bytes drops) 0/0

Class-map: gold (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: ip precedence 2
  Weighted Fair Queueing
    Output Queue: Conversation 265
    Bandwidth 100 (kbps) Max Threshold 64 (packets)
    (pkts matched/bytes matched) 0/0
    (depth/total drops/no-buffer drops) 0/0/0

Class-map: silver (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: ip precedence 1
  Weighted Fair Queueing
    Output Queue: Conversation 266
    Bandwidth 80 (kbps)
    (pkts matched/bytes matched) 0/0
    (depth/total drops/no-buffer drops) 0/0/0
    exponential weight: 9
    mean queue depth: 0
```

class	Transmitted pkts/bytes	Random drop pkts/bytes	Tail drop pkts/bytes	Minimum thresh	Maximum thresh	Mark prob
0	0/0	0/0	0/0	20	40	1/10
1	0/0	0/0	0/0	22	40	1/10
2	0/0	0/0	0/0	24	40	1/10
3	0/0	0/0	0/0	26	40	1/10
4	0/0	0/0	0/0	28	40	1/10

```

5          0/0          0/0          0/0          30          40 1/10
6          0/0          0/0          0/0          32          40 1/10
7          0/0          0/0          0/0          34          40 1/10
rsvp      0/0          0/0          0/0          36          40 1/10

```

```

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any

```

The following sample output of the **show policy-map interface** command displays the statistics for the serial 3/2 interface, to which a service policy called p1 (configured as shown below) is attached. Traffic shaping has been enabled on this interface.

```

policy-map p1
  class c1
    shape average 320000

```

```

Router# show policy-map output interface serial3/2

```

```

Serial3/2

```

```

Service-policy output: p1

```

```

Class-map: c1 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: ip precedence 0
  Traffic Shaping
    Target   Byte   Sustain  Excess   Interval  Increment Adapt
    Rate    Limit bits/int bits/int (ms)      (bytes)  Active
    320000  2000  8000    8000    25        1000     -

    Queue   Packets  Bytes   Packets  Bytes   Shaping
    Depth                                Delayed  Delayed  Active
    0        0        0        0        0        no

```

```

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any

```

[Table 58](#) describes the significant fields shown in the displays. The fields in the table are grouped according to the relevant QoS feature.

Table 58 show policy-map interface Field Descriptions ¹

Field	Description
Fields Associated with Classes or Service Policies	
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets and bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class. Note If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified <i>before</i> they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only <i>one</i> tunnel encapsulation, or may include the overhead for <i>all</i> tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Note	In distributed architecture platforms (such as the C7500), the value of the transfer rate, calculated as the difference between the offered rate and the drop rate counters, can sporadically deviate from the average by up to 20 percent or more. This can occur while no corresponding burst is registered by independent traffic analyser equipment.
Match	Match criteria specified for the class of traffic. Choices include criteria such as IP precedence, IP differentiated services code point (DSCP) value, Multiprotocol Label Switching (MPLS) experimental (EXP) value, access groups, and QoS groups. For more information about the variety of match criteria options available, refer to the chapter “Configuring the Modular Quality of Service Command-Line Interface” in the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> .
Fields Associated with Queuing (if Enabled)	
Output Queue	The weighted fair queuing (WFQ) conversation to which this class of traffic is allocated.
Bandwidth	Bandwidth, in either kbps or percentage, configured for this class and the burst size.

Table 58 show policy-map interface Field Descriptions ¹ (continued)

Field	Description
pkts matched/bytes matched	Number of packets (also shown in bytes) matching this class that were placed in the queue. This number reflects the total number of matching packets queued at any time. Packets matching this class are queued only when congestion exists. If packets match the class but are never queued because the network was not congested, those packets are not included in this total. However, if process switching is in use, the number of packets is always incremented even if the network is not congested.
depth/total drops/no-buffer drops	Number of packets discarded for this class. No-buffer indicates that no memory buffer exists to service the packet.
Fields Associated with Weighted Random Early Detection (WRED) (if Enabled)	
exponential weight	Exponent used in the average queue size calculation for a WRED parameter group.
mean queue depth	Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a fluctuating average. The minimum and maximum thresholds are compared against this value to determine drop decisions.
class	IP precedence level.
Transmitted pkts/bytes	Number of packets (also shown in bytes) passed through WRED and not dropped by WRED. Note If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped <i>after</i> the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as “no-buffer drops”) are not taken into account by the WRED packet counter.
Random drop pkts/bytes	Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence level.
Tail drop pkts/bytes	Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence level.
Minimum thresh	Minimum threshold. Minimum WRED threshold in number of packets.
Maximum thresh	Maximum threshold. Maximum WRED threshold in number of packets.
Mark prob	Mark probability. Fraction of packets dropped when the average queue depth is at the maximum threshold.
Fields Associated with Traffic Shaping (if Enabled)	
Target Rate	Rate used for shaping traffic.
Byte Limit	Maximum number of bytes that can be transmitted per interval. Calculated as follows: $((Bc+Be) / 8) \times 1$
Sustain bits/int	Committed burst (Bc) rate.
Excess bits/int	Excess burst (Be) rate.
Interval (ms)	Time interval value in milliseconds (ms).

Table 58 show policy-map interface Field Descriptions ¹ (continued)

Field	Description
Increment (bytes)	Number of credits (in bytes) received in the token bucket of the traffic shaper during each time interval.
Queue Depth	Current queue depth of the traffic shaper.
Packets	Total number of packets that have entered the traffic shaper system.
Bytes	Total number of bytes that have entered the traffic shaper system.
Packets Delayed	Total number of packets delayed in the queue of the traffic shaper before being transmitted.
Bytes Delayed	Total number of bytes delayed in the queue of the traffic shaper before being transmitted.
Shaping Active	Indicates whether the traffic shaper is active. For example, if a traffic shaper is active, and the traffic being sent exceeds the traffic shaping rate, a “yes” appears in this field.

1. A number in parentheses may appear next to the service-policy output name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

Frame Relay Voice-Adaptive Traffic-Shaping show policy interface Command Example

The following sample output shows that Frame Relay voice-adaptive traffic shaping is currently active and has 29 seconds left on the deactivation timer. With traffic shaping active and the deactivation time set, this means that the current sending rate on DLCI 201 is minCIR, but if no voice packets are detected for 29 seconds, the sending rate will increase to CIR.

```
Router# show policy interface Serial3/1.1

Serial3/1.1:DLCI 201 -

Service-policy output:MQC-SHAPE-LLQ1

Class-map:class-default (match-any)
 1434 packets, 148751 bytes
 30 second offered rate 14000 bps, drop rate 0 bps
Match:any
Traffic Shaping
  Target/Average   Byte   Sustain   Excess   Interval   Increment
  Rate             Limit  bits/int  bits/int  (ms)       (bytes)
  63000/63000     1890   7560     7560     120        945

  Adapt Queue    Packets  Bytes    Packets  Bytes    Shaping
  Active Depth   Delayed  Delayed  Active
  BECN 0         1434    162991  26       2704    yes
  Voice Adaptive Shaping active, time left 29 secs
```

Table 59 describes the significant fields shown in the display. Significant fields that are not described in Table 59 are described in Table 58, “show policy-map interface Field Descriptions.”

Table 59 *show policy-map interface Field Descriptions—Configured for Frame Relay Voice-Adaptive Traffic Shaping*

Field	Description
Voice Adaptive Shaping active/inactive	Indicates whether Frame Relay voice-adaptive traffic shaping is active or inactive.
time left	Number of seconds left on the Frame Relay voice-adaptive traffic shaping deactivation timer.

Two-Rate Traffic Policing show policy-map interface Command Example

The following is sample output from the **show policy-map interface** command when two-rate traffic policing has been configured. In the example below, 1.25 Mbps of traffic is sent (“offered”) to a policer class.

```
Router# show policy-map interface serial3/0
```

```
Serial3/0
```

```
Service-policy output: policy1
```

```
Class-map: police (match all)
```

```
148803 packets, 36605538 bytes
```

```
30 second offered rate 1249000 bps, drop rate 249000 bps
```

```
Match: access-group 101
```

```
police:
```

```
  cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
```

```
  conformed 59538 packets, 14646348 bytes; action: transmit
```

```
  exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
```

```
  violated 29731 packets, 7313826 bytes; action: drop
```

```
  conformed 499000 bps, exceed 500000 bps violate 249000 bps
```

```
Class-map: class-default (match-any)
```

```
19 packets, 1990 bytes
```

```
30 seconds offered rate 0 bps, drop rate 0 bps
```

```
Match: any
```

The two-rate traffic policer marks 500 kbps of traffic as conforming, 500 kbps of traffic as exceeding, and 250 kbps of traffic as violating the specified rate. Packets marked as conforming will be sent as is, and packets marked as exceeding will be marked with IP Precedence 2 and then sent. Packets marked as violating the specified rate are dropped.

Table 60 describes the significant fields shown in the display.

Table 60 show policy-map interface Field Descriptions—Configured for Two-Rate Traffic Policing

Field	Description
police	Indicates that the police command has been configured to enable traffic policing. Also, displays the specified CIR, conform burst size, peak information rate (PIR), and peak burst size used for marking packets.
conformed	Displays the action to be taken on packets conforming to a specified rate. Displays the number of packets and bytes on which the action was taken.
exceeded	Displays the action to be taken on packets exceeding a specified rate. Displays the number of packets and bytes on which the action was taken.
violated	Displays the action to be taken on packets violating a specified rate. Displays the number of packets and bytes on which the action was taken.

Multiple Traffic Policing Actions show policy-map interface Command Example

The following is sample output from the **show policy-map** command when the Policer Enhancement—Multiple Actions feature has been configured. The sample output of the **show policy-map interface** command displays the statistics for the serial 3/2 interface, to which a service policy called “police” (configured as shown below) is attached.

```

policy-map police
  class class-default
    police cir 1000000 pir 2000000
      conform-action transmit
      exceed-action set-prec-transmit 4
      exceed-action set-frde-transmit
      violate-action set-prec-transmit 2
      violate-action set-frde-transmit

Router# show policy-map interface serial13/2

Serial3/2: DLCI 100 -

Service-policy output: police

  Class-map: class-default (match-any)
    172984 packets, 42553700 bytes
    5 minute offered rate 960000 bps, drop rate 277000 bps
    Match: any
    police:
      cir 1000000 bps, bc 31250 bytes, pir 2000000 bps, be 31250 bytes
      conformed 59679 packets, 14680670 bytes; actions:
        transmit
      exceeded 59549 packets, 14649054 bytes; actions:
        set-prec-transmit 4
        set-frde-transmit
      violated 53758 packets, 13224468 bytes; actions:
        set-prec-transmit 2
        set-frde-transmit
      conformed 340000 bps, exceed 341000 bps, violate 314000 bps
  
```

The sample output of **show policy-map interface** command shows the following:

- 59679 packets were marked as conforming packets (that is, packets conforming to the CIR) and were transmitted unaltered.
- 59549 packets were marked as exceeding packets (that is, packets exceeding the CIR but not exceeding the PIR). Therefore, the IP Precedence value of these packets was changed to an IP Precedence level of 4, the discard eligibility (DE) bit was set to 1, and the packets were transmitted with these changes.
- 53758 packets were marked as violating packets (that is, exceeding the PIR). Therefore, the IP Precedence value of these packets was changed to an IP Precedence level of 2, the DE bit was set to 1, and the packets were transmitted with these changes.



Note

Actions are specified by using the *action* argument of the **police** command. For more information about the available actions, see the [police](#) command reference page.

[Table 61](#) describes the significant fields shown in the display.

Table 61 *show policy-map interface Field Descriptions—Configured for Multiple Traffic Policing Actions*

Field	Description
police	Indicates that the police command has been configured to enable traffic policing. Also, displays the specified CIR, conform burst size (BC), PIR, and peak burst size (BE) used for marking packets.
conformed, packets, bytes, actions	Displays the number of packets (also shown in bytes) marked as conforming to a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately.
exceeded, packets, bytes, actions	Displays the number of packets (also shown in bytes) marked as exceeding a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately.
violated, packets, bytes, actions	Displays the number of packets (also shown in bytes) marked as violating a specified rate and the actions taken on the packet. If there are multiple actions, each action is listed separately.

Explicit Congestion Notification show policy-map interface Command Example

The following is sample output from the **show policy-map interface** command when the WRED — Explicit Congestion Notification (ECN) feature has been configured. The words “explicit congestion notification” included in the output indicate that ECN has been enabled.

```
Router# show policy-map interface Serial4/1

Serial4/1

Service-policy output:policy_ecn
  Class-map:precl (match-all)
    1000 packets, 125000 bytes
    30 second offered rate 14000 bps, drop rate 5000 bps
  Match:ip precedence 1
  Weighted Fair Queueing
    Output Queue:Conversation 42
    Bandwidth 20 (%)
    Bandwidth 100 (kbps)
    (pkts matched/bytes matched) 989/123625
```

```
(depth/total drops/no-buffer drops) 0/455/0
exponential weight:9
explicit congestion notification
mean queue depth:0

class Transmitted Random drop Tail drop Minimum Maximum Mark
      pkts/bytes  pkts/bytes  pkts/bytes  threshold  threshold  probability
  0      0/0          0/0          0/0          20          40          1/10
  1    545/68125     0/0          0/0          22          40          1/10
  2      0/0          0/0          0/0          24          40          1/10
  3      0/0          0/0          0/0          26          40          1/10
  4      0/0          0/0          0/0          28          40          1/10
  5      0/0          0/0          0/0          30          40          1/10
  6      0/0          0/0          0/0          32          40          1/10
  7      0/0          0/0          0/0          34          40          1/10
rsvp    0/0          0/0          0/0          36          40          1/10
class  ECN Mark
      pkts/bytes
  0      0/0
  1    43/5375
  2      0/0
  3      0/0
  4      0/0
  5      0/0
  6      0/0
  7      0/0
rsvp    0/0
```

Table 62 describes the significant fields shown in the display.

Table 62 show policy-map interface Field Descriptions—Configured for ECN

Field	Description
explicit congestion notification	Indication that Explicit Congestion Notification is enabled.
mean queue depth	Average queue depth based on the actual queue depth on the interface and the exponential weighting constant. It is a moving average. The minimum and maximum thresholds are compared against this value to determine drop decisions.
class	IP precedence value.
Transmitted pkts/bytes	Number of packets (also shown in bytes) passed through WRED and not dropped by WRED. Note If there is insufficient memory in the buffer to accommodate the packet, the packet can be dropped <i>after</i> the packet passes through WRED. Packets dropped because of insufficient memory in the buffer (sometimes referred to as “no-buffer drops”) are not taken into account by the WRED packet counter.
Random drop pkts/bytes	Number of packets (also shown in bytes) randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP precedence value.
Tail drop pkts/bytes	Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP precedence value.
Minimum threshold	Minimum WRED threshold in number of packets.

Table 62 show policy-map interface Field Descriptions—Configured for ECN (continued)

Field	Description
Maximum threshold	Maximum WRED threshold in number of packets.
Mark probability	Fraction of packets dropped when the average queue depth is at the maximum threshold.
ECN Mark pkts/bytes	Number of packets (also shown in bytes) marked by ECN.

Class-Based RTP and TCP Header Compression show policy-map interface Command Example

The following sample output of the **show policy-map interface** command shows the RTP header compression has been configured for a class called “prec2” in the policy map called “p1”.

The **show policy-map interface** command output displays the type of header compression configured (RTP), the interface to which the policy map called “p1” is attached (Serial 4/1), the total number of packets, the number of packets compressed, the number of packets saved, the number of packets sent, and the rate at which the packets were compressed (in bits per second (bps)).

In this example, User Datagram Protocol (UDP)/RTP header compressions have been configured, and the compression statistics are included at the end of the display.

```
Router# show policy-map interface Serial 4/1

Serial4/1

Service-policy output:p1

  Class-map:class-default (match-any)
    1005 packets, 64320 bytes
    30 second offered rate 16000 bps, drop rate 0 bps
    Match:any
  compress:
    header ip rtp
    UDP/RTP Compression:
    Sent:1000 total, 999 compressed,
      41957 bytes saved, 17983 bytes sent
      3.33 efficiency improvement factor
      99% hit ratio, five minute miss rate 0 misses/sec, 0 max
      rate 5000 bps
```

[Table 63](#) describes the significant fields shown in the display.

Table 63 show policy-map interface Field Descriptions—Configured for Class-Based RTP and TCP Header Compression¹

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.

Table 63 *show policy-map interface Field Descriptions—Configured for Class-Based RTP and TCP Header Compression¹ (continued)*

Field	Description
offered rate	Rate, in kbps, of packets coming in to the class. Note If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified <i>before</i> they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only <i>one</i> tunnel encapsulation, or may include the overhead for <i>all</i> tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
UDP/RTP Compression	Indicates that RTP header compression has been configured for the class.
Sent total	Count of every packet sent, both compressed packets and full-header packets.
Sent compressed	Count of number of compressed packets sent.
bytes saved	Total number of bytes saved (that is, bytes not needing to be sent).
bytes sent	Total number of bytes sent for both compressed and full-header packets.
efficiency improvement factor	The percentage of increased bandwidth efficiency as a result of header compression. For example, with RTP streams, the efficiency improvement factor can be as much as 2.9 (or 290 percent).
hit ratio	Used mainly for troubleshooting purposes, this is the percentage of packets found in the context database. In most instances, this percentage should be high.
five minute miss rate	The number of new traffic flows found in the last five minutes.
misses/sec max	The average number of new traffic flows found per second, and the highest rate of new traffic flows to date.
rate	The actual traffic rate (in bits per second) after the packets are compressed.

1. A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

Modular QoS CLI (MQC) Unconditional Packet Discard show policy-map interface Command Example

The following sample output of the **show policy-map interface** command displays the statistics for the Serial2/0 interface, to which a policy map called “policy1” is attached. The discarding action has been specified for all the packets belonging to a class called “c1.” In this example, 32000 bps of traffic is sent (“offered”) to the class and all of them are dropped. Therefore, the drop rate shows 32000 bps.

```
Router# show policy-map interface Serial2/0

Serial2/0

Service-policy output: policy1

Class-map: c1 (match-all)
  10184 packets, 1056436 bytes
  5 minute offered rate 32000 bps, drop rate 32000 bps
Match: ip precedence 0
drop
```

Table 64 describes the significant fields shown in the display.

Table 64 *show policy-map interface Field Descriptions—Configured for MQC Unconditional Packet Discard¹*

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class. Note If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified <i>before</i> they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only <i>one</i> tunnel encapsulation, or may include the overhead for <i>all</i> tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.

Table 64 *show policy-map interface Field Descriptions—Configured for MQC Unconditional Packet Discard¹ (continued)*

Field	Description
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Match	Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and QoS groups. For more information about the variety of match criteria options available, refer to the chapter “Configuring the Modular Quality of Service Command-Line Interface” in the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> .
drop	Indicates that the packet discarding action for all the packets belonging to the specified class has been configured.

1. A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

Percentage-Based Policing and Shaping show policy-map interface Command Example

The following sample output of the **show policy-map interface** command shows traffic policing configured using a CIR based on a bandwidth of 20 percent. The CIR and committed burst (Bc) in milliseconds (ms) are included in the display.

```
Router# show policy-map interface Serial3/1

Serial3/1

Service-policy output: mypolicy

Class-map: gold (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
  police:
    cir 20 % bc 10 ms
    cir 2000000 bps, bc 2500 bytes
    pir 40 % be 20 ms
    pir 4000000 bps, be 10000 bytes
  conformed 0 packets, 0 bytes; actions:
  transmit
  exceeded 0 packets, 0 bytes; actions:
  drop
  violated 0 packets, 0 bytes; actions:
  drop
  conformed 0 bps, exceed 0 bps, violate 0 bps
```

Table 65 describes the significant fields shown in the display.

Table 65 show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping¹

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class. Note If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified <i>before</i> they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only <i>one</i> tunnel encapsulation, or may include the overhead for <i>all</i> tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
police	Indicates that traffic policing based on a percentage of bandwidth has been enabled. Also, displays the bandwidth percentage, the CIR, and the committed burst (Bc) size in ms.
conformed, actions	Displays the number of packets and bytes marked as conforming to the specified rates, and the action to be taken on those packets.
exceeded, actions	Displays the number of packets and bytes marked as exceeding the specified rates, and the action to be taken on those packets.

1. A number in parentheses may appear next to the service-policy output name and the class-map name. The number is for Cisco internal use only and can be disregarded.

The second sample output of the **show policy-map interface** command (shown below) displays the statistics for the serial 3/2 interface. Traffic shaping has been enabled on this interface, and an average rate of 20 percent of the bandwidth has been specified.

```
Router# show policy-map interface Serial3/2

Serial3/2

Service-policy output: p1

Class-map: c1 (match-all)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match: any
```

```

Traffic Shaping
Target/Average      Byte   Sustain   Excess      Interval  Increment  Adapt
Rate                Limit  bits/int  bits/int    (ms)      (bytes)    Active
  20 %
201500/201500      1952   7808      7808        38         976        -

Queue   Packets  Bytes   Packets  Bytes   Shaping
Depth   Delayed  Delayed  Active
0        0        0        0        0        no
    
```

Table 66 describes the significant fields shown in the display.

Table 66 *show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping (with Traffic Shaping Enabled)¹*

Field	Description
Service-policy output	Name of the output service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class. Note If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified <i>before</i> they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only <i>one</i> tunnel encapsulation, or may include the overhead for <i>all</i> tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Match	Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and quality of service (QoS) groups. For more information about the variety of match criteria options that are available, refer to the chapter “Configuring the Modular Quality of Service Command-Line Interface” in the <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> , Release 12.2.
Traffic Shaping	Indicates that traffic shaping based on a percentage of bandwidth has been enabled.
Target /Average Rate	Rate (percentage) used for shaping traffic and the number of packets meeting that rate.

Table 66 show policy-map interface Field Descriptions—Configured for Percentage-Based Policing and Shaping (with Traffic Shaping Enabled)¹ (continued)

Field	Description
Byte Limit	Maximum number of bytes that can be transmitted per interval. Calculated as follows: $((Bc+Be) / 8) \times 1$
Sustain bits/int	Committed burst (Bc) rate.
Excess bits/int	Excess burst (Be) rate.
Interval (ms)	Time interval value in milliseconds (ms).
Increment (bytes)	Number of credits (in bytes) received in the token bucket of the traffic shaper during each time interval.
Adapt Active	Indicates whether adaptive shaping is enabled.
Queue Depth	Current queue depth of the traffic shaper.
Packets	Total number of packets that have entered the traffic shaper system.
Bytes	Total number of bytes that have entered the traffic shaper system.
Packets Delayed	Total number of packets delayed in the queue of the traffic shaper before being transmitted.
Bytes Delayed	Total number of bytes delayed in the queue of the traffic shaper before being transmitted.
Shaping Active	Indicates whether the traffic shaper is active. For example, if a traffic shaper is active, and the traffic being sent exceeds the traffic shaping rate, a “yes” appears in this field.

1. A number in parentheses may appear next to the service-policy output name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

Packet Classification Based on Layer 3 Packet Length show policy-map interface Example

The following sample output of the **show policy-map interface** command displays the packet statistics for the Ethernet4/1 interface, to which a service policy called “mypolicy” is attached. The Layer 3 packet length has been specified as a match criterion for the traffic in the class called “class1”.

```
Router# show policy-map interface Ethernet4/1

Ethernet4/1

Service-policy input: mypolicy

Class-map: class1 (match-all)
  500 packets, 125000 bytes
  5 minute offered rate 4000 bps, drop rate 0 bps
  Match: packet length min 100 max 300
  QoS Set
    qos-group 20
    Packets marked 500
```

Table 67 describes the significant fields shown in the display.

Table 67 *show policy-map interface Field Descriptions—Configured for Packet Classification Based on Layer 3 Packet Length¹*

Field	Description
Service-policy input	Name of the input service policy applied to the specified interface or VC.
Class-map	Class of traffic being displayed. Output is displayed for each configured class in the policy. The choice for implementing class matches (for example, match-all or match-any) can also appear next to the traffic class.
packets, bytes	Number of packets (also shown in bytes) identified as belonging to the class of traffic being displayed.
offered rate	Rate, in kbps, of packets coming in to the class. Note If the packets are compressed over an outgoing interface, the improved packet rate achieved by packet compression is not reflected in the offered rate. Also, if the packets are classified <i>before</i> they enter a combination of tunnels (for example, a generic routing encapsulation (GRE) tunnel and an IP Security (IPSec) tunnel), the offered rate does not include all the extra overhead associated with tunnel encapsulation in general. Depending on the configuration, the offered rate may include no overhead, may include the overhead for only <i>one</i> tunnel encapsulation, or may include the overhead for <i>all</i> tunnel encapsulations. In most of the GRE and IPSec tunnel configurations, the offered rate includes the overhead for GRE tunnel encapsulation only.
drop rate	Rate, in kbps, at which packets are dropped from the class. The drop rate is calculated by subtracting the number of successfully transmitted packets from the offered rate.
Match	Match criteria specified for the class of traffic. Choices include criteria such as the Layer 3 packet length, IP precedence, IP DSCP value, MPLS experimental value, access groups, and QoS groups.
QoS Set, qos-group, Packets marked	Indicates that class-based packet marking based on the QoS group has been configured. Includes the qos-group number and the number of packets marked.

1. A number in parentheses may appear next to the service-policy input name, class-map name, and match criteria information. The number is for Cisco internal use only and can be disregarded.

Enhanced Packet Marking show policy-map interface Example

The sample output of the **show table-map** command shows the contents of a table map called “map 1.” In “map1”, a “to–from” relationship has been established and a default value has been defined. The fields for establishing the “to–from” mappings are further defined by the policy map in which the table map will be configured. (Configuring a policy map is the next logical step after creating a table map.)

For instance, a precedence or DSCP value of 0 could be mapped to a class of service (CoS) value of 1, or vice versa, depending on the how the values are defined in the table map. Any values not explicitly defined in a “to–from” relationship will be set to a default value.

The following sample output of the **show table-map** command displays the contents of a table map called “map1”. In this table map, a packet-marking value of 0 is mapped to a packet-marking value of 1. All other packet-marking values are mapped to the default value 3.

```
Router# show table-map map1
```

```
Table Map map1
from 0 to 1
default 3
```

Table 68 describes the fields shown in the display.

Table 68 show policy-map interface Field Descriptions—Configured for Enhanced Packet Marking

Field	Description
Table Map	The name of the table map being displayed.
from, to	The values of the “to–from” relationship established by the table-map (value mapping) command and further defined by the policy map in which the table map will be configured.
default	The default action to be used for any values not explicitly defined in a “to–from” relationship by the table-map (value mapping) command. If a default action is not specified in the table-map (value mapping) command, the default action is “copy”.

Related Commands

Command	Description
compression header ip	Configures RTP or TCP IP header compression for a specific class.
drop	Configures a traffic class to discard packets belonging to a specific class.
match fr-dlci	Specifies the Frame Relay DLCI number as a match criterion in a class map.
match packet length (class-map)	Specifies the length of the Layer 3 packet in the IP header as a match criterion in a class map.
police	Configures traffic policing.
police (percent)	Configures traffic policing based on a percentage of bandwidth available on an interfaces.
police (two rates)	Configures traffic policing using two rates, the CIR and the PIR.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
random-detect ecn	Enables ECN.
shape (percent)	Specifies average or peak rate traffic shaping based on a percentage of bandwidth available on an interface.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map class	Displays the configuration for the specified class of the specified policy map.
show table-map	Displays the configuration of a specified table map or of all table maps.
table-map (value mapping)	Creates and configures a mapping table for mapping and converting one packet-marking value to another.

show qdm status

To view the status of the Quality of Service Device Manager (QDM) clients connected to the router, use the **show qdm status** command in EXEC mode.

show qdm status

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	Release 12.1(1)E	This command was introduced.
	Release 12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Usage Guidelines Use the **show qdm status** command to obtain the following information:

- Number of connected QDM clients
- Client IDs of the connected QDM clients
- Version of the QDM client software
- IP addresses of the connected QDM clients

Examples The following example illustrates the **show qdm status** output when two QDM clients are connected to the router:

```
Router# show qdm status

Number of QDM Clients :2
QDM Client v1.0(0.13)-System_1 @ 172.16.0.0 (id:30)
    connected since 09:22:36 UTC Wed Mar 15 2000
QDM Client v1.0(0.12)-System_2 @ 172.31.255.255 (id:29)
    connected since 17:10:23 UTC Tue Mar 14 2000
```

Related Commands	Command	Description
	disconnect qdm	Disconnects a QDM client.