

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	<i>limit</i>	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 route-cache flow	Enables NetFlow switching for IP routing.
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

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

Command	Description
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 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	<i>priority</i>	(Optional) A value in the range 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	The ip rsvp dsbm-candidate command was introduced.
	12.1(1)	This command was introduced, replacing the ip rsvp dsbm-candidate command.

Usage Guidelines	<p>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.</p>
-------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

You can configure an interface to have a DSBM priority in the range 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 interface Ethernet2 as a DSBM candidate with a priority of 100:

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

Related Commands

Command	Description
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	Parameter	Description
	rate <i>kbps</i>	The average rate (in kbps) for the DSBM candidate.
	burst <i>kilobytes</i>	The maximum burst size (in KB) for the DSBM candidate.
	peak <i>kbps</i>	The peak rate (in kbps) for the DSBM candidate.
	min-unit <i>bytes</i>	The minimum policed unit (in bytes) for the DSBM candidate.
	max-unit <i>bytes</i>	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. To configure the parameters for unlimited, you can either omit the command, or enter the no version 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 interface Ethernet2 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

None (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.

■ ip rsvp flow-assist

Examples

The following example enables RSVP on the atm2/0/0 interface to attach itself to NetFlow:

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

Related Commands

Command	Description
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	<i>access-list-number</i>	Number of a standard or extended access list. It can be any number in the range 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: <pre>interface ethernet 0 ip rsvp neighbor 1</pre>
-----------------	------------------------------------------------------------------------------------------------------------------------------------------------------------

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 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 **conform** nor **exceed** 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 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 **conform** or **exceed** 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 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 **conform** or **exceed** 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 atm0 interface 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 the ATM1 interface 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 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.
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

<i>session-ip-address</i>	For unicast sessions, this is the address of the intended receiver; for multicast sessions, this is the IP multicast address of the session.
<i>sender-ip-address</i>	The IP address of the sender.
tcp udp <i>ip-protocol</i>	TCP, User Datagram Protocol (UDP), or IP protocol in the range 0 to 255.
<i>session-dport</i> <i>sender-sport</i>	<i>session-dport</i> is the destination port. <i>sender-sport</i> 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 ignored and can therefore be zero).
<i>next-hop-ip-address</i>	Host name or address of the receiver or the router closest to the receiver.
<i>next-hop-interface</i>	Next hop interface or subinterface type and number. Interface type can be ethernet , loopback , null , or serial .
ff se wf	Reservation style: <ul style="list-style-type: none"> 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.
<i>bandwidth</i>	Average bit rate (in kbps) to reserve up to 75 percent of total on interface. The range is 1 to 10000000.
<i>burst-size</i>	Maximum burst size (KB of data in queue). The range is 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.

ip rsvp reservation-host

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

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

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

Syntax Description

<i>session-ip-address</i>	For unicast sessions, this is the address of the intended receiver. IP multicast addresses cannot be used with this command. It must be a logical address configured on an interface on the router you are configuring.
<i>sender-ip-address</i>	The IP address of the sender.
tcp udp <i>ip-protocol</i>	TCP, User Datagram Protocol UDP, or IP protocol in the range 0 to 255.
<i>session-dport</i> <i>sender-sport</i>	<i>session-dport</i> is the destination port. <i>sender-sport</i> 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).
ff se wf	Reservation style: <ul style="list-style-type: none"> 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.
<i>bandwidth</i>	Average bit rate (in kbps) to reserve up to 75 percent of total on interface. The range is 1 to 10000000.
<i>burst-size</i>	Maximum burst size (KB of data in queue). The range is 1 to 65535.

Defaults

The router does not simulate a host generating RSVP RESV messages by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Use this command to make the router simulate a host generating its own RSVP RESV messages. This command is similar to the **ip rsvp reservation** command, which can cause the router to generate RESV messages on behalf of another host.

The main differences between the **ip rsvp reservation-host** and **ip rsvp reservation** commands follow:

- When you enter the **ip rsvp reservation-host** command, the *session-ip-address* argument must be a local address configured on an interface on the router. Therefore, you cannot proxy a reservation on behalf of a flow destined for another host. Also, you cannot use this command to generate reservation messages for multicast sessions.
- Because the message is assumed to originate from the router you are configuring, you do not specify a next hop or incoming interface for the RSVP RESV message when entering the **ip rsvp reservation-host** command.

Because you cannot use the command to proxy RSVP for non-RSVP-capable hosts or for multicast sessions, the **ip rsvp reservation-host** command is used mostly for debugging and testing purposes.

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-host 10.1.1.1 10.30.1.4 UDP 20 30 se load 100 60
ip rsvp reservation-host 10.40.2.2 10.22.1.1 TCP 20 30 se load 150 65
```

Related Commands

Command	Description
fair-queue (WFQ)	Enables WFQ for an interface.
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp neighbor	Enables neighbors to request a reservation.
ip rsvp reservation	Enables a router to simulate receiving and forwarding 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.
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 sender

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

ip rsvp sender *session-ip-address sender-ip-address {tcp | udp | ip-protocol} session-dport sender-sport previous-hop-ip-address previous-hop-interface bandwidth burst-size*

no ip rsvp sender *session-ip-address sender-ip-address {tcp | udp | ip-protocol} session-dport sender-sport previous-hop-ip-address previous-hop-interface bandwidth burst-size*

Syntax Description

<i>session-ip-address</i>	For unicast sessions, this is the address of the intended receiver; for multicast sessions, it is the IP multicast address of the session.
<i>sender-ip-address</i>	The IP address of the sender.
tcp udp ip-protocol	TCP, User Datagram Protocol (UDP), or IP protocol in the range 0 to 255.
<i>session-dport</i> <i>sender-sport</i>	<i>session-dport</i> is the destination port. <i>sender-sport</i> 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 ignored and can therefore be zero).
<i>previous-hop-ip-address</i>	Address of the sender or the router closest to the sender.
<i>previous-hop-interface</i>	Address of the previous hop interface or subinterface. Interface type can be ethernet , loopback , null , or serial .
<i>bandwidth</i>	Average bit rate (in kbps) to reserve up to 75 percent of total on interface. The range is 1 to 10000000.
<i>burst-size</i>	Maximum burst size (KB of data in queue). The range is 1 to 65535.

Defaults

The router does not simulate receiving and processing RSVP PATH 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 that it is receiving RSVP PATH messages from an upstream host. The command can be used to proxy RSVP PATH messages for non-RSVP-capable senders. By including a local (loopback) previous hop address and previous hop interface, you can also use this command to proxy RSVP for the router you are configuring.

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

Examples

The following example sets up the router to act like it is receiving RSVP PATH messages using UDP over the loopback 1 interface:

```
ip rsvp sender 224.250.0.1 172.16.2.1 udp 20 30 172.16.2.1 loopback 1 50 5
ip rsvp sender 224.250.0.2 172.16.2.1 udp 20 30 172.16.2.1 loopback 1 50 5
```

Related Commands

Command	Description
fair-queue (WFQ)	Enables WFQ for an interface.
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp neighbor	Enables neighbors to request a reservation.
ip rsvp reservation	Enables a router to simulate receiving and forwarding RSVP RESV messages.
ip rsvp reservation-host	Enables a router to simulate a host generating RSVP RESV messages.
ip rsvp sender-host	Enables a router to simulate a host generating RSVP PATH messages.
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 sender-host

To enable a router to simulate a host generating a Resource Reservation Protocol (RSVP) PATH message, use the **ip rsvp sender-host** global configuration command. To disable this feature, use the **no** form of this command.

ip rsvp sender-host *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-dport sender-sport bandwidth burst-size*

no ip rsvp sender-host *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-dport sender-sport bandwidth burst-size*

Syntax Description

<i>session-ip-address</i>	For unicast sessions, this is the address of the intended receiver; for multicast sessions, it is the IP multicast address of the session.
<i>sender-ip-address</i>	The IP address of the sender. It must be a logical address configured on an interface on the router you are configuring.
tcp udp <i>ip-protocol</i>	TCP, User Datagram Protocol (UDP), or IP protocol in the range 0 to 255.
<i>session-dport</i> <i>sender-sport</i>	<i>session-dport</i> is the destination port. <i>sender-sport</i> 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 ignored and can therefore be zero).
<i>bandwidth</i>	Average bit rate (in kbps) to reserve up to 75 percent of total on interface. The range is 1 to 10000000.
<i>burst-size</i>	Maximum burst size (KB of data in queue). The range is 1 to 65535.

Defaults

The router does not simulate RSVP PATH message generation by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.

Usage Guidelines

Use this command to make the router simulate a host generating its own RSVP PATH messages. This command is similar to the **ip rsvp sender** command, which can cause the router to generate RSVP PATH messages on behalf of another host.

The main differences between the **ip rsvp sender-host** and **ip rsvp sender** commands follow:

- When you enter the **ip rsvp sender-host** command, the *sender-ip-address* argument must be a local address configured on an interface on the router.
- Because the message is assumed to originate from the router you are configuring, you do not specify a previous hop or incoming interface for the RSVP PATH message when entering the **ip rsvp sender-host** command.

Because you cannot use the command to proxy RSVP for non-RSVP-capable hosts, the **ip rsvp sender-host** command is used mostly for debugging and testing purposes.

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

Examples

The following example sets up the router to act like a host that will send traffic to the given multicast address:

```
ip rsvp sender-host 224.250.0.1 10.24.2.1 udp 20 30 50 5
ip rsvp sender-host 227.0.0.1 10.24.2.1 udp 20 30 50 5
```

Related Commands

Command	Description
fair-queue (WFQ)	Enables WFQ for an interface.
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp neighbor	Enables neighbors to request a reservation.
ip rsvp reservation	Enables a router to simulate receiving and forwarding RSVP RESV messages.
ip rsvp reservation-host	Enables a router to simulate a host generating RSVP RESV messages.
ip rsvp sender	Enables a router to simulate receiving 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 svc-required

To enable creation of a switched virtual circuit (SVC) to service any new Resource Reservation Protocol (RSVP) reservation made on the interface or subinterface of an Enhanced ATM port adapter (PA-A3), use the **ip rsvp svc-required** interface configuration command. To disable SVC creation for RSVP reservations, use the **no** form of this command.

ip rsvp svc-required

no ip rsvp svc-required

Syntax Description This command has no arguments or keywords.

Defaults Disabled. This command applies exclusively to the RSVP-ATM QoS Interworking feature.

Command Modes Interface configuration

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

Usage Guidelines Usually reservations are serviced when RSVP classifies packets and a queueing mechanism schedules them for transmission to manage congestion. Traditionally, RSVP is used with weighted fair queueing (WFQ). When RSVP is coupled with WFQ, all of the packets visible to WFQ are also visible to RSVP, which allows RSVP to identify and take action on packets important to it. In this case, WFQ provides bandwidth guarantees.

However, when the **ip rsvp svc-required** command is used to configure an interface or subinterface, a new SVC is established and used to service each new reservation on the interface. ATM SVCs are used to provide bandwidth guarantees and NetFlow is used on input interfaces to make data packets visible to RSVP.



Note When RSVP is enabled, all packets are processed by the Route Switch Processor (RSP).

This command must be executed on both ends of an SVC driven by RSVP. This command is supported only for the Enhanced ATM port adapter (PA-A3) and its subinterfaces.



Note For this command to take effect, NetFlow must be enabled. Therefore, the **ip route-cache flow** command must precede this command in the configuration.

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

Examples

The following example signals RSVP that reservations made on the atm2/0/0 interface will be serviced by creation of an SVC:

```
interface atm2/0/0
 ip rsvp svc-required
```

Related Commands

Command	Description
ip route-cache flow	Enables NetFlow switching for IP routing.
ip rsvp atm-peak-rate-limit	Sets a limit on the peak cell rate of reservations for all newly created RSVP SVCs established on the current interface or any of its subinterfaces.
ip rsvp precedence	Allows you to set the IP Precedence values to be applied to packets that either conform to or exceed the RSVP flowspec.
show ip rsvp interface	Displays RSVP-related interface information.

ip rsvp tos

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

```
ip rsvp tos {[conform tos-value] [exceed tos-value]}
```

```
no ip rsvp tos [conform] [exceed]
```

Syntax Description

conform <i>tos-value</i>	(Optional) Specifies a ToS value in the range 0 to 31 for traffic that conforms to the RSVP flowspec. The ToS value is written to the five low-order bits (bits 0 to 4) of the ToS byte in the IP header of a packet. Either conform or exceed is required; both keywords may be specified. When used with the no form of the command, the conform keyword is optional.
exceed <i>tos-value</i>	(Optional) Specifies a ToS value in the range of 0 to 31 for traffic that exceeds the RSVP flowspec. The ToS byte value is written to the five low-order bits (bits 0 to 4) of the ToS byte in the IP header of a packet. Either conform or exceed is required; both keywords may be specified. When used with the no form of the command, the exceed keyword is optional.

Defaults

The ToS bits of the ToS byte are left unmodified when this command is not used. (The default behavior is equivalent to use of the **no ip rsvp tos** 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 tos** command allows you to set the ToS values to be applied to packets belonging to these two classes. You must specify the ToS value for at least one class of traffic when you use this command. You can use a single instance of the command to specify values for both classes, in which case you can specify the **conform** and **exceed** keywords in either order.

As part of its input processing, RSVP uses the **ip rsvp tos** command configuration to set the ToS bits of the ToS byte on conforming and nonconforming packets. If per-virtual circuit (VC) VIP-Distributed Weighted Random Early Detection (DWRED) is configured, it uses the ToS bit and IP Precedence bit settings on the output interface in its packet drop process. The ToS bit and IP Precedence bit settings of a packet can also be used by interfaces on downstream routers.

Execution of the **ip rsvp tos** command causes ToS bit values for all preexisting reservations on the interface to be modified.

**Note**

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

**Note**

The **ip rsvp tos** command sets bits 0 to 4 so that in combination with the IP Precedence bit settings every bit in the ToS byte is set. Use of these bits is made with full knowledge of the fact that certain canonical texts that address the ToS byte specify that only bits 1 to 4 are used as the ToS bits.

RSVP receives packets from the underlying forwarding mechanism. Therefore, to use the **ip rsvp tos** command to set the ToS bits, one of the following features is required:

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

**Note**

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

Examples

The following example sets the ToS bits value to 4 for all traffic on the atm1 interface that conforms to the RSVP flowspec. ToS bits on packets exceeding the flowspec are not altered.

```
interface atm1
 ip rsvp tos conform 4
```

Related Commands	Command	Description
	ip rsvp bandwidth	Enables RSVP for IP on an interface.
	ip rsvp flow-assist	Enables RSVP to attach itself to NetFlow so that it can leverage NetFlow services.
	ip rsvp precedence	Allows you to set the IP Precedence values to be applied to packets that either conform to or exceed the RSVP flowspec.
	show ip rsvp	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 udp-multicasts

To instruct the router to generate User Datagram Protocol (UDP)-encapsulated Resource Reservation Protocol (RSVP) multicasts whenever it generates an IP-encapsulated multicast packet, use the **ip rsvp udp-multicasts** interface configuration command. To disable this feature, use the **no** form of this command.

ip rsvp udp-multicasts [*multicast-address*]

no ip rsvp udp-multicasts [*multicast-address*]

Syntax Description	<i>multicast-address</i> (Optional) Host name or UDP multicast address of router.
---------------------------	-----------------------------------------------------------------------------------

Defaults	The generation of UDP multicasts is disabled. If a system sends a UDP-encapsulated RSVP message to the router, the router begins using UDP for contact with the neighboring system. The router uses multicast address 224.0.0.14 and starts sending to UDP port 1699. If the command is entered with no specifying multicast address, the router uses the same multicast address.
-----------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Command Modes	Interface configuration
----------------------	-------------------------

Command History	Release	Modification
	11.2	This command was introduced.

Usage Guidelines	Use this command to instruct a router to generate UDP-encapsulated RSVP multicasts whenever it generates an IP-encapsulated multicast packet. Some hosts require this trigger from the router. RSVP cannot be configured with VIP-Distributed Cisco Express Forwarding (dCEF).
-------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Examples	The following example reserves up to 7500 kbps on Ethernet interface 2, with up to 1 Mbps per flow. The router is configured to use UDP encapsulation with the multicast address 224.0.0.14.
-----------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

```
interface ethernet 2
 ip rsvp bandwidth 7500 1000
 ip rsvp udp-multicasts 224.0.0.14
```

Related Commands	Command	Description
	ip rsvp bandwidth	Enables RSVP for IP on an interface.
	ip rsvp neighbor	Enables neighbors to request a reservation.
	ip rsvp reservation	Enables a router to simulate receiving and forwarding RSVP RESV messages.
	ip rsvp sender	Enables a router to simulate receiving and forwarding RSVP PATH messages.

ip rtp priority

To reserve a strict priority queue for a set of Real-Time Transport Protocol (RTP) packet flows belonging to a range of User Datagram Protocol (UDP) destination ports, use the **ip rtp priority** interface configuration command. To disable the strict priority queue, use the **no** form of this command.

ip rtp priority *starting-rtp-port-number port-number-range bandwidth*

no ip rtp priority

Syntax Description

<i>starting-rtp-port-number</i>	The starting RTP port number. The lowest port number to which the packets are sent.
<i>port-number-range</i>	The range of UDP destination ports. Number, which added to the <i>starting-rtp-port-number</i> argument, yields the highest UDP port number.
<i>bandwidth</i>	Maximum allowed bandwidth (in kbps).

Defaults

This command has no default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

This command is most useful for voice applications, or other applications that are delay-sensitive.

This command extends and improves on the functionality offered by the **ip rtp reserve** command by allowing you to specify a range of UDP/RTP ports whose voice traffic is guaranteed strict priority service over any other queues or classes using the same output interface. Strict priority means that if packets exist in the priority queue, they are dequeued and sent first—that is, before packets in other queues are dequeued. We recommend that you use the **ip rtp priority** command instead of the **ip rtp reserve** command for voice configurations.

This command can be used in conjunction with either weighted fair queuing (WFQ) or class-based WFQ (CBWFQ) on the same outgoing interface. In either case, traffic matching the range of ports specified for the priority queue is guaranteed strict priority over other CBWFQ classes or WFQ flows; voice packets in the priority queue are always serviced first.

Remember the following when using the **ip rtp priority** command:

- When used in conjunction with WFQ, the **ip rtp priority** command provides strict priority to voice, and WFQ scheduling is applied to the remaining queues.
- When used in conjunction with CBWFQ, the **ip rtp priority** command provides strict priority to voice. CBWFQ can be used to set up classes for other types of traffic (such as Systems Network Architecture [SNA]) that need dedicated bandwidth and need to be treated better than best effort and not as strict priority; the nonvoice traffic is serviced fairly based on the weights assigned to the enqueued packets. CBWFQ can also support flow-based WFQ within the default CBWFQ class if so configured.

Remember the following guidelines when configuring the *bandwidth* parameter:

- It is always safest to allocate to the priority queue slightly more than the known required amount of bandwidth, to allow room for network bursts.
- The IP RTP Priority admission control policy takes RTP header compression into account. Therefore, while configuring the *bandwidth* parameter of the **ip rtp priority** command you only need to configure for the bandwidth of the compressed call. Because the *bandwidth* parameter is the maximum total bandwidth, you need to allocate enough bandwidth for all calls if there will be more than one call.
- Configure a bandwidth that allows room for Layer 2 headers. The bandwidth allocation takes into account the payload plus the IP, UDP, and RTP headers but does not account for Layer 2 headers. Allowing 25 percent bandwidth for other overhead is conservative and safe.
- The sum of all bandwidth allocation for voice and data flows on an interface cannot exceed 75 percent of the total available bandwidth, unless you change the default maximum reservable bandwidth. To change the maximum reservable bandwidth, use the **max-reserved-bandwidth** command on the interface.

For more information on IP RTP Priority bandwidth allocation, refer to the section “IP RTP Priority” in the chapter “Congestion Management Overview” in the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Examples

The following example first defines a CBWFQ configuration and then reserves a strict priority queue with the following values: a starting RTP port number of 16384, a range of 16383 UDP ports, and a maximum bandwidth of 40 kbps:

```
! The following commands define a class map:
class-map class1
match access-group 101
exit

! The following commands create and attach a policy map:
policy-map policy1
class class1
bandwidth 3000
queue-limit 30
random-detect
random-detect precedence 0 32 256 100
exit
interface Serial1
service-policy output policy1

! The following command reserves a strict priority queue:
ip rtp priority 16384 16383 40
```

Related Commands	Command	Description
	bandwidth (policy-map class)	Specifies or modifies the bandwidth allocated for a class belonging to a policy map.
	fair queue (WFQ)	Enables WFQ for an interface.
	frame-relay ip rtp priority	Reserves a strict priority queue on a Frame Relay PVC for a set of RTP packet flows belonging to a range of UDP destination ports.
	ip rtp reserve	Reserves a special queue for a set of RTP packet flows belonging to a range of UDP destination ports.
	max-reserved-bandwidth	Changes the percent of interface bandwidth allocated for CBWFQ, LLQ, and IP RTP Priority.
	policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
	ppp multilink	Enables MLP on an interface and, optionally, enables dynamic bandwidth allocation.
	ppp multilink fragment-delay	Configures a maximum delay allowed for transmission of a packet fragment on an MLP bundle.
	ppp multilink interleave	Enables interleaving of RTP packets among the fragments of larger packets on an MLP bundle.
	priority	Gives priority to a class within a policy map.
	service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
	show policy-map	Displays the configuration of all classes comprising the specified service policy map or all classes for all existing policy maps.
	show queue	Displays the contents of packets inside a queue for a particular interface or VC.