Control Plane DSCP Support for RSVP

First Published: June 7, 2001
Last Updated: February 19, 2007

The Control Plane DSCP Support for RSVP feature lets you prioritize Resource Reservation Protocol (RSVP) messages to improve delivery by decreasing the likelihood of high priority messages being dropped.

History for the Control Plane DSCP Support for RSVP Feature

Release	Modification
12.2(2)T	This feature was introduced.
12.2(18)SXF2	This feature was integrated into Cisco IOS Release 12.2(18)SXF2.
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

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

Prerequisites for Control Plane DSCP Support for RSVP

The network must support RSVP before you can enable the Control Plane DSCP Support for RSVP feature.

Restrictions for Control Plane DSCP Support for RSVP

You can configure the Control Plane DSCP Support for RSVP feature on interfaces and subinterfaces only. This feature affects all RSVP messages that are sent out the interface or that are on any logical circuit of the interface, including subinterfaces, permanent virtual circuits (PVCs), and switched virtual circuits (SVCs).

Information About Control Plane DSCP Support for RSVP

To use the Control Plane DSCP Support for RSVP feature, you need to understand the following concepts:

- Feature Overview of Control Plane DSCP Support for RSVP, page 2
- Benefits of Control Plane DSCP Support for RSVP, page 3

Feature Overview of Control Plane DSCP Support for RSVP

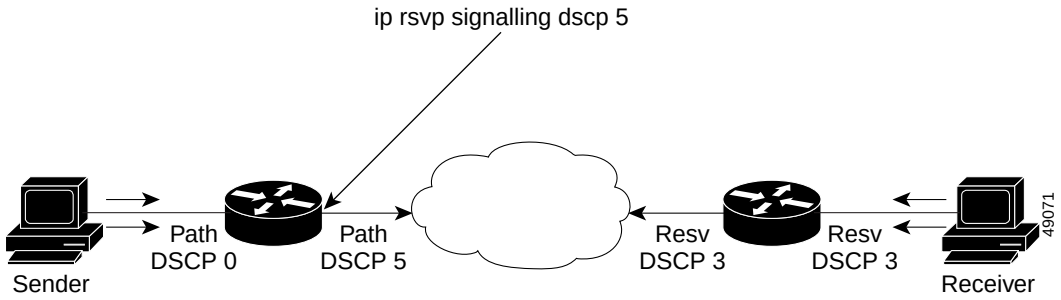
Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

Before traffic can be handled according to its unique requirements, it must be identified or labeled (that is, classified). There are numerous classification techniques for doing this. These include Layer 3 schemes such as IP precedence or the differentiated services code point (DSCP), Layer 2 schemes such as 802.1P, and implicit characteristics of the data itself, such as the traffic type using the Real-Time Transport Protocol (RTP) and a defined port range.

The Control Plane DSCP Support for RSVP feature allows you to set the priority value in the type of service (ToS) byte/differentiated services (DiffServ) field in the Internet Protocol (IP) header for RSVP messages. The IP header functions with resource providers such as weighted fair queueing (WFQ), so that voice frames have priority over data fragments and data frames. When packets arrive in a router's output queue, the voice packets are placed ahead of the data frames.

Figure 1 shows a path message originating from a sender with a DSCP value of 0 (the default) that is changed to 5 to give the message a higher priority and a reservation (resv) message originating from a receiver with a DSCP of 3.

Figure 1 Control Plane DSCP Support for RSVP



Raising the DSCP value reduces the possibility of packets being dropped, thereby improving call setup time in VoIP environments.

Benefits of Control Plane DSCP Support for RSVP

Faster Call Setup Time

The Control Plane DSCP Support for RSVP feature allows you to set the priority for RSVP messages. In a DiffServ QoS environment, higher priority packets get serviced before lower priority packets, thereby improving the call setup time for RSVP sessions.

Improved Message Delivery

During periods of congestion, routers drop lower priority traffic before they drop higher priority traffic. Since RSVP messages can now be marked with higher priority, the likelihood of these messages being dropped is significantly reduced.

Faster Recovery After Failure Conditions

When heavy congestion occurs, many packets are dropped. Network resources attempt to retransmit almost instantaneously resulting in further congestion. This leads to a considerable reduction in throughput.

Previously, RSVP messages were marked best effort and subject to being dropped by congestion avoidance mechanisms such as weighted random early detection (WRED). However, with the Control Plane DSCP Support for RSVP feature, RSVP messages are likely to be dropped later, if at all, thereby providing faster recovery of RSVP reservations.

How to Configure Control Plane DSCP Support for RSVP

This section contains the following procedures:

- Enabling RSVP on an Interface, page 4 (required)
- Specifying the DSCP, page 5 (required)
- Verifying the Configuration, page 6 (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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [*name-tag*] **Example:** `Router(config)# interface Ethernet0/0`	Configures the interface type and enters interface configuration mode. • The optional *name-tag* 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 bandwidth** [*interface-kbps*] [*single-flow-kbps*] **Example:** `Router(config-if)# ip rsvp bandwidth 7500 7500`	Enables RSVP on an interface. • The optional *interface-kbps* and *single-flow-kbps* 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. **Note** Repeat this command for each interface that you want to enable.
Step 5	**end** **Example:** `Router(config-if)# end`	(Optional) Exits to privileged EXEC mode.

Specifying the DSCP

Perform this task to specify the DSCP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number* [*name-tag*]
4. **ip rsvp signalling dscp** *value*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* [*name-tag*] **Example:** `Router(config)# interface Ethernet0/0`	Configures the interface type and enters interface configuration mode. • The optional *name-tag* 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 signalling dscp** *value* **Example:** `Router(config-if)# ip rsvp signalling dscp 6`	Specifies the DSCP value to be used on all RSVP messages transmitted on an interface. • Enter a number from 0 to 63.
Step 5	**end** **Example:** `Router(config-if)# end`	(Optional) Exits to privileged EXEC mode.

Verifying the Configuration

Perform the following task to verify that the Control Plane DSCP Support for RSVP feature has been configured.

SUMMARY STEPS

1. **enable**
2. **show ip rsvp interface** [*interface-type interface-number*] [**detail**]
3. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip rsvp interface** [*interface-type interface-number*] [**detail**] **Example:** `Router# show ip rsvp interface detail`	Displays RSVP-related information. • The optional *interface-type* specifies the type of the interface. • The optional *interface-number* specifies the number of the interface. • The optional **detail** keyword displays additional information about interfaces.
Step 3	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode.

Examples

This section provides the following example output:

Sample Output for the show ip rsvp interface detail Command

In the following sample output from the **show ip rsvp interface detail** command, only the serial interface 2/0 has DSCP configured. Interfaces that are not configured for DSCP do not show the DSCP value, which is 0 by default.

```
Router# show ip rsvp interface detail

Et1/1:
   Bandwidth:
     Curr allocated:0M bits/sec
     Max. allowed (total):7500K bits/sec
     Max. allowed (per flow):7500K bits/sec
   Neighbors:
     Using IP enacp:1.  Using UDP encaps:0
```

```
 Et1/2:
   Bandwidth:
     Curr allocated:0M bits/sec
     Max. allowed (total):7500K bits/sec
     Max. allowed (per flow):7500K bits/sec
   Neighbors:
     Using IP enacp:0.  Using UDP encaps:0

Se2/0:
   Bandwidth:
     Curr allocated:10K bits/sec
     Max. allowed (total):1536K bits/sec
     Max. allowed (per flow):1536K bits/sec
   Neighbors:
     Using IP enacp:1.  Using UDP encaps:0
   DSCP value used in Path/Resv msgs:0x6
   Burst Police Factor:300%
   RSVP:Data Packet Classification provided by: none
```

Configuration Examples for Control Plane DSCP Support for RSVP

This section provides the following configuration examples:

- Configuring a DSCP: Example, page 7
- Verifying Control Plane DSCP Support for RSVP: Example, page 7

Configuring a DSCP: Example

The following example configures a DSCP value on an interface:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface Serial2/0
Router(config-if)# ip rsvp signalling dscp 48
```

Verifying Control Plane DSCP Support for RSVP: Example

The following example verifies that the Control Plane DSCP Support for RSVP feature has been configured:

```
Router# show running-config interface Serial2/0

 interface Serial2/0
 ip address 10.1.1.1 255.255.255.0
 fair-queue 64 256 235
 ip rsvp signalling dscp 48
 ip rsvp bandwidth 7500 7500
```

Additional References

The following sections provide references related to the Control Plane DSCP Support for RSVP Scalability feature.

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples.	• *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 12.4T

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	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	*Resource Reservation Protocol*
RFC 2206	*RSVP Management Information Base Using SMIv*

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 only commands that are modified.

- **ip rsvp signalling dscp**
- **show ip rsvp interface**

ip rsvp signalling dscp

To specify the differentiated services code point (DSCP) value to be used on all Resource Reservation Protocol (RSVP) messages transmitted on an interface, use the **ip rsvp signalling dscp** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip rsvp signalling dscp *value*

no ip rsvp signalling dscp

Syntax Description

value	A number for the DSCP. Range is from 0 to 63. Default is 0.

Defaults

The default value is 0.

Command Modes

Interface configuration.

Command History

Release	Modification
12.1	This command was introduced
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

You configure the DSCP per interface, not per flow. The DSCP determines the priority that a packet receives from various hops as it travels to its destination.

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

Examples

Here is an example of the **ip rsvp signalling dscp** command with a DSCP value of 6

```
Router(config-if)# ip rsvp signalling dscp 6
Router(config-if)# end
```

To verify the DSCP value, enter the **show ip rsvp interface detail** command:

```
Router# show ip rsvp interface serial2/0 detail

Se2/0:
   Bandwidth:
     Curr allocated:10K bits/sec
     Max. allowed (total):1536K bits/sec
     Max. allowed (per flow):1536K bits/sec
```

```
Neighbors:
  Using IP enacp:1.  Using UDP encaps:0
DSCP value used in Path/Resv msgs:0x6
Burst Police Factor:300%
RSVP:Data Packet Classification provided by: none
```

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

interface-type	(Optional) Type of the interface.
interface-number	(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: • 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: • 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 1 describes the fields shown in the display.

Table 1 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 2 describes the significant fields shown in the detailed display for interface PO0/0. The fields for the other interfaces are similar.

Table 2 show ip rsvp interface detail Field Descriptions—Detailed RSVP Information Example

Field	Description
PO0/0	Interface name.
Bandwidth	The RSVP bandwidth parameters in effect including the following: • 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	The RSVP signalling parameters in effect including the following: • 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 3 describes the significant fields shown in the display for Ethernet interface 2/1. The fields for serial interface 3/0 are similar.

Table 3 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: • 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: • Header Compression methods supported: – 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 4 describes the significant fields shown in the display.

Table 4 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: • 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 4 show ip rsvp interface detail Field Descriptions—Cryptographic Authentication Example (continued)

Field	Description
Authentication	Authentication is either enabled (active) or disabled (inactive). The parameters include the following: • 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.

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.