ip nbar port-map

To configure Network-Based Application Recognition (NBAR) to search for a protocol or protocol name using a port number other than the well-known port, use the **ip nbar port-map** global configuration command. To look for the protocol name using only the well-known port number, use the **no** form of this command.

ip nbar port-map *protocol-name* [**tcp** | **udp**] *port-number*

no ip nbar port-map *protocol-name* [**tcp** | **udp**] *port-number*

Syntax Description

protocol-name	Name of protocol known to NBAR.
tcp	(Optional) Specifies that a TCP port will be searched for the specified *protocol-name* argument.
udp	(Optional) Specifies that a UDP port will be searched for the specified *protocol-name* argument.
port-number	Assigned port for named protocol. The *port-number* argument is either a UDP or a TCP port number, depending on which protocol is specified in this command line. Up to 16 *port-number* arguments can be specified in one command line. Port number values can range from 0 to 65535.

Defaults

This command has no default behavior or values.

Command Modes

Global configuration

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.

Usage Guidelines

This command is used in global configuration mode to tell NBAR to look for the protocol or protocol name, using a port number or numbers other than the well-known Internet Assigned Numbers Authority (IANA)-assigned) port number. For example, use this command to configure NBAR to look for Telnet on a port other than 23. Up to 16 ports can be specified with this command. Port number values can range from 0 to 65535.

Examples

The following example configures NBAR to look for the protocol SQL*NET on port numbers 63000 and 63001 instead of on the well-known port number:

```
ip nbar port-map sqlnet tcp 63000 63001
```

Related Commands

Command	Description
show ip nbar port-map	Displays the current protocol-to-port mappings in use by NBAR.

ip nbar protocol-discovery

To configure Networked-Based Application Recognition (NBAR) to discover traffic for all protocols known to NBAR on a particular interface, use the **ip nbar protocol-discovery** interface configuration command. To disable traffic discovery, use the **no** form of this command.

ip nbar protocol-discovery

no ip nbar protocol-discovery

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default behavior or values.

Command Modes

Interface configuration

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.

Usage Guidelines

Use the **ip nbar protocol-discovery** command to configure NBAR to keep traffic statistics for all protocols known to NBAR. Protocol discovery provides an easy way to discover application protocols transiting an interface so that QoS policies can be developed and applied. The Protocol Discovery feature discovers any protocol traffic supported by NBAR. Protocol discovery can be used to monitor both input and output traffic and may be applied with or without a service policy enabled.

Examples

The following example configures protocol discovery on an Ethernet interface:

```
interface ethernet 1/3
ip nbar protocol-discovery
```

Related Commands

Command	Description
show ip nbar protocol-discovery	Displays the statistics gathered by the NBAR Protocol Discovery feature.

ip rsvp atm-peak-rate-limit

To set a limit on the peak cell rate (PCR) of reservations for all newly created Resource Reservation Protocol (RSVP) switched virtual circuits (SVCs) established on the current interface or any of its subinterfaces, use the **ip rsvp atm-peak-rate-limit** interface configuration command. To remove the current peak rate limit, in which case the reservation peak rate is limited by the line rate, use the **no** form of this command.

ip rsvp atm-peak-rate-limit *limit*

no ip rsvp atm-peak-rate-limit

Syntax Description

limit	The peak rate limit of the reservation specified, in KB. The minimum value allowed is 1 KB; the maximum value allowed is 2 GB.

Defaults

The peak rate of a reservation defaults to the line rate.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Each RSVP reservation corresponds to an ATM SVC with a certain PCR, sustainable cell rate (SCR), and maximum burst size. The PCR, also referred to as the peak rate, can be configured by the user or allowed to default to the line rate.

RSVP controlled-load reservations do not define any peak rate for the data. By convention, the allowable peak rate in such reservations is taken to be infinity, which is usually represented by a very large number. Under these circumstances, when a controlled-load reservation is converted to an ATM SVC, the PCR for the SVC becomes correspondingly large and may be out of range for the switch. You can use the **ip rsvp atm-peak-rate-limit** command to limit the peak rate.

The following conditions determine the peak rate limit on the RSVP SVC:

- The peak rate defaults to the line rate.
- If the peak rate is greater than the configured peak rate limiter, the peak rate is lowered to the peak rate limiter.
- The peak rate cannot be less than the reservation bandwidth. If this is the case, the peak rate is raised to the reservation bandwidth.

Note Bandwidth conversions applied to the ATM space from the RSVP space are also applied to the peak rate.

The peak rate limit is local to the router; it does not affect the normal messaging of RSVP. Only the SVC setup is affected. Large peak rates are sent to the next host without modification.

For RSVP SVCs established on subinterfaces, the peak rate limit applied to the subinterface takes effect on all SVCs created on that subinterface. If a peak rate limit is applied to the main interface, the rate limit has no effect on SVCs created on a subinterface of the main interface even if the limit value on the main interface is lower than the limit applied to the subinterface.

For a given interface or subinterface, a peak rate limit applied to that interface affects only new SVCs created on the interface, not existing SVCs.

Note This command is available only on interfaces that support the **ip rsvp svc-required** command.

Use the **show ip rsvp atm-peak-rate-limit** command to determine the peak rate limit set for an interface or subinterface, if one is configured.

Examples

The following example sets the peak rate limit for interface atm2/0/0.1 to 100 KB:

```
interface atm2/0/0.1
 ip rsvp atm-peak-rate-limit 100
```

Related Commands

Command	Description
ip rsvp svc-required	Enables creation of an SVC to service any new RSVP reservation made on the interface or subinterface.
show ip rsvp atm-peak-rate-limit	Displays the current peak rate limit set for an interface.
show ip rsvp interface	Displays RSVP-related interface information.

ip rsvp bandwidth

To enable Resource Reservation Protocol (RSVP) for IP on an interface, use the **ip rsvp bandwidth** interface configuration command. To disable RSVP, use the **no** form of this command.

ip rsvp bandwidth [*interface-kbps* [*single-flow-kbps*]]

no ip rsvp bandwidth [*interface-kbps* [*single-flow-kbps*]]

Syntax Description

interface-kbps	(Optional) Maximum amount of bandwidth, in kbps, that may be allocated by RSVP flows. The range is from 1 to 10,000,000.
single-flow-kbps	(Optional) Maximum amount of bandwidth, in kbps, that may be allocated to a single flow. The range is from 1 to 10,000,000.

Defaults

RSVP is disabled by default. If the **ip rsvp bandwidth** command is entered but no bandwidth values are supplied (for example, **ip rsvp bandwidth** is entered followed by a carriage return, or pressing the Return or Enter key), a default bandwidth value is assumed for both the i*nterface-kbps* and *single-flow-kbps* arguments.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

RSVP is disabled by default to allow backward compatibility with systems that do not implement RSVP. Weighted Random Early Detection (WRED) or fair queueing must be enabled first.

Examples

The following example shows a T1 (1536 kbps) link configured to permit RSVP reservation of up to 1158 kbps, but no more than 100 kbps for any given flow on serial interface 0. Fair queueing is configured with 15 reservable queues to support those reserved flows, should they be required.

```
interface serial 0
 fair-queue 64 256 15
 ip rsvp bandwidth 1158 100
```

Related Commands

Command	Description
fair-queue (WFQ)	Enables WFQ for an interface.
ip rsvp neighbor	Enables neighbors to request a reservation.
ip rsvp reservation	Enables a router to simulate receiving and forwarding RSVP RESV messages.
ip rsvp sender	Enables a router to simulate receiving and forwarding RSVP PATH messages.
ip rsvp udp-multicasts	Instructs the router to generate UDP-encapsulated RSVP multicasts whenever it generates an IP-encapsulated multicast packet.
random-detect (interface)	Enables WRED or DWRED.
show ip rsvp installed	Displays RSVP-related installed filters and corresponding bandwidth information.
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp neighbor	Displays current RSVP neighbors.
show ip rsvp reservation	Displays RSVP-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.

ip rsvp burst policing

To configure a burst factor within the Resource Reservation Protocol (RSVP) token bucket policer on a per-interface basis, use the **ip rsvp burst policing** interface configuration command. To return to the default value, enter the **no** form of this command.

ip rsvp burst policing [*factor*]

no ip rsvp burst policing

Syntax Description

factor	(Optional) Indicates a burst factor value as a percentage of the requested burst of the receiver.

Defaults

The default value is 200; the minimum value is 100, and the maximum value is 700.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

You configure the burst police factor per interface, not per flow. The burst factor controls how strictly or loosely the traffic of the sender is policed with respect to burst.

The burst factor applies to all RSVP flows installed on a specific interface. You can configure each interface independently for burst policing.

Examples

Here is an example of the **ip rsvp burst policing** command with a burst factor of 200:

```
ip rsvp burst policing 200
```

ip rsvp dsbm candidate

To configure an interface as a Designated Subnetwork Bandwidth Manager (DSBM) candidate, use the **ip rsvp dsbm candidate** interface configuration command. To disable DSBM on an interface, which exempts the interface as a DSBM candidate, use the **no** form of this command.

ip rsvp dsbm candidate [*priority*]

no ip rsvp dsbm candidate

Syntax Description

priority	(Optional) A value in the range from 64 to 128. Among contenders for the DSBM, the interface with the highest priority number wins the DSBM election process.

Defaults

An interface is not configured as a DSBM contender by default. If you use this command to enable the interface as a DSBM candidate and you do not specify a priority, the default priority of 64 is assumed.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

SBM protocol entities, any one of which can manage resources on a segment, can reside in Layer 2 or Layer 3 devices. Many SBM-capable devices may be attached to a shared Layer 2 segment. When more than one SBM exists on a given segment, one of the SBMs is elected to be the DSBM. The elected DSBM is responsible for exercising admission control over requests for resource reservations on a segment, which, in the process, becomes a managed segment. A managed segment includes those interconnected parts of a shared LAN that are not separated by DSBMs. In all circumstances, only one, if any, DSBM exists for each Layer 2 segment.

You can configure an interface to have a DSBM priority in the range from 64 to 128. You can exempt an interface from participation in the DSBM election on a segment but still allow the system to interact with the DSBM if a DSBM is present on the segment. In other words, you can allow a Resource Reservation Protocol (RSVP)-enabled interface on a router connected to a managed segment to be managed by the DSBM even if you do not configure that interface to participate as a candidate in the DSBM election process. To exempt an interface from DSBM candidacy, do not issue the **ip rsvp dsbm candidate** command on that interface.

RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

Examples

The following example configures Ethernet interface 2 as a DSBM candidate with a priority of 100:

```
interface Ethernet2
 ip rsvp dsbm candidate 100
```

Related Commands

Command	Description
debug ip rsvp	Displays information about SBM message processing, the DSBM election process, and standard RSVP enabled message processing information
debug ip rsvp detail	Displays detailed information about RSVP and SBM.
debug ip rsvp detail sbm	Display detailed information about SBM messages only, and SBM and DSBM state transitions
ip rsvp dsbm non-resv-send-limit	Configures the NonResvSendLimit object parameters.
show ip rsvp sbm	Displays information about an SBM configured for a specific RSVP-enabled interface or for all RSVP-enabled interfaces on the router.

ip rsvp dsbm non-resv-send-limit

To configure the NonResvSendLimit object parameters, use the **ip rsvp dsbm non-resv-send-limit** interface configuration command. To use the default NonResvSendLimit object parameters, use the **no** form of this command.

ip rsvp dsbm non-resv-send-limit {**rate** *kbps* | **burst** *kilobytes* | **peak** *kbps* | **min-unit** *bytes* | **max-unit** *bytes*}

no ip rsvp dsbm non-resv-send-limit {**rate** *kbps* | **burst** *kilobytes* | **peak** *kbps* | **min-unit** *bytes* | **max-unit** *bytes*}

Syntax Description

rate *kbps*	The average rate, in kBps, for the Designated Subnetwork Bandwidth Manager (DSBM) candidate.
burst *kilobytes*	The maximum burst size, in KB, for the DSBM candidate.
peak *kbps*	The peak rate, in kBps, for the DSBM candidate.
min-unit *bytes*	The minimum policed unit, in bytes, for the DSBM candidate.
max-unit *bytes*	The maximum packet size, in bytes, for the DSBM candidate.

Defaults

The default for the **rate**, **burst**, **peak**, **min-unit**, and **max-unit** keywords is unlimited; all traffic can be sent without a valid Resource Reservation Protocol (RSVP) reservation.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(1)	This command was introduced.

Usage Guidelines

To configure the per-flow limit on the amount of traffic that can be sent without a valid RSVP reservation, configure the **rate**, **burst**, **peak**, **min-unit**, and **max-unit** values for finite values greater than 0.

To allow all traffic to be sent without a valid RSVP reservation, configure the **rate**, **burst**, **peak**, **min-unit**, and **max-unit** values for unlimited traffic. To configure the parameters for unlimited traffic, you can either omit the command, or enter the **no** form of the command (for example, **no ip rsvp dsbm non-resv-send-limit rate**). Unlimited is the default value.

The absence of the NonResvSendLimit object allows any amount of traffic to be sent without a valid RSVP reservation.

RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

Examples

The following example configures Ethernet interface 2 as a DSBM candidate with a priority of 100, an average rate of 500 kBps, a maximum burst size of 1000 KB, a peak rate of 500 kBps, and unlimited minimum and maximum packet sizes:

```
interface Ethernet2
 ip rsvp dsbm candidate 100
 ip rsvp dsbm non-resv-send-limit rate 500
 ip rsvp dsbm non-resv-send-limit burst 1000
 ip rsvp dsbm non-resv-send-limit peak 500
```

Related Commands

Command	Description
ip rsvp dsbm candidate	Configures an interface as a DSBM candidate.
show ip rsvp sbm	Displays information about an SBM configured for a specific RSVP-enabled interface or for all RSVP-enabled interfaces on the router.

ip rsvp flow-assist

To enable Resource Reservation Protocol (RSVP) to attach itself to NetFlow so that it can leverage NetFlow services to obtain flow classification information about packets in order to update its token bucket and set IP Precedence as required, use the **ip rsvp flow-assist** interface configuration command. To detach RSVP from NetFlow, use the **no** form of this command.

ip rsvp flow-assist

no ip rsvp flow-assist

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default behavior or values. (RSVP does not use NetFlow as a packet filtering mechanism.)

Command Modes

Interface configuration

Command History

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

Usage Guidelines

For RSVP to maintain token buckets and set IP Precedence on packets traversing the flow, it must interact with the underlying packet forwarding mechanism in order to obtain the information it needs. RSVP uses NetFlow for this purpose.

If RSVP is used on non-ATM links and RSVP must set IP Precedence without relying on traffic policing, weighted fair queueing (WFQ) cannot be used. In this case, a method of attaching RSVP to the underlying forwarding mechanism is required. The **ip rsvp flow-assist** command satisfies this requirement. It allows RSVP to attach itself to NetFlow so that it can use NetFlow to obtain information about packets, which it can then use to update its token bucket and set IP Precedence. NetFlow does not police packets or flows. For this reason, when RSVP is configured in this mode, it can only set IP Precedence and not otherwise police traffic.

In summary, you should use this command only when all of the following conditions exist:

- You want to set IP Precedence and type of service (ToS) bits using the **ip rsvp precedence** command or the **ip rsvp tos** command.
- You are not running WFQ on the interface.
- You are not running ATM or you have not specified the **ip rsvp svc-required** command.

When all of these conditions prevail, RSVP is completely detached from the data flow path and, thus, has no way to detect packets. Use of this command enables RSVP to detect packets so that it can mark them.

RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

Use the **show ip rsvp interface** command to determine whether this command is in effect for an interface or subinterface.

Examples

The following example enables RSVP on the ATM interface 2/0/0 to attach itself to NetFlow:

```
interface atm2/0/0
 ip rsvp flow-assist
```

Related Commands

Command	Description
ip rsvp precedence	Allows you to set the IP Precedence values to be applied to packets that either conform to or exceed the RSVP flowspec.
ip rsvp tos	Allows you to set the ToS values to be applied to packets that either conform to or exceed the RSVP flowspec.
ip rsvp svc-required	Enables creation of an SVC to service any new RSVP reservation made on the interface or subinterface.
show ip rsvp interface	Displays RSVP-related interface information.

ip rsvp neighbor

To enable neighbors to request a reservation, use the **ip rsvp neighbor** interface configuration command. To disable this feature, use the **no** form of this command.

ip rsvp neighbor *access-list-number*

no ip rsvp neighbor *access-list-number*

Syntax Description

access-list-number	Number of a standard or extended access list. It can be any number in the range from 1 to 199.

Defaults

The router accepts messages from any neighbor.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to allow only specific Resource Reservation Protocol (RSVP) neighbors to make a reservation. If no limits are specified, any neighbor can request a reservation. If an access list is specified, only neighbors meeting the specified access list requirements can make a reservation.

RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

Examples

The following example allows neighbors meeting access list 1 requirements to request a reservation:

```
interface ethernet 0
 ip rsvp neighbor 1
```

Related Commands

Command	Description
fair-queue (WFQ)	Enables WFQ for an interface.
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp reservation	Enables a router to simulate receiving and forwarding RSVP RESV messages.
ip rsvp sender	Enables a router to simulate receiving and forwarding RSVP PATH messages.
ip rsvp udp-multicasts	Instructs the router to generate UDP-encapsulated RSVP multicasts whenever it generates an IP-encapsulated multicast packet.
random-detect (interface)	Enables WRED or DWRED.

Command	Description
show ip rsvp installed	Displays RSVP-related installed filters and corresponding bandwidth information.
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp neighbor	Displays current RSVP neighbors.
show ip rsvp reservation	Displays RSVP-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.

ip rsvp policy cops minimal

To lower the load of the COPS server and to improve latency times for messages on the governed router, use the **ip rsvp policy cops minimal** global configuration command to restrict the COPS RSVP policy to adjudicate only PATH and RESV messages. To turn off the restriction, use the **no** form of this command.

ip rsvp policy cops minimal

no ip rsvp policy cops minimal

Syntax Description

This command has no arguments or keywords.

Defaults

The default state is OFF, causing all adjudicable RSVP messages to be processed by the configured COPS policy.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

When this command is used, COPS does not attempt to adjudicate PATHERROR and RESVERROR messages. Instead, those messages are all accepted and forwarded.

Examples

In the following example, COPS authentication is restricted to PATH and RESV messages:

```
ip rsvp policy cops minimal
```

In the following example, that restriction is removed:

```
no ip rsvp policy cops minimal
```

ip rsvp policy cops report-all

To enable a router to report on its success and failure with outsourcing decisions, use the **ip rsvp policy cops report-all** global configuration command. To return the router to its default, use the **no** form of this command.

ip rsvp policy cops report-all

no ip rsvp policy cops report-all

Syntax Description

This command has no arguments or keywords.

Defaults

The default state of this command is to send reports to the PDP about configuration decisions only.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

In the default state, the router reports to the Policy Decision Point (PDP) when the router has succeeded or failed to implement Resource Reservation Protocol (RSVP) configuration decisions.

A *configuration decision* contains at least one of the following:

- A RESV ALLOC context (with or without additional contexts)
- A stateless or named decision object

A decision that does not contain at least one of those elements is an *outsourcing decision.*

Some brands of policy server might expect reports about RSVP messaging, which the default state of the Cisco Common Open Policy Service (COPS) for RSVP does not issue. In such cases, use the **ip rsvp policy cops report-all** command to ensure interoperability between the router and the policy server. Doing so does not adversely affect policy processing on the router.

Unicast FF reservation requests always stimulate a report from the router to the PDP, because those requests contain a RESV ALLOC context (combined with an IN CONTEXT and an OUT CONTEXT).

Examples

In order to show the Policy Enforcement Point (PEP)-to-PDP reporting process, the **debug cops** command in the following example already is enabled when a new PATH message arrives at the router:

```
router-1(config)# ip rsvp policy cops report-all

router-1(config)# 00:02:48:COPS:** SENDING MESSAGE **
Contents of router's request to PDP:
    COPS HEADER:Version 1, Flags 0, Opcode 1 (REQ), Client-type:1, Length:216
    HANDLE (1/1) object. Length:8.    00 00 02 01
    CONTEXT (2/1) object. Length:8.   R-type:5.     M-type:1
    IN_IF (3/1) object. Length:12.   Address:10.1.2.1.    If_index:4
    OUT_IF (4/1) object. Length:12.   Address:10.33.0.1.    If_index:3
    CLIENT SI (9/1) object. Length:168.   CSI data:
    [A 27-line Path message omitted here]
00:02:48:COPS:Sent 216 bytes on socket,
00:02:48:COPS:Message event!
00:02:48:COPS:State of TCP is 4
00:02:48:In read function
00:02:48:COPS:Read block of 96 bytes, num=104 (len=104)
00:02:48:COPS:** RECEIVED MESSAGE **
Contents of PDP's decision received by router:
    COPS HEADER:Version 1, Flags 1, Opcode 2 (DEC), Client-type:1, Length:104
    HANDLE (1/1) object. Length:8.    00 00 02 01
    CONTEXT (2/1) object. Length:8.   R-type:1.     M-type:1
    DECISION (6/1) object. Length:8.   COMMAND cmd:1, flags:0
    DECISION (6/3) object. Length:56.   REPLACEMENT
    [A 52-byte replacement object omitted here]
    CONTEXT (2/1) object. Length:8.   R-type:4.     M-type:1
    DECISION (6/1) object. Length:8.   COMMAND cmd:1, flags:0
00:02:48:Notifying client (callback code 2)
00:02:48:COPS:** SENDING MESSAGE **
Contents of router's report to PDP:
    COPS HEADER:Version 1, Flags 1, Opcode 3 (RPT), Client-type:1, Length:24
    HANDLE (1/1) object. Length:8.    00 00 02 01
    REPORT (12/1) object. Length:8.   REPORT type COMMIT (1)
00:02:48:COPS:Sent 24 bytes on socket,
```

ip rsvp policy cops servers

To specify that Resource Reservation Protocol (RSVP) should use Common Open Policy Service (COPS) policy for remote adjudication, use the **ip rsvp policy cops servers** global configuration command. To turn off the use of COPS for RSVP, use the **no** form of this command.

ip rsvp policy cops [*acl*] **servers** *server-ip* [*server-ip*]

no ip rsvp policy cops [*acl*] **servers**

Syntax Description

acl	(Optional) Specifies the access control list (ACL) whose sessions will be governed by the COPS policy.
server-ip	Specifies the IP addresses of the servers governing the COPS policy. As many as eight servers can be specified, with the first being treated as the primary server.

Defaults

If no ACL is specified, the default behavior is for all reservations to be governed by the specified policy servers.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

If more than one server is specified, the first server is treated by RSVP as the primary serer, and functions as such for *all* ACLs specified.

All servers in the list must have the same policy configuration.

If the connection of the router to the server breaks, the router tries to reconnect to that same server. If the reconnection attempt fails, the router then obeys the following algorithm:

If the connection to the Policy Decision Point (PDP) is closed (either because the PDP closed the connection, a TCP/IP error occurred, or the keepalives failed), the Policy Enforcement Point (PEP) issues a CLIENT-CLOSE message and then attempts to reconnect to the same PDP. If the PEP receives a CLIENT-CLOSE message containing a PDP redirect address, the PEP attempts to connect to the redirected PDP. Note the following points:

- If either attempt fails, the PEP attempts to connect to the PDPs previously specified in the **ip rsvp policy cops servers** configuration command, obeying the sequence of servers given in that command, always starting with the first server in that list.
- If the PEP reaches the end of the list of servers without connecting, it waits a certain time (called the *reconnect delay*) before trying again to connect to the first server in the list. This reconnect delay is initially 30 seconds, and doubles each time the PEP reaches the end of the list without having connected, until the reconnect delay becomes its maximum of 30 minutes. As soon as a connection is made, the delay is reset to 30 seconds.

The **no** form of this command need not contain any server IP addresses, but it must contain *all* the previously specified access lists (see the last example in the following section).

Examples

This first example applies the COPS policy residing on server 172.27.224.117 to all reservations passing through router-9. It also identifies the backup COPS server for this router as the one at address 172.27.229.130:

```
router-9(config)# ip rsvp policy cops servers 172.27.224.117 172.27.229.130
```

The next example applies the COPS policy residing on server 172.27.224.117 to reservations passing through router-9 only if they match access lists 40 and 160. Other reservations passing through that router will not be governed by this server. The command statement also identifies the backup COPS server for that router to be the one at address 172.27.229.130:

```
router-9(config)# ip rsvp policy cops 40 160 servers 172.27.224.117 172.27.229.130
```

The following example turns off COPS for the previously specified access lists 40 and 160 (you cannot turn off just one of the previously specified lists):

```
router-9(config)# no ip rsvp policy cops 40 160 servers
```

ip rsvp policy cops timeout

To configure the amount of time the Policy Enforcement Point (PEP) router will retain policy information after losing connection with the Common Open Policy Service (COPS) server, use the **ip rsvp policy cops timeout** global configuration command. To restore the router to the default value (5 minutes), use the **no** form of this command.

ip rsvp policy cops timeout *policy-timeout*

no ip rsvp policy cops timeout

Syntax Description

policy-timeout	Duration of timeout, from 1 to 10,000 seconds.

Defaults

Timeout default is 300 seconds (5 minutes).

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Examples

The following example configures the router to time out all policy information relating to a lost server in 10 minutes:

```
ip rsvp policy cops timeout 600
```

The following example resets the timeout to the default value:

```
no ip rsvp policy cops timeout
```

ip rsvp policy default-reject

To reject all messages that do not match the policy access control lists (ACLs), use the **ip rsvp policy default-reject** global configuration command. To restore the default behavior, which passes along all messages that do not match the ACLs, use the **no** form of this command.

ip rsvp policy default-reject

no ip rsvp policy default-reject

Syntax Description

This command has no arguments or keywords.

Defaults

Without this command, the default behavior of Resource Reservation Protocol (RSVP) is to accept, install, or forward all unmatched RSVP messages. Once this command is invoked, all unmatched RSVP messages are rejected.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

If COPS is configured without an ACL, or if any policy ACL is configured to use the **permit ip any any** command, the behavior of that ACL will take precedence, and no session will go unmatched.

Note This command makes one exception to its blocking of unmatched messages. It forwards RESVERROR and PATHERROR messages that were generated by its own rejection of RESV and PATH messages. That is done to ensure that the default-reject operation does not remain totally hidden from network managers.

Caution Be extremely careful with this command. It will shut down *all* RSVP processing on the router if access lists are too narrow or if no Common Open Policy Service (COPS) server has been specified. (Use the **ip rsvp policy cops servers** command to specify a COPS server.)

Examples

The following example configures RSVP to reject all unmatched reservations:

```
ip rsvp policy default-reject
```

The following example configures RSVP to accept all unmatched reservations:

```
no ip rsvp policy default-reject
```

ip rsvp pq-profile

To specify the criteria for Resource Reservation Protocol (RSVP) to use to determine which flows to direct into the priority queue (PQ) within weighted fair queueing (WFQ), use the **ip rsvp pq-profile** global configuration command. To disable the specified criteria, use the **no** form of this command.

ip rsvp pq-profile [*voice-like* | *r'* [*b'*[*p-to-r'* | *ignore-peak-value*]]

no ip rsvp pq-profile

Syntax Description

voice-like	(Optional) Indicates pq-profile parameters sufficient for most voice flows. The default values for r', b', and p-to-r' are used. These values should cause all voice flows generated from Cisco IOS applications and most voice flows from other RSVP applications, such as Microsoft NetMeeting, to be directed into the PQ.
r'	(Optional) Indicates maximum rate of a flow in bytes per second. Valid range is from 1 to 1048576 bytes per second.
b'	(Optional) Indicates maximum burst of a flow in bytes. Valid range is from 1 to 8192 bytes.
p-to-r'	(Optional) Indicates maximum ratio of peak rate to average rate as a percentage. Valid range is from 100 to 4000 percent.
ignore-peak-value	(Optional) Indicates that the peak rate to average rate ratio of the flow is not evaluated when RSVP identifies flows.

Defaults

The default value for r' is 12288 bytes per second.

The default value for b' is 592 bytes.

The default value for p-to-r' is 110 percent.

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

Use this command to define the profile of RSVP flows to be placed in the PQ within the WFQ system. You can have only one profile in effect at a time. Changes to this configuration affect only new flows, not existing flows.

This command applies only on interfaces that are running RSVP and WFQ.

RSVP recognizes voice flows based upon the r, b, and p values within the flowspec of a receiver. A reserved flow is granted the PQ as long as the flowspec parameters of a receiver meet the following default criteria:

(r <= r') AND (b <= b') AND (p/r <= p-to-r')

Examples

In the following example, voice-like flows (with the default criteria for voice) are put into the PQ:

```
Router(config)# ip rsvp pq-profile
Router(config)# ip rsvp pq-profile voice-like
Router(config)# ip rsvp pq-profile 12288 592 110
Router(config)# default ip rsvp pq-profile
Router# show run | include pq-profile
```

In the following example, all flows matching the voice criteria are put into the PQ:

```
Router(config)# ip rsvp pq-profile 10240 512 100
Router# show run | include pq-profile
ip rsvp pq-profile 10240 512 100
```

In the following example, no flows are put into the PQ:

```
Router(config)# no ip rsvp pq-profile
Router# show run | include pq-profile
no ip rsvp pq-profile
```

In the following example, flows with the criteria given for r' and b' and the default value for p-to-r' are put into the PQ:

```
Router(config)# ip rsvp pq-profile 9000 300
Router# show run | include pq-profile
ip rsvp pq-profile 9000 300 110
```

In the following example, flows with the criteria given for r' and b' and ignoring the peak value of the flow are put into the PQ:

```
Router(config)# ip rsvp pq-profile 9000 300 ignore-peak-value
Router# show run | include pq-profile
ip rsvp pq-profile 9000 300 ignore-peak-value
```

In the following example, Microsoft NetMeeting voice flows with G.711 or adaptive differential pulse code modulation (ADPCM) codecs are put into the PQ:

```
Router(config)# ip rsvp pq-profile 10200 1200
```

ip rsvp precedence

To enable the router to mark the IP Precedence value of the type of service (ToS) byte for packets in a Resource Reservation Protocol (RSVP) reserved path using the specified values for packets that either conform to or exceed the RSVP flowspec, use the **ip rsvp precedence** interface configuration command. To remove existing IP Precedence settings, use the **no** form of this command; if neither the **conform** nor **exceed** keyword is specified, all IP Precedence settings are removed.

ip rsvp precedence {[**conform** *precedence-value*] [**exceed** *precedence-value*]}

no ip rsvp precedence [**conform**] [**exceed**]

Syntax Description

conform *precedence-value*	(Optional) Specifies an IP Precedence value in the range from 0 to 7 for traffic that conforms to the RSVP flowspec. The IP Precedence value is written to the three high-order bits (bits 5 to 7) of the ToS byte in the IP header of a packet. Either the **conform** or **exceed** keyword is required; both keywords may be specified. When used with the **no** form of the command, the **conform** keyword is optional.
exceed *precedence-value*	(Optional) Specifies an IP Precedence value in the range from 0 to 7 for traffic that exceeds the RSVP flowspec. The IP Precedence value is written to the three high-order bits (bits 5 to 7) of the ToS byte in the IP header of a packet. Either the **conform** or **exceed** keyword is required; both keywords may be specified. When used with the **no** form of the command, the **exceed** keyword is optional.

Defaults

The IP Precedence bits of the ToS byte are left unmodified when this command is not used. The default state is equivalent to execution of the **no ip rsvp precedence** command.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

Packets in an RSVP reserved path are divided into two classes: those that conform to the reservation flowspec and those that correspond to a reservation but that exceed, or are outside, the reservation flowspec.

The **ip rsvp precedence** command allows you to set the IP Precedence values to be applied to packets belonging to these two classes. You must specify the IP Precedence value for at least one class of traffic when you use this command. You can use a single instance of the command to specify values for both classes, in which case you can specify the **conform** and **exceed** keywords in either order.

As part of its input processing, RSVP uses the **ip rsvp precedence** command to set the IP Precedence bits on conforming and nonconforming packets. If per-VC DWRED is configured, the system uses the IP Precedence and ToS bit settings on the output interface in its packet drop process. The IP Precedence setting of a packet can also be used by interfaces on downstream routers.

Execution of the **ip rsvp precedence** command causes IP Precedence values for all preexisting reservations on the interface to be modified.

Note RSVP must be enabled on an interface before you can use this command; that is, use of the **ip rsvp bandwidth** command must precede use of the **ip rsvp precedence** command. RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

RSVP receives packets from the underlying forwarding mechanism. Therefore, before you use the **ip rsvp precedence** command to set IP Precedence, one of the following features is required:

- Weighted fair queueing (WFQ) must be enabled on the interface.
- RSVP switched virtual circuits (SVCs) must be used.
- NetFlow must be configured to assist RSVP.

Note Use of the **no** form of this command is not equivalent to giving the **ip rsvp precedence 0** command, which sets all precedence on the packets to 0, regardless of previous precedence setting.

Examples

The following example sets the IP Precedence value to 3 for all traffic on the ATM interface 0 that conforms to the RSVP flowspec and to 2 for all traffic that exceeds the flowspec:

```
interface atm0
 ip rsvp precedence conform 3 exceed 2
```

The following example sets the IP Precedence value to 2 for all traffic on ATM interface 1 that conforms to the RSVP flowspec. The IP Precedence values of those packets that exceed the flowspec are not altered in any way.

```
interface ATM1
 ip rsvp precedence conform 2
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp policy cops minimal	Lowers the COPS server's load and improves latency times for messages on the governed router.
ip rsvp tos	Allows you to set the ToS values to be applied to packets that either conform to or exceed the RSVP flowspec.
show ip rsvp	Displays the IP Precedence and ToS bit values to be applied to packets that either conform to or exceed the RSVP flowspec for a given interface.

ip rsvp reservation

To enable a router to simulate receiving and forwarding Resource Reservation Protocol (RSVP) RESV messages, use the **ip rsvp reservation** global configuration command. To disable this feature, use the **no** form of this command.

ip rsvp reservation *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-dport sender-sport next-hop-ip-address next-hop-interface* {**ff** | **se** | **wf**} {**rate** | **load**} *bandwidth burst-size*

no ip rsvp reservation *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-dport sender-sport next-hop-ip-address next-hop-interface* {**ff** | **se** | **wf**} {**rate** | **load**} *bandwidth burst-size*

Syntax Description

session-ip-address	For unicast sessions, this is the address of the intended receiver; for multicast sessions, this is the IP multicast address of the session.
sender-ip-address	The IP address of the sender.
tcp | **udp** | *ip-protocol*	TCP, User Datagram Protocol (UDP), or IP protocol in the range from 0 to 255.
session-dport *sender-sport*	*session-dport* is the destination port. *sender-sport* is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If destination is zero, source must be zero, and the implication is that ports are not checked. If destination is nonzero, source must be nonzero (except for **wf** reservations, for which the source port is always ignored and can therefore be zero).
next-hop-ip-address	Host name or address of the receiver or the router closest to the receiver.
next-hop-interface	Next hop interface or subinterface type and number. Interface type can be **ethernet**, **loopback**, **null**, or **serial**.
ff | **se** | **wf**	Reservation style: • Fixed Filter (**ff**) is single reservation. • Shared Explicit (**se**) is shared reservation, limited scope. • Wild Card Filter (**wf**) is shared reservation, unlimited scope.
rate | **load**	QoS guaranteed bit rate service or controlled load service.
bandwidth	Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000.
burst-size	Maximum burst size (KB of data in queue). The range is from 1 to 65535.

Defaults

The router does not simulate receiving and processing RSVP RESV messages by default.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

Use this command to make the router simulate receiving RSVP RESV messages from a downstream host. This command can be used to proxy RSVP RESV messages for non-RSVP-capable receivers. By giving a local (loopback) next hop address and next hop interface, you can also use this command to proxy RSVP for the router you are configuring.

Note RSVP cannot be configured with VIP-distributed Cisco Express Forwarding (dCEF).

Examples

The following example specifies the use of a Shared Explicit style of reservation and the controlled load service, with token buckets of 100 or 150 kbps and 60 or 65 kbps maximum queue depth:

```
ip rsvp reservation 224.250.0.2 172.16.1.1 UDP 20 30 172.16.4.1 Et1 se load 100 60
ip rsvp reservation 224.250.0.2 172.16.2.1 TCP 20 30 172.16.4.1 Et1 se load 150 65
```

The following example specifies the use of a Wild Card Filter style of reservation and the guaranteed bit rate service, with token buckets of 300 or 350 kbps and 60 or 65 kbps maximum queue depth:

```
ip rsvp reservation 224.250.0.3 0.0.0.0 UDP 20 0 172.16.4.1 Et1 wf rate 300 60
ip rsvp reservation 226.0.0.1 0.0.0.0 UDP 20 0 172.16.4.1 Et1 wf rate 350 65
```

Note that the Wild Card Filter does not admit the specification of the sender; it accepts all senders. This action is denoted by setting the source address and port to zero. If, in any filter style, the destination port is specified to be zero, RSVP does not permit the source port to be anything else; it understands that such protocols do not use ports or that the specification applies to all ports.

Related Commands

Command	Description
fair-queue (WFQ)	Enables WFQ for an interface.
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp neighbor	Enables neighbors to request a reservation.
ip rsvp reservation-host	Enables a router to simulate a host generating RSVP RESV messages.
ip rsvp sender	Enables a router to simulate receiving and forwarding RSVP PATH messages.
ip rsvp sender-host	Enables a router to simulate a host generating RSVP PATH messages.
ip rsvp udp-multicasts	Instructs the router to generate UDP-encapsulated RSVP multicasts whenever it generates an IP-encapsulated multicast packet.
random-detect (interface)	Enables WRED or DWRED.
show ip rsvp installed	Displays RSVP-related installed filters and corresponding bandwidth information.
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp neighbor	Displays current RSVP neighbors.

Command	Description
show ip rsvp reservation	Displays RSVP-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.