



RSVP Scalability Enhancements

First Published: June 7, 2001

Last Updated: February 19, 2007

The RSVP Scalability Enhancements let you select a resource provider and disable data packet classification so that Resource Reservation Protocol (RSVP) performs admission control only.

History for RSVP Scalability Enhancements

Release	Modification
12.2(2)T	This feature was introduced.
12.2(14)S	This feature was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXF2	This feature was integrated into Cisco IOS Release 12.2(18)SXF2.
12.2(18)SXF5	This feature was integrated into Cisco IOS Release 12.2(18)SXF5.
12.2(33)SRB	This feature was integrated into Cisco IOS Release 12.2(33)SRB.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS and Catalyst OS software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Contents

- [Prerequisites for RSVP Scalability Enhancements, page 2](#)
- [Restrictions for RSVP Scalability Enhancements, page 2](#)
- [Information About RSVP Scalability Enhancements, page 2](#)
- [How to Configure RSVP Scalability Enhancements, page 4](#)
- [Configuration Examples for RSVP Scalability Enhancements, page 15](#)
- [Additional References, page 20](#)
- [Command Reference, page 21](#)
- [Glossary, page 44](#)



Americas Headquarters:

Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2001, 2006, 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for RSVP Scalability Enhancements

The network must support the following Cisco IOS features before the RSVP Scalability Enhancements are enabled:

- RSVP
- Class-based weighted fair queueing (CBWFQ)

Restrictions for RSVP Scalability Enhancements

- Sources should not send marked packets without an installed reservation.
- Sources should not send marked packets that exceed the reserved bandwidth.
- Sources should not send marked packets to a destination other than the reserved path.

Information About RSVP Scalability Enhancements

To use the RSVP Scalability Enhancements, you should understand the following concepts:

- [Feature Overview of the RSVP Scalability Enhancements, page 2](#)
- [Benefits of the RSVP Scalability Enhancements, page 3](#)

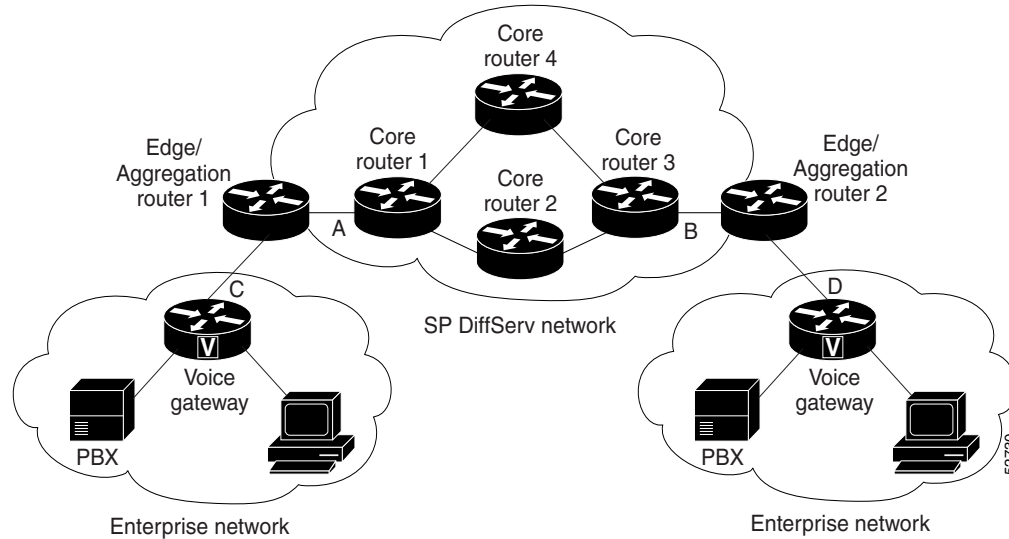
Feature Overview of the RSVP Scalability Enhancements

RSVP typically performs admission control, classification, policing, and scheduling of data packets on a per-flow basis and keeps a database of information for each flow. RSVP Scalability Enhancements let you select a resource provider (formerly called a quality of service [QoS] provider) and disable data packet classification so that RSVP performs admission control only. This facilitates integration with service provider (differentiated services [DiffServ]) networks and enables scalability across enterprise networks.

Class-based weighted fair queueing (CBWFQ) provides the classification, policing, and scheduling functions. CBWFQ puts packets into classes based on the differentiated services code point (DSCP) value in the packet's IP header, thereby eliminating the need for per-flow state and per-flow processing.

[Figure 1](#) shows two enterprise networks interconnected through a service provider (SP) network. The SP network has an IP backbone configured as a DiffServ network. Each enterprise network has a voice gateway connected to an SP edge/aggregation router via a WAN link. The enterprise networks are connected to a private branch exchange (PBX).

Figure 1 *RSVP/DiffServ Integration Topology*



The voice gateways are running classic RSVP, which means RSVP is keeping a state per flow and also classifying, marking, and scheduling packets on a per-flow basis. The edge/aggregation routers are running classic RSVP on the interfaces (labeled C and D) connected to the voice gateways and running RSVP for admission control only on the interfaces connected to core routers 1 and 3. The core routers in the DiffServ network are not running RSVP, but are forwarding the RSVP messages to the next hop. The core routers inside the DiffServ network implement a specific per hop behavior (PHB) for a collection of flows that have the same DSCP value.

The voice gateways identify voice data packets and set the appropriate DSCP in their IP headers such that the packets are classified into the priority class in the edge/aggregation routers and in core routers 1, 2, 3 or 1, 4, 3.

The interfaces of the edge/aggregation routers (labeled A and B) connected to core routers 1 and 3 are running RSVP, but are doing admission control only per flow against the RSVP bandwidth pool configured on the DiffServ interfaces of the edge/aggregation routers. CBWFQ is performing the classification, policing, and scheduling functions.

Benefits of the RSVP Scalability Enhancements

Enhanced Scalability

RSVP Scalability Enhancements handle similar flows on a per-class basis instead of on a per-flow basis. Because fewer resources are required to maintain per-class QoS guarantees, faster processing results, thereby enhancing scalability.

Improved Router Performance

RSVP Scalability Enhancements improve router performance by reducing the cost for data packet classification and scheduling, which decreases CPU resource consumption. The saved resources can then be used for other network management functions.

How to Configure RSVP Scalability Enhancements

This section contains the following procedures:

- [Enabling RSVP on an Interface, page 4](#) (required)
- [Setting the Resource Provider, page 5](#) (required)
- [Disabling Data Packet Classification, page 6](#) (required)
- [Configuring Class and Policy Maps, page 7](#) (required)
- [Attaching a Policy Map to an Interface, page 10](#) (required)
- [Verifying the Configuration, page 11](#) (optional)

Enabling RSVP on an Interface

Perform this task to enable RSVP on an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip rsvp bandwidth** [*interface-kbps*] [*single-flow-kbps*]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> [<i>name-tag</i>] Example: Router(config)# interface Ethernet0/0	Configures the interface type and enters interface configuration mode. <ul style="list-style-type: none"> • The optional <i>name-tag</i> argument specifies the logic name to identify the server configuration so that multiple server configurations can be entered. <p>Note This optional argument is for use with the Redundant Link Manager (RLM) feature.</p>

	Command or Action	Purpose
Step 4	<pre>ip rsvp bandwidth [interface-kbps] [<i>single-flow-kbps</i>]</pre> <p>Example: Router(config-if)# ip rsvp bandwidth 7500 7500</p>	<p>Enables RSVP on an interface.</p> <ul style="list-style-type: none"> The optional <i>interface-kbps</i> and <i>single-flow-kbps</i> arguments specify the amount of bandwidth that can be allocated by RSVP flows or to a single flow, respectively. Values are from 1 to 10,000,000. <p>Note Repeat this command for each interface that you want to enable.</p>
Step 5	<pre>end</pre> <p>Example: Router(config-if)# end</p>	(Optional) Exits to privileged EXEC mode.

Setting the Resource Provider

Perform this task to set the resource provider.



Note

Resource provider was formerly called QoS provider.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip rsvp resource-provider none** [**none** | **wfq-interface** | **wfq-pvc**]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>enable</pre> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<pre>configure terminal</pre> <p>Example: Router# configure terminal</p>	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<p>interface <i>type number</i> [<i>name-tag</i>]</p> <p>Example: Router(config)# interface Ethernet0/0</p>	<p>Configures the interface type and enters interface configuration mode.</p> <ul style="list-style-type: none"> The optional <i>name-tag</i> argument specifies the logic name to identify the server configuration so that multiple server configurations can be entered. <p>Note This optional argument is for use with the Redundant Link Manager (RLM) feature.</p>
Step 4	<p>ip rsvp resource-provider [none wfq-interface wfq-pvc]</p> <p>Example: Router(config-if)# ip rsvp resource-provider none</p>	<p>Sets the resource provider.</p> <ul style="list-style-type: none"> Enter the optional none keyword to set the resource provider to none regardless of whether one is configured on the interface. <p>Note Setting the resource provider to none instructs RSVP to <i>not</i> associate any resources, such as weighted fair queueing (WFQ) queues or bandwidth, with a reservation.</p> <ul style="list-style-type: none"> Enter the optional wfq-interface keyword to specify WFQ as the resource provider on the interface. Enter the optional wfq-pvc keyword to specify WFQ as the resource provider on the permanent virtual circuit (PVC) or connection.
Step 5	<p>end</p> <p>Example: Router(config-if)# end</p>	<p>(Optional) Exits to privileged EXEC mode.</p>

Disabling Data Packet Classification

Perform this task to turn off (disable) data packet classification.



Note

Disabling data packet classification instructs RSVP *not* to process every packet, but to perform admission control only.

SUMMARY STEPS

- enable**
- configure terminal**
- interface** *type number* [*name-tag*]
- ip rsvp data-packet classification none**
- end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>interface number</i> [<i>name-tag</i>] Example: Router(config)# interface Ethernet0/0	Configures the interface type and enters interface configuration mode. <ul style="list-style-type: none">The optional <i>name-tag</i> argument specifies the logic name to identify the server configuration so that multiple server configurations can be entered. Note This optional argument is for use with the Redundant Link Manager (RLM) feature.
Step 4	ip rsvp data-packet classification none Example: Router(config-if)# ip rsvp data-packet classification none	Turns off (disables) data packet classification.
Step 5	end Example: Router(config-if)# end	(Optional) Exits to privileged EXEC mode.

Configuring Class and Policy Maps

Perform this task to configure class and policy maps.

SUMMARY STEPS

- enable**
- configure terminal**
- class-map** [*type* {**stack** | **access-control** | **port-filter** | **queue-threshold**}] [**match-all** | **match-any**] *class-map-name*
- match access-group** {*access-group* | **name** *access-group-name*}
- exit**
- policy-map** [*type* **access-control**] *policy-map-name*
- class** {*class-name* | **class-default**}
- priority** {*bandwidth-kbps* | **percent** *percentage*} [*burst*]
- end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p><code>configure terminal</code></p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><code>class-map [type {stack access-control port-filter queue-threshold}] [match-all match-any] class-map-name</code></p> <p>Example: Router(config)# class-map match-all voice</p>	<p>Creates a class map to be used for matching packets to a specified class and enters class-map configuration mode.</p> <ul style="list-style-type: none"> The optional type stack keywords enable the flexible packet matching (FPM) functionality to determine the correct protocol stack in which to examine. <p>Note If the appropriate protocol header description files (PHDFs) have been loaded onto the router (via the load protocol command), a stack of protocol headers can be defined so the filter can determine which headers are present and in what order.</p> <ul style="list-style-type: none"> The optional type access-control keywords determine the exact pattern to look for in the protocol stack of interest. <p>Note You must specify a stack class map (via the type stack keywords) before you can specify an access-control class map (via the type access-control keywords).</p> <ul style="list-style-type: none"> The optional type port-filter keywords create a port-filter class-map that enables the TCP/UDP port policing of control plane packets. <p>Note When enabled, these keywords provide filtering of traffic destined to specific ports on the control plane host subinterface.</p> <ul style="list-style-type: none"> The optional type queue-threshold keywords enable queue thresholding that limits the total number of packets for a specified protocol that is allowed in the control plane IP input queue. This feature applies only to control plane host subinterface. The optional match-all match-any keywords determine how packets are evaluated when multiple match criteria exist. Packets must either meet all of the match criteria (match-all) or one of the match criteria (match-any) in order to be considered a member of the class.

	Command or Action	Purpose
Step 4	<p>match access-group {<i>access-group</i> name <i>access-group-name</i>}</p> <p>Example: Router(config-cmap)# match access-group 100</p>	<p>Specifies the numbered access list against whose contents packets are checked to determine if they match the criteria specified in the class map.</p> <p>Note After you create the class map, you configure its match criteria. Here are some of the commands that you can use:</p> <ul style="list-style-type: none"> - match access-group - match input-interface - match mpls experimental - match protocol
Step 5	<p>exit</p> <p>Example: Router(config-cmap)# exit</p>	Exits to global configuration mode.
Step 6	<p>policy-map [type access-control] <i>policy-map-name</i></p> <p>Example: Router(config)# policy-map wfq-voip</p>	<p>Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy and enters policy-map configuration mode.</p> <ul style="list-style-type: none"> • The optional type access-control keywords determine the exact pattern to look for in the protocol stack of interest.
Step 7	<p>class {<i>class-name</i> class-default}</p> <p>Example: Router(config-pmap-c)# class voice</p>	<p>Specifies the class so that you can configure or modify its policy. Enters policy-map class configuration mode.</p> <ul style="list-style-type: none"> • Enter the class name or use the class-default keyword.
Step 8	<p>priority {<i>bandwidth-kbps</i> percent <i>percentage</i>} [<i>burst</i>]</p> <p>Example: Router(config-pmap-c)# priority 24</p>	<p>(Optional) Prioritizes a class of traffic belonging to a policy map.</p> <ul style="list-style-type: none"> • The optional <i>burst</i> argument specifies the burst size in bytes. The burst size configures the network to accommodate temporary bursts of traffic. The default burst value, which is computed as 200 milliseconds of traffic at the configured bandwidth rate, is used when the burst argument is not specified. The range of the burst is from 32 to 2000000 bytes.
Step 9	<p>end</p> <p>Example: Router(config-pmap)# end</p>	(Optional) Exits to privileged EXEC mode.

Attaching a Policy Map to an Interface

Perform this task to attach a policy map to an interface.



Note

If at the time you configure the RSVP Scalability Enhancements, there are existing reservations that use classic RSVP, no additional marking, classification, or scheduling is provided for these flows. You can also delete these reservations after you configure the RSVP Scalability Enhancements.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **service-policy** [**type access-control**] {**input** | **output**} *policy-map-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> [<i>name-tag</i>] Example: Router(config)# interface atm1/0	Configures an interface or subinterface type and enters interface configuration mode. <ul style="list-style-type: none"> • The optional <i>name-tag</i> argument specifies the logic name to identify the server configuration so that multiple server configurations can be entered. <p>Note This optional argument is for use with the Redundant Link Manager (RLM) feature.</p>

	Command or Action	Purpose
Step 4	<pre>service-policy [type access-control] {input output} policy-map-name</pre> <p>Example: Router(config-if)# service-policy output POLICY-ATM</p>	<p>Specifies the name of the policy map to be attached to the input or output direction of the interface.</p> <p>Note Policy maps can be attached in the input or output direction of an interface. The direction and the router to which the policy map should be attached vary according to the network configuration. When using the service-policy command to attach the policy map to an interface, be sure to choose the router and the interface direction that are appropriate for the network configuration.</p> <ul style="list-style-type: none"> • The optional type access-control keywords determine the exact pattern to look for in the protocol stack of interest. • Enter the policy-map name.
Step 5	<pre>end</pre> <p>Example: Router(config-if) end</p>	(Optional) Exits to privileged EXEC mode.

Verifying the Configuration

Perform the following task to verify the RSVP Scalability Enhancements are configured.

SUMMARY STEPS

1. **enable**
2. **show ip rsvp interface** [*interface-type interface-number*] [**detail**]
3. **show ip rsvp installed** [*interface-type interface-number*] [**detail**]
4. **show queueing** [**custom** | **fair** | **priority** | **random-detect**] [**interface** *atm-subinterface* [**vc** [[*vpi/vci*]]]]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>show ip rsvp interface [<i>interface-type</i> <i>interface-number</i>] [detail]</p> <p>Example: Router# show ip rsvp interface detail</p>	<p>Displays RSVP-related information.</p> <ul style="list-style-type: none"> • The optional <i>interface-type</i> specifies the type of the interface. • The optional <i>interface-number</i> specifies the number of the interface. • The optional detail keyword displays additional information about interfaces.
Step 3	<p>show ip rsvp installed [<i>interface-type</i> <i>interface-number</i>] [detail]</p> <p>Example: Router# show ip rsvp installed detail</p>	<p>Displays information about interfaces and their admitted reservations.</p> <ul style="list-style-type: none"> • The optional <i>interface-type</i> specifies the type of the interface. • The optional <i>interface-number</i> specifies the number of the interface. • The optional detail keyword displays additional information about interfaces and their admitted reservations.

	Command or Action	Purpose
Step 4	<pre>show queueing [custom fair priority random-detect [interface atm-subinterface [vc [[vpi/] vci]]]]</pre> <p>Example: Router# show queueing</p>	<p>Lists all or selected configured queueing strategies.</p> <ul style="list-style-type: none"> The optional custom keyword shows the status of the custom queueing list configuration. The optional fair keyword shows the status of the fair queueing configuration. The optional priority keyword shows the status of the fair queueing configuration. The optional random-detect keywords show the status of the Weighted Random Early Detection (WRED) and distributed WRED (DWRED) configuration, including configuration of flow-based WRED. The optional interface atm-subinterface keyword-argument combination displays the WRED parameters of every virtual circuit (VC) with WRED enabled on the specified ATM subinterface. The optional vc keyword displays the WRED parameters associated with a specific VC. If desired, both the virtual path identifier (VPI) and virtual circuit identifier (VCI) values, or just the VCI value, can be specified. The optional <i>vpi/</i> argument specifies the VPI. If the <i>vpi</i> argument is omitted, 0 is used as the VPI value for locating the permanent virtual circuit (PVC). If the <i>vpi</i> argument is specified, the / separator is required. The optional <i>vci</i> argument specifies the VCI.
Step 5	<pre>exit</pre> <p>Example: Router# exit</p>	<p>(Optional) Exits privileged EXEC mode.</p>

Examples

This section provides the following example output:

- [Sample Output for the show ip rsvp interface detail Command, page 13](#)
- [Sample Output for the show ip rsvp installed detail Command, page 14](#)

Sample Output for the show ip rsvp interface detail Command

Enter the **show ip rsvp interface detail** command to display information about interfaces, subinterfaces, resource providers, and data packet classification. The output in the following example shows that the ATM 6/0 interface has resource provider none configured and data packet classification is turned off:

```
Router# show ip rsvp interface detail

AT6/0:
  Bandwidth:
    Curr allocated: 190K bits/sec
    Max. allowed (total): 112320K bits/sec
```

```

Max. allowed (per flow): 112320K bits/sec
Neighbors:
  Using IP encap: 1.  Using UDP encaps: 0
  DSCP value used in Path/Resv msgs: 0x30
  RSVP Data Packet Classification is OFF <-----! disabled data packet classification!
  RSVP resource provider is: none <-----! resource provider none!

```



Note The last two lines in the preceding output verify that the RSVP Scalability Enhancements (disabled data packet classification and resource provider none) are present.

Sample Output for the show ip rsvp installed detail Command

Enter the **show ip rsvp installed detail** command to display information about interfaces, subinterfaces, their admitted reservations, bandwidth, resource providers, and data packet classification.

```
Router# show ip rsvp installed detail
```

```

RSVP: Ethernet3/3 has no installed reservations

RSVP: ATM6/0 has the following installed reservations
RSVP Reservation. Destination is 10.1.1.2, Source is 10.1.1.1,
  Protocol is UDP, Destination port is 14, Source port is 14
  Reserved bandwidth: 50K bits/sec, Maximum burst: 1K bytes, Peak rate: 50K bits/sec
  Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
  Resource provider for this flow: None
  Conversation supports 1 reservations
  Data given reserved service: 0 packets (0 bytes)
  Data given best-effort service: 0 packets (0 bytes)
  Reserved traffic classified for 54 seconds
  Long-term average bitrate (bits/sec): 0M reserved, 0M best-effort
RSVP Reservation. Destination is 10.1.1.2, Source is 10.1.1.1,
  Protocol is UDP, Destination port is 10, Source port is 10
  Reserved bandwidth: 20K bits/sec, Maximum burst: 1K bytes, Peak rate: 20K bits/sec
  Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
  Resource provider for this flow: None
  Conversation supports 1 reservations
  Data given reserved service: 0 packets (0 bytes)
  Data given best-effort service: 0 packets (0 bytes)
  Reserved traffic classified for 80 seconds
  Long-term average bitrate (bits/sec): 0M reserved, 0M best-effort

```

Wait for a while, then enter the **show ip rsvp installed detail** command again. In the following output, notice there is no increment in the number of packets classified:

```
Router# show ip rsvp installed detail
```

```

RSVP: Ethernet3/3 has no installed reservations

RSVP: ATM6/0 has the following installed reservations
RSVP Reservation. Destination is 10.1.1.2, Source is 10.1.1.1,
  Protocol is UDP, Destination port is 14, Source port is 14
  Reserved bandwidth: 50K bits/sec, Maximum burst: 1K bytes, Peak rate: 50K bits/sec
  Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
  Resource provider for this flow: None
  Conversation supports 1 reservations
  Data given reserved service: 0 packets (0 bytes)
  Data given best-effort service: 0 packets (0 bytes)
  Reserved traffic classified for 60 seconds
  Long-term average bitrate (bits/sec): 0 reserved, 0M best-effort
RSVP Reservation. Destination is 10.1.1.2, Source is 10.1.1.1,
  Protocol is UDP, Destination port is 10, Source port is 10
  Reserved bandwidth: 20K bits/sec, Maximum burst: 1K bytes, Peak rate: 20K bits/sec

```

```

Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
Resource provider for this flow: None
Conversation supports 1 reservations
Data given reserved service: 0 packets (0 bytes)
Data given best-effort service: 0 packets (0 bytes)
Reserved traffic classified for 86 seconds
Long-term average bitrate (bits/sec): 0M reserved, 0M best-effort

```

Configuration Examples for RSVP Scalability Enhancements

This section provides the following configuration examples:

- [Configuring CBWFQ to Accommodate Reserved Traffic: Examples, page 15](#)
- [Configuring the Resource Provider as None with Data Classification Turned Off: Examples, page 16](#)

Configuring CBWFQ to Accommodate Reserved Traffic: Examples

The following output shows a class map and a policy map being configured for voice:

```

Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# class-map match-all voice
Router(config-cmap)# match access-group 100
Router(config-cmap)# exit
Router(config)# policy-map wfq-voip
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 24
Router(config-pmap-c)# end

```



Note

The bandwidth that you configured for the CBWFQ priority queue (24 kbps) must match the bandwidth that you configured for the interface. See the section [“Enabling RSVP on an Interface”](#).

The following output shows an access list being configured:

```

Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# access-list 100 permit udp any any range 16384 32500

```

The following output shows a class being applied to the outgoing interface:

```

Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface atm6/0
Router(config-if)# service-policy output wfq-voip

```

The following output shows bandwidth being configured on an interface:

```

Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface atm6/0
Router(config-if)# ip rsvp bandwidth 24

```

**Note**

The bandwidth that you configure for the interface (24 kbps) must match the bandwidth that you configured for the CBWFQ priority queue.

Configuring the Resource Provider as None with Data Classification Turned Off: Examples

The **show running-config** command displays the current configuration in the router:

```
Router# show running-config interface atm6/0

class-map match-all voice
  match access-group 100
!
policy-map wfq-voip
  class voice
    priority 24
  class class-default
    fair-queue
!
interface ATM6/0
ip address 10.20.22.1 255.255.255.0
no ip redirects
no ip proxy-arp
no ip route-cache cef
atm uni-version 4.0
atm pvc 1 0 5 qsaal
atm pvc 2 0 16 ilmi
atm esi-address 111111111181.00
no atm auto-configuration
no atm ilmi-keepalive
pvc blue 200/100
  abr 700 600
  inarp 1
  broadcast
  encapsulation aal5snap
  service-policy output wfq-voip
!
ip rsvp bandwidth 24 24
ip rsvp signalling dscp 48
access-list 100 permit udp any any range 16384 32500
```

Here is output from the **show ip rsvp interface detail** command before resource provider none is configured and data-packet classification is turned off:

```
Router# show ip rsvp interface detail

AT6/0:
  Bandwidth:
    Curr allocated: 190K bits/sec
    Max. allowed (total): 112320K bits/sec
    Max. allowed (per flow): 112320K bits/sec
  Neighbors:
    Using IP encap: 1. Using UDP encaps: 0
    DSCP value used in Path/Resv msgs: 0x30
```

Here is output from the **show queueing** command before resource provider none is configured and data packet classification is turned off:

```
Router# show queueing interface atm6/0

Interface ATM6/0 VC 200/100
Queueing strategy: weighted fair
Output queue: 63/512/64/3950945 (size/max total/threshold/drops)
  Conversations 2/5/64 (active/max active/max total)
  Reserved Conversations 0/0 (allocated/max allocated)
  Available Bandwidth 450 kilobits/sec
```



Note

New reservations do not reduce the available bandwidth (450 kbps shown above). Instead RSVP performs admission control only by using the bandwidth limit configured in the **ip rsvp bandwidth** command. The bandwidth configured in this command should match the bandwidth configured in the CBWFQ class that you set up to handle the reserved traffic.

The following output shows resource provider none being configured:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface atm6/0
Router(config-if)# ip rsvp resource-provider none
Router(config-if)# end
```

The following output shows data packet classification being turned off:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface atm6/0
Router(config-if)# ip rsvp data-packet classification none
Router(config-if)# end
```

Here is output from the **show ip rsvp interface detail** command after resource provider none has been configured and data packet classification has been turned off:

```
Router# show ip rsvp interface detail

AT6/0:
  Bandwidth:
    Curr allocated: 190K bits/sec
    Max. allowed (total): 112320K bits/sec
    Max. allowed (per flow): 112320K bits/sec
  Neighbors:
    Using IP encap: 1. Using UDP encaps: 0
  DSCP value used in Path/Resv msgs: 0x30
  RSVP Data Packet Classification is OFF
  RSVP resource provider is: none
```

The following output from the **show ip rsvp installed detail** command verifies that resource provider none is configured and data packet classification is turned off:

```
Router# show ip rsvp installed detail

RSVP: ATM6/0 has the following installed reservations
RSVP Reservation. Destination is 10.1.1.2, Source is 10.1.1.1,
  Protocol is UDP, Destination port is 14, Source port is 14
  Reserved bandwidth: 50K bits/sec, Maximum burst: 1K bytes, Peak rate: 50K bits/sec
```

```

Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
Resource provider for this flow: None
Conversation supports 1 reservations
Data given reserved service: 3192 packets (1557696 bytes)
Data given best-effort service: 42 packets (20496 bytes)
Reserved traffic classified for 271 seconds
Long-term average bitrate (bits/sec): 45880 reserved, 603 best-effort
RSVP Reservation. Destination is 10.1.1.2, Source is 10.1.1.1,
Protocol is UDP, Destination port is 10, Source port is 10
Reserved bandwidth: 20K bits/sec, Maximum burst: 1K bytes, Peak rate: 20K bits/sec
Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
Resource provider for this flow: None
Conversation supports 1 reservations
Data given reserved service: 1348 packets (657824 bytes)
Data given best-effort service: 0 packets (0 bytes)
Reserved traffic classified for 296 seconds
Long-term average bitrate (bits/sec): 17755 reserved, 0M best-effort

```

The following output shows no increments in packet counts after the source sends data packets that match the reservation:

```
Router# show ip rsvp installed detail
```

```

RSVP: Ethernet3/3 has no installed reservations

RSVP: ATM6/0 has the following installed reservations
RSVP Reservation. Destination is 10.1.1.2, Source is 10.1.1.1,
Protocol is UDP, Destination port is 14, Source port is 14
Reserved bandwidth: 50K bits/sec, Maximum burst: 1K bytes, Peak rate: 50K bits/sec
Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
Resource provider for this flow: None
Conversation supports 1 reservations
Data given reserved service: 3192 packets (1557696 bytes)
Data given best-effort service: 42 packets (20496 bytes)
Reserved traffic classified for 282 seconds
Long-term average bitrate (bits/sec): 44051 reserved, 579 best-effort
RSVP Reservation. Destination is 10.1.1.2, Source is 10.1.1.1,
Protocol is UDP, Destination port is 10, Source port is 10
Reserved bandwidth: 20K bits/sec, Maximum burst: 1K bytes, Peak rate: 20K bits/sec
Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
Resource provider for this flow: None
Conversation supports 1 reservations
Data given reserved service: 1348 packets (657824 bytes)
Data given best-effort service: 0 packets (0 bytes)
Reserved traffic classified for 307 seconds
Long-term average bitrate (bits/sec): 17121 reserved, 0M best-effort

```

The following output shows that data packet classification is enabled again:

```

Router# configure terminal
Router(config)# interface atm6/0
Router(config-if) no ip rsvp data-packet classification
Router(config-if)# end

```

The following output verifies that data packet classification is occurring:

```

Router# show ip rsvp installed detail

Enter configuration commands, one per line. End with CNTL/Z.
RSVP: ATM6/0 has the following installed reservations
RSVP Reservation. Destination is 10.1.1.2, Source is 10.1.1.1,
Protocol is UDP, Destination port is 14, Source port is 14

```

```

Reserved bandwidth: 50K bits/sec, Maximum burst: 1K bytes, Peak rate: 50K bits/sec
Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
Resource provider for this flow: None
Conversation supports 1 reservations
Data given reserved service: 3683 packets (1797304 bytes)
Data given best-effort service: 47 packets (22936 bytes)
Reserved traffic classified for 340 seconds
Long-term average bitrate (bits/sec): 42201 reserved, 538 best-effort
RSVP Reservation. Destination is 10.1.1.2, Source is 10.1.1.1,
Protocol is UDP, Destination port is 10, Source port is 10
Reserved bandwidth: 20K bits/sec, Maximum burst: 1K bytes, Peak rate: 20K bits/sec
Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
Resource provider for this flow: None
Conversation supports 1 reservations
Data given reserved service: 1556 packets (759328 bytes)
Data given best-effort service: 0 packets (0 bytes)
Reserved traffic classified for 364 seconds
Long-term average bitrate (bits/sec): 16643 reserved, 0M best-effort

```

Here is output from the **show running-config** command after you have performed all the previous configuration tasks:

```

Router# show running-config interface atm6/0

class-map match-all voice
  match access-group 100
!
policy-map wfq-voip
  class voice
    priority 24
  class class-default
    fair-queue
!
interface ATM6/0
  ip address 10.20.22.1 255.255.255.0
  no ip redirects
  no ip proxy-arp
  no ip route-cache cef
  atm uni-version 4.0
  atm pvc 1 0 5 qsaal
  atm pvc 2 0 16 ilmi
  atm esi-address 11111111181.00
  no atm auto-configuration
  no atm ilmi-keepalive
  pvc blue 200/100
    abr 700 600
    inarp 1
    broadcast
    encapsulation aal5snap
    service-policy output wfq-voip
!
  ip rsvp bandwidth 24 24
  ip rsvp signalling dscp 48
  ip rsvp data-packet classification none
  ip rsvp resource-provider none

access-list 100 permit udp any any range 16384 32500

```

Additional References

The following sections provide references related to the RSVP Scalability Enhancements.

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	<ul style="list-style-type: none"> • Cisco IOS Quality of Service Solutions Command Reference, Release 12.4T • Cisco IOS Quality of Service Solutions Command Reference, Release 12.2SR
QoS features including signaling, classification, and congestion management	Cisco IOS Quality of Service Solutions Configuration Guide , Release 12.4

Standards

Standard	Title
None	—

MIBs

MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2205	<i>Resource Reservation Protocol</i>
RFC 2206	<i>RSVP Management Information Base Using SMIv</i>

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Command Reference

This section documents modified commands only.

- [debug ip rsvp traffic-control](#)
- [debug ip rsvp wfq](#)
- [ip rsvp data-packet classification none](#)
- [ip rsvp resource-provider](#)
- [show ip rsvp installed](#)
- [show ip rsvp interface](#)
- [show queueing](#)

debug ip rsvp traffic-control

To display debugging messages for compression-related events, use the **debug ip rsvp traffic-control** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip rsvp traffic-control

no debug ip rsvp traffic-control

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0	This command was introduced.
	12.2(15)T	The command output was modified to include compression-related events.
	12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(18)SXF2	This command was integrated into Cisco IOS Release 12.2(18)SXF2.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines Use the **debug ip rsvp traffic-control** command to troubleshoot compression-related problems.

Examples The following example from the **debug ip rsvp traffic-control** command shows that compression was successfully predicted:

```
Router# debug ip rsvp traffic-control

RSVP debugging is on

Router# show debugging

00:44:49: RSVP-TC: Attempting to install QoS for rsb 62CC66F0
00:44:49: RSVP-TC: Adding new tcsb 02000406 for rsb 62CC66F0
00:44:49: RSVP-TC: Assigning WFQ QoS (on FR VC 101) to tcsb 02000406
00:44:49: RSVP-TC: Predicted compression for TCSB 2000406:
00:44:49: RSVP-TC:   method      = rtp
00:44:49: RSVP-TC:   context ID = 2
00:44:49: RSVP-TC:   factor      = 82 percent
00:44:49: RSVP-TC:   bytes-saved = 36 bytes
00:44:49: RSVP-TC: Bandwidth check: requested bw=65600 old bw=0
00:44:49: RSVP-TC: RSVP bandwidth is available
00:44:49: RSVP-TC: Consulting policy for tcsb 02000406
00:44:49: RSVP-TC: Policy granted QoS for tcsb 02000406
00:44:49: RSVP-TC: Requesting QoS for tcsb 02000406
00:44:49: RSVP-TC:   ( r = 8200      bytes/s   M = 164      bytes
00:44:49: RSVP-TC:     b = 328      bytes     m = 164      bytes )
00:44:49: RSVP-TC:     p = 10000    bytes/s   Service Level = priority
```

```
00:44:49: RSVP-WFQ: Update for tcsb 02000406 on FR PVC dlci 101 on Se3/0
00:44:49: RSVP-WFQ: Admitted 66 kbps of bandwidth
00:44:49: RSVP-WFQ: Allocated PRIORITY queue 24
00:44:49: RSVP-TC: Allocation succeeded for tcsb 02000406
```

The following example from the **debug ip rsvp traffic-control** command shows that compression was unsuccessfully predicted because no compression context IDs were available:

```
Router# debug ip rsvp traffic-control
```

```
RSVP debugging is on
```

```
Router# show debugging
```

```
00:10:16:RSVP-TC:Attempting to install QoS for rsb 62CED62C
00:10:16:RSVP-TC:Adding new tcsb 01000421 for rsb 62CED62C
00:10:16:RSVP-TC:Assigning WFQ QoS (on FR VC 101) to tcsb 01000421
00:10:16:RSVP-TC:sender's flow is not rtp compressible for TCSB 1000421
00:10:16:      reason: no contexts available
00:10:16:RSVP-TC:sender's flow is not udp compressible for TCSB 1000421
00:10:16:      reason: no contexts available
00:10:16:RSVP-TC:Bandwidth check:requested bw=80000 old bw=0
00:10:16:RSVP-TC:RSVP bandwidth is available
00:10:16:RSVP-TC:Consulting policy for tcsb 01000421
00:10:16:RSVP-TC:Policy granted QoS for tcsb 01000421
00:10:16:RSVP-TC:Requesting QoS for tcsb 01000421
00:10:16:RSVP-TC:  ( r = 10000      bytes/s   M = 200      bytes
00:10:16:RSVP-TC:      b = 400      bytes     m = 200      bytes )
00:10:16:RSVP-TC:      p = 10000      bytes/s   Service Level = priority
00:10:16:RSVP-WFQ:Update for tcsb 01000421 on FR PVC dlci 101 on Se3/0
00:10:16:RSVP-WFQ:Admitted 80 kbps of bandwidth
00:10:16:RSVP-WFQ:Allocated PRIORITY queue 24
00:10:16:RSVP-TC:Allocation succeeded for tcsb 01000421
```

Related Commands

Command	Description
show debugging	Displays active debugging output.

debug ip rsvp wfq

To display debugging messages for the weighted fair queue (WFQ), use the **debug ip rsvp wfq** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug ip rsvp wfq

no debug ip rsvp wfq

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC

Command History	Release	Modification
	12.1(3)T	This command was introduced.
	12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(18)SXF2	This command was integrated into Cisco IOS Release 12.2(18)SXF2.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples The following is sample output from the **debug ip rsvp wfq** command:

```
Router# debug ip rsvp wfq

RSVP debugging is on

Router# show debugging

IP RSVP debugging is on
IP RSVP debugging (Traffic Control events) is on
IP RSVP debugging (WFQ events) is on
Router#
03:03:23:RSVP-TC:Attempting to install QoS for rsb 6268A538
03:03:23:RSVP-TC:Adding new tcsb 00001A01 for rsb 6268A538
03:03:23:RSVP-TC:Assigning WFQ QoS to tcsb 00001A01
03:03:23:RSVP-TC:Consulting policy for tcsb 00001A01
03:03:23:RSVP-TC:Policy granted QoS for tcsb 00001A01
03:03:23:RSVP-TC:Requesting QoS for tcsb 00001A01
03:03:23:RSVP-TC:   ( r = 12500      bytes/s   M = 1514      bytes
03:03:23:RSVP-TC:     b = 1000      bytes     m = 0          bytes )
03:03:23:RSVP-TC:     p = 12500      bytes/s   Service Level = non-priority
```

```
03:03:23:RSVP-WFQ:Requesting a RESERVED queue on Et0/1 for tcsb 00001A01
03:03:23:RSVP-WFQ:Queue 265 allocated for tcsb 00001A01
03:03:23:RSVP-TC:Allocation succeeded for tcsb 00001A01
```

```
Router# no debug ip rsvp wfq
```

```
RSVP debugging is off
```

Related Commands

Command	Description
show debug	Displays active debugging output.

ip rsvp data-packet classification none

To turn off (disable) Resource Reservation Protocol (RSVP) data packet classification, use the **ip rsvp data-packet classification none** command in interface configuration mode. To turn on (enable) data-packet classification, use the **no** form of this command.

ip rsvp data-packet classification none

no ip rsvp data-packet classification none

Syntax Description This command has no arguments or keywords.

Command Default RSVP data packet classification is disabled.

Command Modes Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXF2	This command was integrated into Cisco IOS Release 12.2(18)SXF2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Use the **ip rsvp data-packet classification none** command when you do not want RSVP to process every packet. Configuring RSVP so that not every packet is processed eliminates overhead and improves network performance and scalability.

Examples

This section contains two examples of the **ip rsvp data-packet classification none** command. In the first example, data packet classification is turned off (disabled), as follows:

```
Router# configure terminal
Router(config)# interface atm6/0
Router(config-if)# ip rsvp data-packet classification none
```

In the second example, data packet classification is turned on (enabled), as follows:

```
Router# configure terminal
Router(config)# interface atm6/0
Router(config-if)# no ip rsvp data-packet classification none
```

Related Commands

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

ip rsvp resource-provider

To configure a resource provider for an aggregate flow, use the **ip rsvp resource-provider** command in interface configuration mode. To disable a resource provider for an aggregate flow, use the **no** form of this command.

ip rsvp resource-provider { none | wfq interface | wfq pvc }

no ip rsvp resource-provider

Syntax Description

none	No resource provider specified regardless of whether one is configured on the interface.
wfq interface	Weighted fair queueing (WFQ) specified as the resource provider on the interface.
wfq pvc	WFQ specified as the resource provider on the permanent virtual circuit (PVC) or connection.

Defaults

The **wfq interface** is the default resource provider that Resource Reservation Protocol (RSVP) configures on the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXF2	This command was integrated into Cisco IOS Release 12.2(18)SXF2.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Use the **ip rsvp resource-provider** command to configure the resource provider with which you want RSVP to interact when it installs a reservation.

To ensure that a flow receives quality of service (QoS) guarantees when using WFQ on a per-flow basis, configure **wfq interface** or **wfq pvc** as the resource provider. To ensure that a flow receives QoS guarantees when using class-based weighted fair queueing (CBWFQ) for data packet processing, configure **none** as the resource provider.



Note

Resource provider was formerly called QoS provider.

Examples

In the following example, the **ip rsvp resource-provider** command is configured with **wfq interface** or **wfq pvc** as the resource provider, ensuring that a flow receives QoS guarantees when using WFQ on a per-flow basis:

```
Router# configure terminal
Router(config)# interface atm6/0
Router(config-if)# ip rsvp resource-provider wfq pvc
```

In the following example, the **ip rsvp resource-provider** command is configured with **none** as the resource provider, ensuring that a flow receives QoS guarantees when using CBWFQ for data packet processing:

```
Router# configure terminal
Router(config)# interface atm6/0
Router(config-if)# ip rsvp resource-provider none
```

Related Commands

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

show ip rsvp installed

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

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

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

Command Modes Privileged EXEC

Command History	Release	Modification
	11.2	This command was introduced.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(15)T	The command output was modified to display the resources required for a traffic control state block (TCSB) after compression has been taken into account.
	12.2(18)SXF2	This command was integrated into Cisco IOS Release 12.2(18)SXF2.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

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

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

```
Router# show ip rsvp installed

RSVP: Ethernet1: has no installed reservations
RSVP: Serial0:
  kbps  To          From          Protocol DPort Sport Weight Conversation
  0     192.168.0.0  172.16.2.28  UDP 20    30    128    270
  150   192.168.0.1  172.16.2.1   UDP 20    30    128    268
  100   192.168.0.1  172.16.1.1   UDP 20    30    128    267
  200   192.168.0.1  172.16.1.25  UDP 20    30    256    265
  200   192.168.0.2  172.16.1.25  UDP 20    30    128    271
  0     192.168.0.2  172.16.2.28  UDP 20    30    128    269
  150   192.168.0.2  172.16.2.1   UDP 20    30    128    266
  350   192.168.0.3  172.16.0.0   UDP 20    30    128    26
```

Table 1 describes the significant fields shown in the display.

Table 1 *show ip rsvp installed Field Descriptions*

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

RSVP Compression Method Prediction Example

The following example of the **show ip rsvp installed detail** command shows the compression parameters, including the compression method, the compression context ID, and the bytes saved per packet, on serial interface 3/0 in effect:

```
Router# show ip rsvp installed detail

RSVP:Ethernet2/1 has no installed reservations

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

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

```
Router# show ip rsvp installed detail

RSVP:Ethernet2/1 has no installed reservations

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

```

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

```

**Note**

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

Related Commands

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

show ip rsvp interface

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
11.2	This command was introduced.
12.2(2)T	The optional detail keyword was added.
12.2(4)T	This command was implemented on the Cisco 7500 series and the ATM-permanent virtual circuit (PVC) interface.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(13)T	The following modifications were made to this command: <ul style="list-style-type: none"> Rate-limiting and refresh-reduction information were added to the output display. This command was modified to display RSVP global settings when no keywords or arguments are entered.
12.2(15)T	The following modifications were made to this command: <ul style="list-style-type: none"> The command output was modified to display the effects of compression on admission control and the RSVP bandwidth limit counter. Cryptographic authentication parameters were added to the display.
12.2(18)SFX2	This command was integrated into Cisco IOS Release 12.2(18)SFX2.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

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

- Total RSVP bandwidth
- RSVP bandwidth allocated to existing flows

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

Examples

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

```
Router# show ip rsvp interface

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

Table 2 describes the fields shown in the display.

Table 2 *show ip rsvp interface Field Descriptions*

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

Detailed RSVP Information Example

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

```
Router# show ip rsvp interface detail

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

PO1/0:
  Bandwidth:
    Curr allocated:0 bits/sec
    Max. allowed (total):50M bits/sec
    Max. allowed (per flow):50M bits/sec
    Max. allowed for LSP tunnels using sub-pools:0 bits/sec
    Set aside by policy (total):0 bits/sec
```

```
Signalling:
  DSCP value used in RSVP msgs:0x3F
  Number of refresh intervals to enforce blockade state:4
  Number of missed refresh messages:4
  Refresh interval:30

PO1/1:
  Bandwidth:
    Curr allocated:0 bits/sec
    Max. allowed (total):50M bits/sec
    Max. allowed (per flow):50M bits/sec
    Max. allowed for LSP tunnels using sub-pools:0 bits/sec
    Set aside by policy (total):0 bits/sec
  Signalling:
    DSCP value used in RSVP msgs:0x3F
    Number of refresh intervals to enforce blockade state:4
    Number of missed refresh messages:4
    Refresh interval:30

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

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

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

Table 3 describes the significant fields shown in the detailed display for interface PO0/0. The fields for the other interfaces are similar.

Table 3 *show ip rsvp interface detail Field Descriptions—Detailed RSVP Information Example*

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

RSVP Compression Method Prediction Example

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

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

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

```

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

```

Table 4 describes the significant fields shown in the display for Ethernet interface 2/1. The fields for serial interface 3/0 are similar.

Table 4 *show ip rsvp interface detail Field Descriptions—RSVP Compression Method Prediction Example*

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

Cryptographic Authentication Example

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

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

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

Table 5 describes the significant fields shown in the display.

Table 5 *show ip rsvp interface detail Field Descriptions—Cryptographic Authentication Example*

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

Table 5 *show ip rsvp interface detail Field Descriptions—Cryptographic Authentication Example (continued)*

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

Related Commands

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

show queueing

To list all or selected configured queueing strategies, use the **show queueing** command in privileged EXEC mode.

```
show queueing [custom | fair | priority | random-detect [interface atm-subinterface
[vc [[vpi/] vci]]]
```

Syntax Description	
custom	(Optional) Status of the custom queueing list configuration.
fair	(Optional) Status of the fair queueing configuration.
priority	(Optional) Status of the priority queueing list configuration.
random-detect	(Optional) Status of the Weighted Random Early Detection (WRED) and distributed WRED (DWRED) configuration, including configuration of flow-based WRED.
interface <i>atm-subinterface</i>	(Optional) Displays the WRED parameters of every virtual circuit (VC) with WRED enabled on the specified ATM subinterface.
vc	(Optional) Displays the WRED parameters associated with a specific VC. If desired, both the virtual path identifier (VPI) and virtual circuit identifier (VCI) values, or just the VCI value, can be specified.
<i>vpi</i>	(Optional) Specifies the VPI. If the <i>vpi</i> argument is omitted, 0 is used as the VPI value for locating the permanent virtual circuit (PVC). If the <i>vpi</i> argument is specified, the / separator is required.
<i>vci</i>	(Optional) Specifies the VCI.

Command Default If no optional keyword is entered, this command shows the configuration of all interfaces.

Command Modes Privileged EXEC

Command History	Release	Modification
	10.3	This command was introduced.
	12.0(4)T	This command was integrated into Cisco IOS Release 12.0(4)T. The red keyword was changed to random-detect .
	12.1(2)T	This command was modified to include information about the Frame Relay PVC Interface Priority Queueing (FR PIPQ) feature.
	12.2(2)T	This command was integrated into Cisco IOS Release 12.2(2)T.
	12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
	12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
	12.2(18)SXF2	This command was integrated into Cisco IOS Release 12.2(18)SXF2.
	12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples**FR PIPQ Example**

The following sample output shows that FR PIPQ (referred to as “DLCI priority queue”) is configured on serial interface 0. The output also shows the size of the four data-link connection identifier (DLCI) priority queues.

Router# **show queueing**

Current fair queue configuration:

Interface	Discard threshold	Dynamic queue count	Reserved queue count
Serial3/1	64	256	0
Serial3/3	64	256	0

Current DLCI priority queue configuration:

Interface	High limit	Medium limit	Normal limit	Low limit
Serial0	20	40	60	80

Current priority queue configuration:

```
List Queue Args
1 low protocol ipx
1 normal protocol vines
1 normal protocol appletalk
1 normal protocol ip
1 normal protocol decnet
1 normal protocol decnet_node
1 normal protocol decnet_rout
1 normal protocol decnet_rout
1 medium protocol xns
1 high protocol clns
1 normal protocol bridge
1 normal protocol arp
```

Current custom queue configuration:

Current random-detect configuration:

Weighted Fair Queueing Example

The following is sample output from the **show queueing** command. There are two active conversations in serial interface 0. Weighted fair queueing (WFQ) ensures that both of these IP data streams—both using TCP—receive equal bandwidth on the interface while they have messages in the pipeline, even though more FTP data is in the queue than remote-procedure call (RCP) data.

Router# **show queueing**

Current fair queue configuration:

Interface	Discard threshold	Dynamic queue count	Reserved queue count
Serial0	64	256	0
Serial1	64	256	0
Serial2	64	256	0
Serial3	64	256	0

Current priority queue configuration:

```
List Queue Args
1 high protocol cdp
2 medium interface Ethernet1
```

Current custom queue configuration:

Current random-detect configuration:

```
Serial5
Queueing strategy:random early detection (WRED)
Exp-weight-constant:9 (1/512)
Mean queue depth:40
```

Class	Random drop	Tail drop	Minimum threshold	Maximum threshold	Mark probability
0	1401	9066	20	40	1/10
1	0	0	22	40	1/10
2	0	0	24	40	1/10
3	0	0	26	40	1/10
4	0	0	28	40	1/10
5	0	0	31	40	1/10
6	0	0	33	40	1/10
7	0	0	35	40	1/10
rsvp	0	0	37	40	1/10

Custom Queueing Example

The following is sample output from the **show queueing custom** command:

```
Router# show queueing custom
```

Current custom queue configuration:

```
List Queue Args
3 10 default
3 3 interface Tunnel3
3 3 protocol ip
3 3 byte-count 444 limit 3
```

Flow-Based WRED Example

The following is sample output from the **show queueing random-detect** command. The output shows that the interface is configured for flow-based WRED to ensure fair packet drop among flows. The **random-detect flow average-depth-factor** command was used to configure a scaling factor of 8 for this interface. The scaling factor is used to scale the number of buffers available per flow and to determine the number of packets allowed in the output queue of each active flow before the queue is susceptible to packet drop. The maximum flow count for this interface was set to 16 by the **random-detect flow count** command.

```
Router# show queueing random-detect
```

Current random-detect configuration:

```
Serial1
Queueing strategy:random early detection (WRED)
Exp-weight-constant:9 (1/512)
Mean queue depth:29
Max flow count:16 Average depth factor:8
Flows (active/max active/max):39/40/16
```

Class	Random drop	Tail drop	Minimum threshold	Maximum threshold	Mark probability
0	31	0	20	40	1/10
1	33	0	22	40	1/10
2	18	0	24	40	1/10
3	14	0	26	40	1/10
4	10	0	28	40	1/10
5	0	0	31	40	1/10
6	0	0	33	40	1/10
7	0	0	35	40	1/10
rsvp	0	0	37	40	1/10

DWRED Example

The following is sample output from the **show queueing random-detect** command for DWRED:

```
Current random-detect configuration:
Serial1
  Queueing strategy:random early detection (WRED)
  Exp-weight-constant:9 (1/512)
  Mean queue depth:29
  Max flow count:16      Average depth factor:8
  Flows (active/max active/max):39/40/16

Class  Random      Tail   Minimum   Maximum   Mark
      drop      drop  threshold threshold probability
0       31           0       20       40       1/10
1       33           0       22       40       1/10
2       18           0       24       40       1/10
3       14           0       26       40       1/10
4       10           0       28       40       1/10
5        0           0       31       40       1/10
6        0           0       33       40       1/10
7        0           0       35       40       1/10
rsvp    0           0       37       40       1/10
```

```
Current random-detect configuration:
FastEthernet2/0/0
  Queueing strategy:fifo
  Packet drop strategy:VIP-based random early detection (DWRED)
  Exp-weight-constant:9 (1/512)
  Mean queue depth:0
  Queue size:0      Maximum available buffers:6308
  Output packets:5 WRED drops:0 No buffer:0

Class  Random      Tail   Minimum   Maximum   Mark      Output
      drop      drop  threshold threshold probability Packets
0       0           0      109      218      1/10      5
1       0           0      122      218      1/10      0
2       0           0      135      218      1/10      0
3       0           0      148      218      1/10      0
4       0           0      161      218      1/10      0
5       0           0      174      218      1/10      0
6       0           0      187      218      1/10      0
7       0           0      200      218      1/10      0
```

[Table 6](#) describes the significant fields shown in the display.

Table 6 *show queueing Field Descriptions*

Field	Description
Discard threshold	Number of messages allowed in each queue.
Dynamic queue count	Number of dynamic queues used for best-effort conversations.
Reserved queue count	Number of reservable queues used for reserved conversations.
High limit	High DLCI priority queue size in maximum number of packets.
Medium limit	Medium DLCI priority queue size, in maximum number of packets.
Normal limit	Normal DLCI priority queue size, in maximum number of packets.

Table 6 *show queueing Field Descriptions (continued)*

Field	Description
Low limit	Low DLCI priority queue size, in maximum number of packets.
List	Custom queueing—Number of the queue list. Priority queueing—Number of the priority list.
Queue	Custom queueing—Number of the queue. Priority queueing—Priority queue level (high , medium , normal , or low keyword).
Args	Packet matching criteria for that queue.
Exp-weight-constant	Exponential weight factor.
Mean queue depth	Average queue depth. It is calculated based on the actual queue depth on the interface and the exponential weighting constant. It is a moving average. The minimum and maximum thresholds are compared against this value to determine drop decisions.
Class	IP Precedence value.
Random drop	Number of packets randomly dropped when the mean queue depth is between the minimum threshold value and the maximum threshold value for the specified IP Precedence value.
Tail drop	Number of packets dropped when the mean queue depth is greater than the maximum threshold value for the specified IP Precedence value.
Minimum threshold	Minimum WRED threshold, in number of packets.
Maximum threshold	Maximum WRED threshold, in number of packets.
Mark probability	Fraction of packets dropped when the average queue depth is at the maximum threshold.

Related Commands

Command	Description
custom-queue-list	Assigns a custom queue list to an interface.
exponential-weighting-constant	Configures the exponential weight factor for the average queue size calculation for a WRED parameter group.
fair-queue (WFQ)	Enables WFQ for an interface.
frame-relay interface-queue priority	Enables the FR PIPQ feature.
precedence (WRED group)	Configures a WRED group for a particular IP Precedence.
priority-group	Assigns the specified priority list to an interface.
priority-list interface	Establishes queueing priorities on packets entering from a given interface.
priority-list queue-limit	Specifies the maximum number of packets that can be waiting in each of the priority queues.
queue-list interface	Establishes queueing priorities on packets entering on an interface.
queue-list queue byte-count	Specifies how many bytes the system allows to be delivered from a given queue during a particular cycle.

Command	Description
random-detect (interface)	Enables WRED or DWRED.
random-detect flow average-depth-factor	Sets the multiplier to be used in determining the average depth factor for a flow when flow-based WRED is enabled.
random-detect flow count	Sets the flow count for flow-based WRED.
show interfaces	Displays the statistical information specific to a serial interface.
show queue	Displays the contents of packets inside a queue for a particular interface or VC.
show queueing interface	Displays the queueing statistics of an interface or VC.

Glossary

admission control—The process in which an RSVP reservation is accepted or rejected based on end-to-end available network resources.

aggregate—A collection of packets with the same DSCP.

bandwidth—The difference between the highest and lowest frequencies available for network signals. This term also describes the rated throughput capacity of a given network medium or protocol.

CBWFQ—class-based weighted fair queueing. A queueing mechanism that extends the standard WFQ functionality to provide support for user-defined traffic classes.

DiffServ—An architecture based on a simple model where traffic entering a network is classified and possibly conditioned at the boundaries of the network. The class of traffic is then identified with a DS code point or bit marking in the IP header. Within the core of the network, packets are forwarded according to the per-hop behavior associated with the DS code point.

DSCP—differentiated services code point. The six most significant bits of the 1-byte IP type of service (ToS) field. The per-hop behavior represented by a particular DSCP value is configurable. DSCP values range between 0 and 63.

enterprise network—A large and diverse network connecting most major points in a company or other organization.

flow—A stream of data traveling between two endpoints across a network (for example, from one LAN station to another). Multiple flows can be transmitted on a single circuit.

packet—A logical grouping of information that includes a header containing control information and (usually) user data. Packets most often refer to network layer units of data.

PBX—private branch exchange. A digital or analog telephone switchboard located on the subscriber premises and used to connect private and public telephone networks.

PHB—per-hop behavior. A DiffServ concept that specifies how specifically marked packets are to be treated by each DiffServ router.

QoS—quality of service. A measure of performance for a transmission system that reflects its transmission quality and service availability.

RSVP—Resource Reservation Protocol. A protocol for reserving network resources to provide quality of service guarantees to application flows.

VoIP—Voice over IP. The ability to carry normal telephony-style voice over an IP-based internet maintaining telephone-like functionality, reliability, and voice quality.

WFQ—weighted fair queueing. A queue management algorithm that provides a certain fraction of link bandwidth to each of several queues, based on relative bandwidth applied to each of the queues.

**Note**

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2001, 2006, 2007 Cisco Systems, Inc. All rights reserved.

