

# COPS for RSVP

---

## Feature Overview

Common Open Policy Service (COPS) is a protocol for communicating network traffic policy information to network devices. Resource ReSerVation Protocol (RSVP) is a means for reserving network resources—primarily bandwidth—to guarantee that applications transmitting end-to-end across the Internet will perform at the desired speed and quality.

Combined, COPS with RSVP gives network managers centralized monitoring and control of RSVP, including the ability to:

- Ensure adequate bandwidth and jitter & delay bounds for time-sensitive traffic such as voice transmission
- Ensure adequate bandwidth for multimedia applications such as videoconferencing and distance learning
- Prevent bandwidth-hungry applications from delaying top priority flows or harming the performance of other applications customarily run over the same network

In so doing, COPS for RSVP supports the following crucial RSVP features:

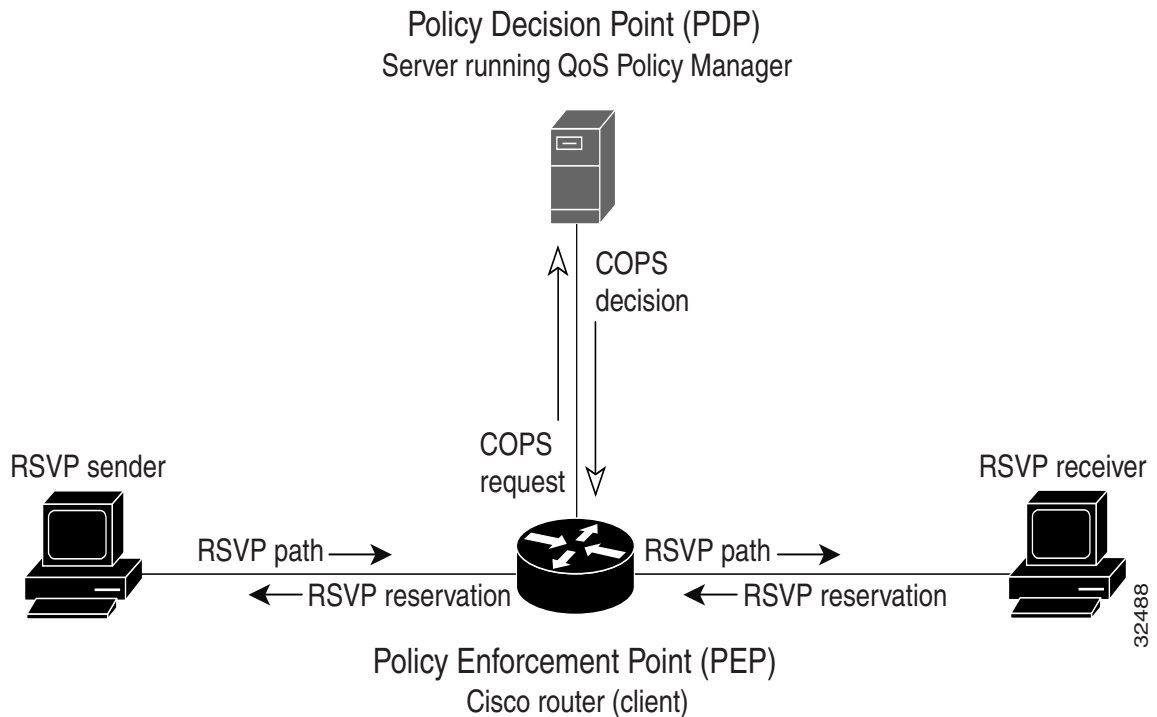
- Admission control—The RSVP reservation is accepted or rejected based on *end-to-end* available network resources.
- Bandwidth guarantee—The RSVP reservation, if accepted, will guarantee that those reserved resources will continue to be available while the reservation is in place.
- Media-independent reservation—An end-to-end RSVP reservation can span arbitrary lower layer media types.
- Data classification—While a reservation is in place, data packets belonging to that RSVP flow are separated from other packets and forwarded as part of the reserved flow.
- Data policing—Data packets belonging to an RSVP flow that exceed the reserved bandwidth size are marked with a lower packet precedence.

## How COPS for RSVP Works

You configure a router to process all RSVP messages coming to it according to policies stored on a particular policy server (called the Policy Decision Point or PDP):

- 1 First, at the PDP server you enter the policies — using Cisco's *COPS QoS Policy Manager* or a compatible policy manager application.

**Figure 1 Sample Arrangement of COPS with RSVP**



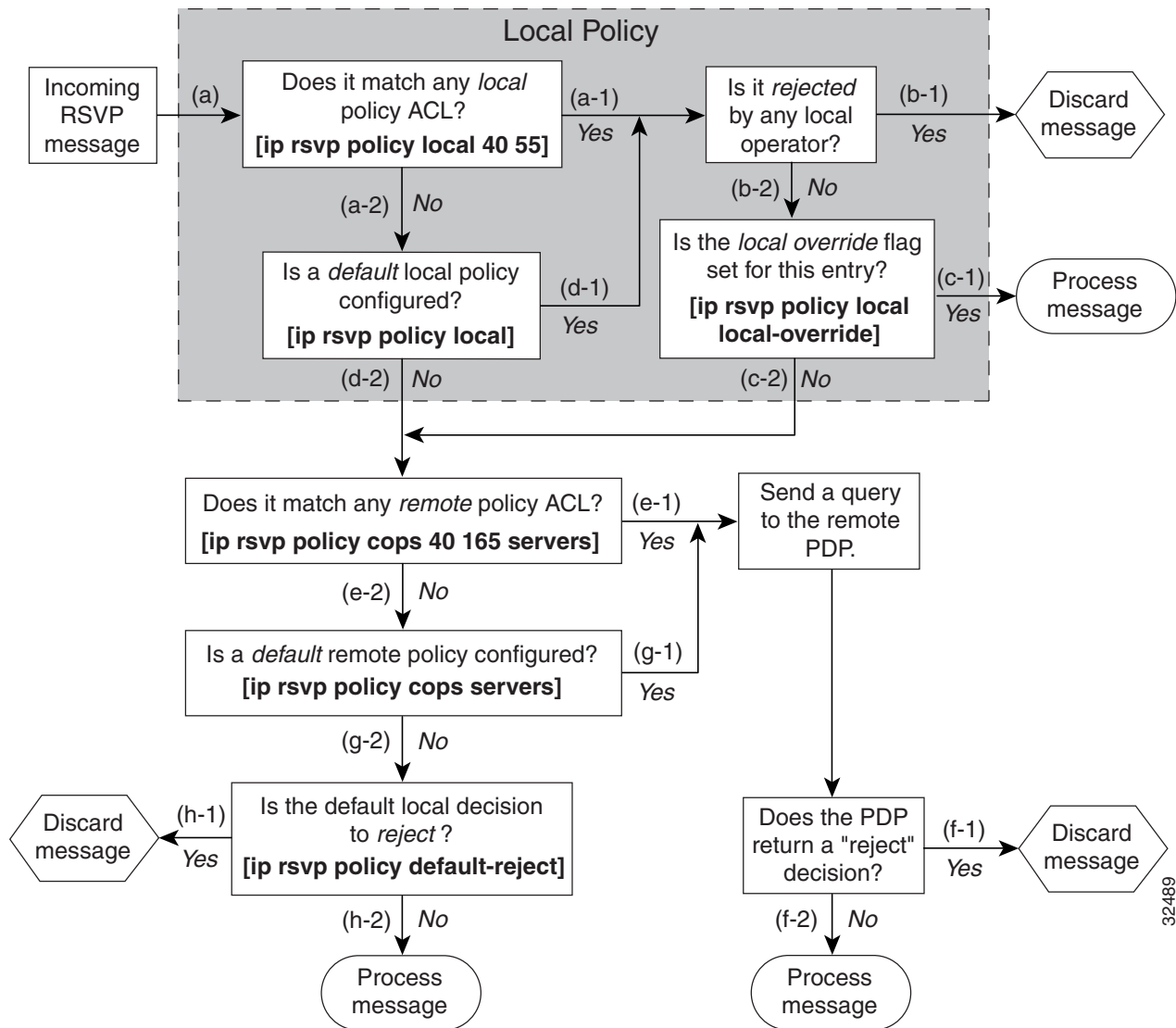
- 2 You configure the router (through its command line interface) to request decisions from the server regarding RSVP messages.
- 3 After that configuration, network flows are processed by the router (Policy Enforcement Point — PEP), as follows:
  - (a) When an RSVP signaling message arrives at the router, the router asks the PDP server how to process the message — either to accept, reject, forward, or install the message.
  - (b) The PDP server sends its decision to the router, which then processes the message as instructed.
- 4 Alternatively, you may configure the router to make those decisions itself (“locally”) without it having to consult first with the PDP server. (The local feature is not supported in this release but will be in a future release.)

## A Detailed Look at COPS-RSVP Functioning

The diagram in Figure 2 traces options available in policy management of RSVP message flows. For each option, an example of the router configuration command used for setting that option is given in brackets and boldface type.

The shaded area covers local policy operations; the remainder of the diagram illustrates remote policy operation. (Configuring local policy will be available in a future release.)

Figure 2 Steps in Processing RSVP PATH and RESV Messages



- (a) The router receives a PATH or RESV message and first tries to adjudicate it locally (that is, without referring to the policy server). If the router has been configured to adjudicate specific access control lists (ACLs) locally and the message matches one of those lists (a-1), the router's policy module applies the operators with which it had been configured. Otherwise, policy processing continues (a-2).
- (b) For each message rejected by the operators, the router sends an ERROR message to the sender and removes the PATH/RESV from the database (b-1). If the message is not rejected, policy processing continues (b-2).
- (c) If the local override flag is set for this entry, the message is immediately accepted with the specified policy operators (c-1). Otherwise, policy processing continues (c-2).
- (d) If the message does not match any ACL configured for local policy (a-2), the router applies the default local policy (d-1). However, if no default local policy has been configured, the message is directed toward remote policy processing (d-2).

- (e) If the router has been configured with specific ACLs against specific policy servers (PDPs), and the message matches one of these ACLs, the router sends that message to the specific PDP for adjudication (e-1). Otherwise, policy processing continues (e-2).
- (f) If the PDP specifies a "reject" decision (f-1), the message is discarded and an ERROR message is sent back to the sender, indicating this condition. If the PDP specifies an "accept" decision (f-2), the message is accepted and processed using normal RSVP processing rules.
- (g) If the message does not match any ACL configured for specific PDPs (e-2), the router applies the *default* PDP configuration. If a default COPS configuration has been entered, policy processing continues (g-1). Otherwise, the message is considered to be unmatched (g-2).
- (h) If the default policy decision for unmatched messages is to reject (h-1), the message is immediately discarded and an ERROR message is sent to the sender indicating this condition. Otherwise, the message is accepted and processed using normal RSVP processing rules (h-2).

Here are certain further, helpful details about PDP-PEP communication and processing:

### **Policy request timer**

Whenever a request for adjudication (of any sort) is sent to a PDP, a 30-second timer associated with the PATH/RESV is started. If the timer runs out before the PDP replies to the request, the PDP is assumed to be down and the request is given to the default policy (step g-2 in Figure 2).

### **PDP tracking of PEP reservations**

When the PDP specifies that a reservation can be installed, this reservation must then be installed on the router. Once bandwidth capacity has been allocated and the reservation installed, the PEP's policy module sends a COMMIT message to the PDP. But if the reservation could not be installed because of insufficient resources, the reservation is folded back to the non-installed state and a NO-COMMIT is sent to the PDP. If the reservation was also new (no previous state), then a DELETE REQUEST instead is sent to the PDP. In these ways, the PDP can keep track of reservations on the PEP.

### **Re-synchronization**

If the PDP sends a SYNCHRONIZE-REQUEST message to the PEP, the PEP's policy module scans its database for all paths/reservations that were previously adjudicated by this PDP, and resends requests for them. The previously adjudicated policy information is retained until a new decision is received. When all the PATH/RESV states have been reported to the PDP, a SYNCHRONIZE-COMPLETE message is sent by the policy module to the PDP. The PEP also sends queries concerning all flows that were locally adjudicated while the PDP was down.

### **Re-adjudication**

- 1 So long as flows governed by the RSVP session continue to pass through the PEP router, the PDP can unilaterally decide to re-adjudicate any of that session's COPS decisions. For example, the PDP might decide that a particular flow that was earlier granted acceptance now needs to be rejected (due perhaps to a sudden preemption or timeout). In such cases, the PDP sends a new decision message to the PEP, which then adjusts its behavior accordingly.
- 2 If the PEP router receives a reservation message in which an object has changed, the policy decision needs to be re-adjudicated. For example, if the sender wants to increase or decrease the bandwidth reservation, a new policy decision must be made. In such cases, the policy flags previously applied to this session are retained, and the session is re-adjudicated.

### Tear-downs

The PEP's policy module is responsible for notifying the PDP whenever a reservation/path that was previously established through policy is torn down for any reason. The PEP does this by sending the PDP a DELETE REQUEST message.

### Connection management

- 1 If the connection to the PDP is closed (either because the PDP closed the connection, a TCP/IP error occurred, or the keepalives failed), the PEP issues a CLIENT-CLOSE message and then attempts to reconnect to the same PDP. If the PEP receives a CLIENT-CLOSE containing a PDP redirect address, the PEP attempts to connect to the redirected PDP.
- 2 If either attempt fails, the PEP attempts to connect to the PDP(s) previously specified in the configuration command **ip rsvp policy cops servers**, obeying the sequence of servers given in that command, always starting with the first server in that list.
- 3 If the PEP reaches the end of the list of servers without connecting, it waits a certain time (called the "reconnect delay") before trying again to connect to the first server in the list. This reconnect delay is initially 30 seconds, and doubles each time the PEP reaches the end of the list without having connected, until the reconnect delay becomes its maximum of 30 minutes. As soon as a connection is made, the delay is reset to 30 seconds.

### Replacement Objects

The following matrix identifies objects that the PDP can replace within RSVP messages passing through the PEP.

Message Context	Objects				Items Affected
	Policy	TSpec	Flowspec	Errorspec	
PATH IN	X	X			1. Installed PATH state. 2. All outbound PATH messages for this PATH.
PATH OUT	X	X			This refresh of the PATH (but not the installed PATH state).
RESV IN	X		X		1. Installed RESV state (incoming as well as traffic control installation). 2. All outbound RESV messages for this RESV.
RESV ALLOC			X		Installed resources for this session.
RESV OUT	X		X		This particular refresh of the RESV (but not the installed RESV state nor the traffic control allocation).
PATHERROR IN	X			X	The forwarded PATHERROR message.
PATHERROR OUT	X			X	The forwarded PATHERROR message.
RESVERROR IN	X			X	All RESVERRORS forwarded by this router.
RESVERROR OUT	X			X	This particular forwarded RESVERROR message.

If an RSVP message whose object was replaced is later refreshed from upstream, the PEP keeps track of both the old and new versions of the object, and does not wrongly interpret the refresh as a change in the PATH/RESV state.

## Restrictions

This release does not support RSVP+.

## Supported Platforms and Interfaces

COPS for RSVP functions on the following platforms, running IOS:

- Cisco 7500 series (non-VIP)
- Cisco 7200 series

COPS for RSVP functions on the following interfaces:

- Ethernet
- Fast Ethernet
- Serial: V.35, EIA/TIA-232, RS-449, and RS-530
- High-speed Serial Interface (HSSI)
- ISDN PRI and ISDN BRI
- ATM
- T1/E1

## Prerequisites

In order to use the COPS for RSVP feature, your network must be running Cisco IOS 12.1(1)T or higher.

Moreover, a compatible policy server must be connected to the network, such as Cisco's *COPS QoS Policy Manager*.

## Supported MIBs and RFCs

Currently there are no MIBs for COPS for RSVP.

COPS for RSVP conforms to the following RFCs:

- *COPS Usage for RSVP* (IETF RFC 2749) by J. Boyle, R. Cohen, D. Durham, S. Herzog, R. Rajan, and A. Sastry
- *Resource ReSerVation Protocol (RSVP)* (IETF RFC 2205) by R. Braden (Ed.), L. Zhang, S. Berson, S. Herzog, and S. Jamin

You may also want to consult this related RFC:

- *The COPS (Common Open Policy Service) Protocol* (IETF RFC 2748) by J. Boyle, R. Cohen, D. Durham, S. Herzog, R. Rajan, and A. Sastry

## Related Features and Technologies

COPS QoS Policy Manager

## Related Documents

- *Cisco IOS Release 12.1 Documentation Set*  
(<http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/index.htm>), in particular the chapter, *Configuring RSVP*, in the *Quality of Service Solutions Configuration Guide*  
([http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/qos\\_c/qcprt5/qcdrsvp.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgr/qos_c/qcprt5/qcdrsvp.htm))
- *COPS QoS Policy Manager Documentation Set*  
<http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ciscoasu/class/index.htm>

## Configuration Tasks

To configure the router (PEP) to process COPS for RSVP, you must at least:

- Specify the COPS server(s) to the router
- Enable COPS for RSVP on the router

You can do both at once, using the command **ip rsvp policy cops [acl] servers**.

Optionally, you can also customize the router to:

- Apply the RSVP policy only to certain access control lists (using the **acl** argument within the same command: **ip rsvp policy cops [acl] servers**)
- Reject all unmatched RESV and PATH messages (using the command **ip rsvp policy default-reject**)
- Accelerate flow processing by confining policy adjudication to just PATH and RESV messages (**ip rsvp policy cops minimal**)
- Hold RSVP information for a specified time after loss of connection with the COPS server (**ip rsvp policy cops timeout**)
- Report the results of outsourcing decisions (not just configuration decisions) to the PDP (**ip rsvp policy cops report-all**)

## Specify COPS servers and enable COPS for RSVP

Step	Command	Purpose
1	router-1# <b>configure terminal</b>	Enters global configuration mode.
2	router-1(config)# <b>ip rsvp policy cops servers 161.44.130.168 161.44.129.6</b>	Tells router to request RSVP policy decisions from the first server listed, and if that fails to connect, from the next server listed. Also enables COPS-RSVP client on the router.
3	router-1(config)# <b>exit</b>	Exits configuration mode.

## Restrict RSVP policy to certain access control lists

Step	Command	Purpose
1	router-1# <b>configure terminal</b>	Enters global configuration mode.
2	router-1(config)# <b>ip rsvp policy cops 40 160 servers 161.44.130.164 161.44.129.2</b>	Tells router to apply RSVP policy to messages that match access control lists #40 and #160, and specifies the servers for those sessions.
3	router-1(config)# <b>exit</b>	Exits configuration mode.

## Reject unmatched RSVP messages

Step	Command	Purpose
1	rtr-1# <b>configure terminal</b>	Enters global configuration mode.

Step	Command	Purpose
2	<code>rtr-1(config)# ip rsvp policy default-reject</code>	Tells router to reject unmatched PATH and RESV messages, instead of just letting them pass through unadjudicated.
3	<code>rtr-1(config)# exit</code>	Exits configuration mode.

## Confine policy to just PATH and RESV messages

Step	Command	Purpose
1	<code>router-1# configure terminal</code>	Enters global configuration mode.
2	<code>router-1(config)# ip rsvp policy cops minimal</code>	Tells router to adjudicate only PATH and RESV messages, and to accept and pass onward PATH ERROR, RESV ERROR, and RESV CONFIRM messages.
3	<code>router-1(config)# exit</code>	Exits configuration mode.

## Keep RSVP information after losing connection with COPS server

Step	Command	Purpose
1	<code>router-1# configure terminal</code>	Enters global configuration mode.
2	<code>router-1(config)# ip rsvp policy cops timeout 600</code>	Tells router to hold policy information for 10 minutes (600 seconds) while attempting to reconnect to a COPS server.
3	<code>router-1(config)# exit</code>	Exits configuration mode.

## Report the results of outsourcing and configuration decisions

Step	Command	Purpose
1	<code>router-1# configure terminal</code>	Enters global configuration mode.
2	<code>router-1(config)# ip rsvp policy cops report-all</code>	Tells router to report to the PDP the success or failure of outsourcing as well as configuration decisions.
3	<code>router-1(config)# exit</code>	Exits configuration mode.

## Verifying Configuration

You can obtain three views of the COPS-RSVP configuration on the PEP router:

- Policy server address(es), port, state, keepalives, and policy client information.  
For this information enter the command **show cops servers**:

```
router-1# show cops servers
COPS SERVER: Address: 161.44.135.172. Port: 3288. State: 0. Keepalive: 120 sec
              Number of clients: 1. Number of sessions: 1.
COPS CLIENT: Client type: 1. State: 0.
```

- Policy server address(es), ACL IDs, and client-server connection status.  
For this information enter the command **show ip rsvp policy cops**:

```
router-1# show ip rsvp policy cops
COPS/RSVP entry. ACLs: 40 60
PDPs: 161.44.135.172
Current state: Connected
Currently connected to PDP 161.44.135.172, port 0
```

- ACL IDs and their connection status.  
For this information enter the command **show ip rsvp policy**:

```
router-1# show ip rsvp policy
Local policy: Currently unsupported
COPS:
ACLs: 40 60 . State: CONNECTED.
ACLs: 40 160 . State: CONNECTING.
```

# Configuration Examples

This section provides the following configuration examples:

- Using the one mandatory configuration command
- Using the remaining configuration commands -- to customize the router's COPS-RSVP behavior

Using the one mandatory configuration command (and implicitly accepting defaults for all the others)

```
router-1# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
  
router-1(config)# ip rsvp policy cops servers 161.44.130.168 161.44.129.6  
  
router-1(config)# exit
```

Using the remaining COPS configuration commands (to customize the router's RSVP behavior)

```
router-1# configure terminal  
Enter configuration commands, one per line. End with CNTL/Z.  
  
router-1(config)# ip rsvp policy cops 40 160 servers 161.44.130.168 161.44.129.6  
  
router-1(config)# ip rsvp policy default-reject  
  
router-1(config)# ip rsvp policy cops minimal  
  
router-1(config)# ip rsvp policy cops timeout 600  
  
router-1(config)# ip rsvp policy cops report-all  
  
router-1(config)# exit
```

## Command Reference

This section documents new and modified commands related to COPS for RSVP. All other commands used with this feature are documented in the Cisco IOS Release 12.1(1)T command references.

The following commands are described here:

- **ip rsvp policy cops minimal**
- **ip rsvp policy cops report-all**
- **ip rsvp policy cops servers**
- **ip rsvp policy cops timeout**
- **ip rsvp policy default-reject**
- **show cops servers**
- **show ip rsvp policy cops**

## ip rsvp policy cops minimal

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

**ip rsvp policy cops minimal**

**no ip rsvp policy cops minimal**

### Syntax Description

There are no additional keywords or arguments for this command.

### Default

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

### Command Mode

Global configuration

### Command History

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

### Usage Guidelines

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

### Examples

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

```
rtr-9(config)#ip rsvp policy cops minimal
```

In the following example, that restriction is removed:

```
rtr-9(config)#no ip rsvp policy cops minimal
```

## ip rsvp policy cops report-all

In the default state, the router reports to the PDP when it has succeeded or failed to implement RSVP configuration decisions. If you want the router to report also on its success and failure with outsourcing decisions, use the **ip rsvp policy cops report-all** command. To return the router to its default, use the **no** form of this command.

**ip rsvp policy cops report-all**

**no ip rsvp policy cops report-all**

---

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

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

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

---

### Syntax Description

There are no additional keywords or arguments for this command.

### Default

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

### Command Mode

Global configuration

### Command History

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

### Usage Guidelines

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

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

### Examples

In order to show the PEP-to-PDP reporting process, the following example has the **debug cops** command already enabled when a new PATH message arrives at the router:

```
router-1(config)# ip rsvp policy cops report-all
router-1(config)# 00:02:48:COPS:** SENDING MESSAGE **
```

**Contents of router's request to PDP:**

```
COPS HEADER:Version 1, Flags 0, Opcode 1 (REQ), Client-type:1, Length:216
HANDLE (1/1) object. Length:8.    00 00 02 01
CONTEXT (2/1) object. Length:8.    R-type:5.    M-type:1
IN_IF (3/1) object. Length:12.    Address:10.1.2.1.    If_index:4
OUT_IF (4/1) object. Length:12.    Address:10.33.0.1.    If_index:3
CLIENT SI (9/1) object. Length:168.    CSI data:
```

**[A 27-line Path message omitted here]**

```
00:02:48:COPS:Sent 216 bytes on socket,
00:02:48:COPS:Message event!
00:02:48:COPS:State of TCP is 4
00:02:48:In read function
00:02:48:COPS:Read block of 96 bytes, num=104 (len=104)
00:02:48:COPS:** RECEIVED MESSAGE **
```

**Contents of PDP's decision received by router:**

```
COPS HEADER:Version 1, Flags 1, Opcode 2 (DEC), Client-type:1, Length:104
HANDLE (1/1) object. Length:8.    00 00 02 01
CONTEXT (2/1) object. Length:8.    R-type:1.    M-type:1
DECISION (6/1) object. Length:8.    COMMAND cmd:1, flags:0
DECISION (6/3) object. Length:56.    REPLACEMENT
```

**[A 52-byte replacement object omitted here]**

```
CONTEXT (2/1) object. Length:8.    R-type:4.    M-type:1
DECISION (6/1) object. Length:8.    COMMAND cmd:1, flags:0
00:02:48:Notifying client (callback code 2)
00:02:48:COPS:** SENDING MESSAGE **
```

**Contents of router's report to PDP:**

```
COPS HEADER:Version 1, Flags 1, Opcode 3 (RPT), Client-type:1, Length:24
HANDLE (1/1) object. Length:8.    00 00 02 01
REPORT (12/1) object. Length:8.    REPORT type COMMIT (1)
00:02:48:COPS:Sent 24 bytes on socket,
```

## ip rsvp policy cops servers

To specify that RSVP should use COPS policy for remote adjudication, use the **ip rsvp policy cops servers** command. To turn off the use of COPS for RSVP, use the **no** form of this command.

**ip rsvp policy cops** [*acl . . .*] **servers** *server\_ip* [*server\_ip . . .*]

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

### Syntax Description

<i>acl</i>	The access control list(s) whose sessions will be governed by the COPS policy.
<b>servers</b>	Precedes the server(s) that govern the COPS policy.
<i>server_ip</i>	IP address(es) of the server(s) governing the COPS policy. As many as eight servers can be specified, with the first being treated as the primary server, and so on down the list.

### Default

If no access control list is specified, the default behavior is for all reservations to be governed by the specified policy server(s).

### Command Mode

Global configuration

### Command History

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

### Usage Guidelines

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

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

If the router's connection to the server breaks, the router tries to reconnect to that same server. If the reconnection attempt fails, the router then obeys an algorithm described in the "Connection management" section of this document.

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

## Examples

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

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

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

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

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

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



## ip rsvp policy default-reject

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

**ip rsvp policy default-reject**

**no ip rsvp policy default-reject**

---

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

---



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

### Syntax Description

There are no special arguments or keywords for this command.

### Default

Without this command, the default behavior of RSVP is to accept, install, and/or forward all unmatched RSVP messages. Once the **default-reject** parameter is invoked, all unmatched RSVP messages are rejected.

### Command Mode

Global configuration

### Command History

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

### Usage Guidelines

If COPS is configured without any ACL, or if any policy ACL has a catch-all in it (“**permit ip any any**”), the behavior of that ACL will take precedence, and no session will go unmatched.

### Examples

The following example configures RSVP to reject all unmatched reservations:

```
router-1(config)#ip rsvp policy default-reject
```

The following example configures RSVP to accept all unmatched reservations:

```
router-1(config)#no ip rsvp policy default-reject
```

## show cops servers

To display the IP address and connection status of the policy server(s) for which the router is configured, use the **show cops servers** command. The display also tells you about the COPS client on the router.

**show cops servers**

### Syntax Description

This command has no keywords or arguments.

### Default

No default behavior or values.

### Command Mode

Exec

### Command History

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

### Example

In the following example, information is displayed about the current policy server and client. When **Client Type** appears followed by an integer, **1** stands for RSVP and **2** stands for Differentiated Services Provisioning. (**0** indicates keepalive.)

```
router-1# show cops servers
COPS SERVER: Address: 161.44.135.172. Port: 3288. State: 0. Keepalive: 120 sec
              Number of clients: 1. Number of sessions: 1.
COPS CLIENT: Client type: 1. State: 0.
```

### Related Command

Command	Description
<b>show ip rsvp policy cops</b>	Displays policy server address(es), ACL IDs, and client-server connection status.

## show ip rsvp policy cops

To display the policy server address(es), ACL IDs, and current state of the router-server connection, use the **show ip rsvp policy cops** command. (If the server connection has recently broken, this command also displays the reconnection attempt interval.)

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

### Syntax Description

**cops** Makes the display include COPS server addresses.

[*acl*] The access control list(s) whose sessions are governed by COPS.

### Default

No default behavior or values.

### Command Mode

Exec

### Command History

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

### Usage Guidelines

If you omit the final keyword of this command (**cops**), the display reports only on the ACLs and their connection status. This is shown in the second example below.

### Examples

The following example shows the full display, using the full command:

```
router-1# show ip rsvp policy cops
COPS/RSVP entry. ACLs: 40 60
PDPs: 161.44.135.172
Current state: Connected
Currently connected to PDP 161.44.135.172, port 0
```

The following example shows the configured ACLs' IDs and their connection status, using the shortened command:

```
router-1# show ip rsvp policy
Local policy: Currently unsupported
COPS:
ACLs: 40 60 . State: CONNECTED.
ACLs: 40 160 . State: CONNECTING.
```

Related Command

<b>Command</b>	<b>Description</b>
<b>show cops servers</b>	Displays policy server address(es), port, state, keepalives, and policy client information.

## Debug Commands

This section documents new and modified debug commands related to the COPS for RSVP feature.

- **debug cops**
- **debug ip rsvp policy**

## debug cops

To display a one-line summary of each COPS message sent from and received by the router, use the **debug cops** privileged EXEC command. Use the **no** form of this command to disable the debug output.

**debug cops [detail]**

**no debug cops [detail]**

### Syntax Description

**detail** Displays additional debug information, including the contents of COPS and RSVP messages.

### Default

COPS process debugging is not enabled.

### Command History

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

### Usage Guidelines

To generate a complete record of the policy process, enter this command and, after entering a carriage return, enter the additional command **debug ip rsvp policy**.

### Examples

This first example displays the one-line COPS message summaries, as the router goes through six different events.

```
router-1# debug cops
COPS debugging is on
```

**Event 1—The router becomes configured to communicate with a policy server:**

```
router-1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router-1(config)# ip rsvp policy cops servers 2.0.0.1
router-1(config)#
15:13:45:COPS: Opened TCP connection to 2.0.0.1/3288
15:13:45:COPS: ** SENDING MESSAGE **
15:13:45:COPS OPN message, Client-type:1, Length:28. Handle:[NONE]
15:13:45:COPS: ** RECEIVED MESSAGE **
15:13:45:COPS CAT message, Client-type:1, Length:16. Handle:[NONE]
router-1(config)#
```

**Event 2—The router receives a PATH message:**

```
15:13:53:COPS:** SENDING MESSAGE **
15:13:53:COPS REQ message, Client-type:1, Length:216. Handle:[ 00 00 04 01]
```

```
15:13:53:COPS:** RECEIVED MESSAGE **
15:13:53:COPS DEC message, Client-type:1, Length:104. Handle:[ 00 00 04 01]
router-1(config)#
```

### Event 3—The router receives a unicast FF RESV message:

```
15:14:00:COPS:** SENDING MESSAGE **
15:14:00:COPS REQ message, Client-type:1, Length:148. Handle:[ 00 00 05 01]
15:14:00:COPS:** RECEIVED MESSAGE **
15:14:00:COPS DEC message, Client-type:1, Length:64. Handle:[ 00 00 05 01]
15:14:00:COPS:** SENDING MESSAGE **
15:14:00:COPS RPT message, Client-type:1, Length:24. Handle:[ 00 00 05 01]
router-1(config)#
```

### Event 4—The router receives a RESV tear:

```
15:14:06:COPS:** SENDING MESSAGE **
15:14:06:COPS DRQ message, Client-type:1, Length:24. Handle:[ 00 00 05 01]
router-1(config)#
```

### Event 5—The router receives a PATH tear:

```
15:14:11:COPS:** SENDING MESSAGE **
15:14:11:COPS DRQ message, Client-type:1, Length:24. Handle:[ 00 00 04 01]
router-1(config)#
```

### Event 6—The router gets configured to cease communicating with the policy server:

```
router-1(config)# no ip rsvp policy cops servers
15:14:23:COPS:** SENDING MESSAGE **
15:14:23:COPS CC message, Client-type:1, Length:16. Handle:[NONE]
15:14:23:COPS:Closed TCP connection to 2.0.0.1/3288
router-1(config)#
```

This second example uses the **detail** keyword to display the contents of the COPS and RSVP messages, as well as additional debugging information:

```
router-1# debug cops detail
COPS debugging is on

02:13:29:COPS:** SENDING MESSAGE **
  COPS HEADER:Version 1, Flags 0, Opcode 1 (REQ), Client-type:1, Length:216
  HANDLE (1/1) object. Length:8.    00 00 21 01
  CONTEXT (2/1) object. Length:8.   R-type:5.    M-type:1
  IN_IF (3/1) object. Length:12.   Address:10.1.2.1.   If_index:4
  OUT_IF (4/1) object. Length:12.  Address:10.33.0.1.  If_index:3
  CLIENT SI (9/1) object. Length:168.  CSI data:
02:13:29: SESSION                type 1 length 12:
02:13:29:   Destination 10.33.0.1, Protocol_Id 17, Don't Police , DstPort 44
02:13:29: HOP                      type 1 length 12:0A010201
02:13:29:                               :00000000
02:13:29: TIME_VALUES              type 1 length 8 :00007530
02:13:29: SENDER_TEMPLATE          type 1 length 12:
02:13:29:   Source 10.31.0.1, udp_source_port 44
02:13:29: SENDER_TSPEC             type 2 length 36:
02:13:29:   version=0, length in words=7
02:13:29:   Token bucket fragment (service_id=1, length=6 words
02:13:29:     parameter id=127, flags=0, parameter length=5
02:13:29:     average rate=1250 bytes/sec, burst depth=10000 bytes
02:13:29:     peak rate   =1250000 bytes/sec
02:13:29:     min unit=0 bytes, max unit=1514 bytes
02:13:29: ADSPEC                          type 2 length 84:
02:13:29: version=0 length in words=19
```

```

02:13:29: General Parameters break bit=0 service length=8
02:13:29:                               IS Hops:1
02:13:29:           Minimum Path Bandwidth (bytes/sec):1250000
02:13:29:           Path Latency (microseconds):0
02:13:29:                               Path MTU:1500
02:13:29: Guaranteed Service break bit=0 service length=8
02:13:29:           Path Delay (microseconds):192000
02:13:29:           Path Jitter (microseconds):1200
02:13:29:           Path delay since shaping (microseconds):192000
02:13:29:           Path Jitter since shaping (microseconds):1200
02:13:29: Controlled Load Service break bit=0 service length=0
02:13:29:COPS:Sent 216 bytes on socket,
02:13:29:COPS:Message event!
02:13:29:COPS:State of TCP is 4
02:13:29:In read function
02:13:29:COPS:Read block of 96 bytes, num=104 (len=104)
02:13:29:COPS:** RECEIVED MESSAGE **
    COPS HEADER:Version 1, Flags 1, Opcode 2 (DEC), Client-type:1, Length:104
    HANDLE (1/1) object. Length:8.    00 00 21 01
    CONTEXT (2/1) object. Length:8.   R-type:1.    M-type:1
    DECISION (6/1) object. Length:8.  COMMAND cmd:1, flags:0
    DECISION (6/3) object. Length:56.  REPLACEMENT 00 10 0E 01 61 62 63 64 65 66 67
68 69 6A 6B 6C 00 24 0C 02 00
00 00 07 01 00 00 06 7F 00 00 05 44 9C 40 00 46 1C 40 00 49 98
96 80 00 00 00 C8 00 00 01 C8
    CONTEXT (2/1) object. Length:8.   R-type:4.    M-type:1
    DECISION (6/1) object. Length:8.  COMMAND cmd:1, flags:0

02:13:29:Notifying client (callback code 2)
02:13:29:COPS:** SENDING MESSAGE **
    COPS HEADER:Version 1, Flags 1, Opcode 3 (RPT), Client-type:1, Length:24
    HANDLE (1/1) object. Length:8.    00 00 21 01
    REPORT (12/1) object. Length:8.   REPORT type COMMIT (1)

02:13:29:COPS:Sent 24 bytes on socket,
02:13:29:Timer for connection entry is zero

```

To see an example where the **debug cops** command is used along with the **debug ip rsvp policy** command, refer to the second example in the “debug ip rsvp policy” section.

### Related Command

Command	Description
<b>debug ip rsvp policy</b>	Displays debug messages for RSVP policy processing.

## debug ip rsvp policy

To display debug messages for RSVP policy processing, use the **debug ip rsvp policy** privileged EXEC command. Use the **no** form of this command to disable debugging output.

**[no] debug ip rsvp policy**

### Syntax Description

This command has no arguments or keywords.

### Default

Debugging for RSVP policy processing is not enabled.

### Command History

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

### Usage Guidelines

You might find it useful to enable the command **debug cops** when you are using the **debug ip rsvp policy** command. Together, these commands generate a complete record of the policy process.

### Examples

This first example uses only the **debug ip rsvp policy** command:

```
router-1# debug ip rsvp policy
RSVP_POLICY debugging is on

02:02:14:RSVP-POLICY:Creating outbound policy IDB entry for Ethernet2/0 (61E6AB38)
02:02:14:RSVP-COPS:COPS query for Path message, 10.31.0.1_44->10.33.0.1_44
02:02:14:RSVP-POLICY:Building incoming Path context
02:02:14:RSVP-POLICY:Building outgoing Path context on Ethernet2/0
02:02:14:RSVP-POLICY:Build REQ message of 216 bytes
02:02:14:RSVP-POLICY:Message sent to PDP
02:02:14:RSVP-COPS:COPS engine called us with reason2, handle 6202A658
02:02:14:RSVP-COPS:Received decision message
02:02:14:RSVP-POLICY:Received decision for Path message
02:02:14:RSVP-POLICY:Accept incoming message
02:02:14:RSVP-POLICY:Send outgoing message to Ethernet2/0
02:02:14:RSVP-POLICY:Replacement policy object for path-in context
02:02:14:RSVP-POLICY:Replacement TSPEC object for path-in context
02:02:14:RSVP-COPS:COPS report for Path message, 10.31.0.1_44->10.33.0.1_44
02:02:14:RSVP-POLICY:Report sent to PDP
02:02:14:RSVP-COPS:COPS report for Path message, 10.31.0.1_44->10.33.0.1_44
```

The following example uses both the **debug ip rsvp policy** and the **debug cops** commands:

```
router-1# debug ip rsvp policy
RSVP_POLICY debugging is on

router-1# debug cops
COPS debugging is on
```

```

02:15:14:RSVP-POLICY:Creating outbound policy IDB entry for Ethernet2/0 (61E6AB38)
02:15:14:RSVP-COPS:COPS query for Path message, 10.31.0.1_44->10.33.0.1_44
02:15:14:RSVP-POLICY:Building incoming Path context
02:15:14:RSVP-POLICY:Building outgoing Path context on Ethernet2/0
02:15:14:RSVP-POLICY:Build REQ message of 216 bytes
02:15:14:COPS:** SENDING MESSAGE **
    COPS HEADER:Version 1, Flags 0, Opcode 1 (REQ), Client-type:1, Length:216
    HANDLE (1/1) object. Length:8.    00 00 22 01
    CONTEXT (2/1) object. Length:8.  R-type:5.    M-type:1
    IN_IF (3/1) object. Length:12.  Address:10.1.2.1.  If_index:4
    OUT_IF (4/1) object. Length:12.  Address:10.33.0.1.  If_index:3
    CLIENT SI (9/1) object. Length:168.  CSI data:
02:15:14: SESSION          type 1 length 12:
02:15:14: Destination 10.33.0.1, Protocol_Id 17, Don't Police , DstPort 44
02:15:14: HOP              type 1 length 12:0A010201
02:15:14:                  :00000000
02:15:14: TIME_VALUES      type 1 length 8 :00007530
02:15:14: SENDER_TEMPLATE  type 1 length 12:
02:15:14: Source 10.31.0.1, udp_source_port 44
02:15:14: SENDER_TSPEC     type 2 length 36:
02:15:14: version=0, length in words=7
02:15:14: Token bucket fragment (service_id=1, length=6 words
02:15:14:     parameter id=127, flags=0, parameter length=5
02:15:14:     average rate=1250 bytes/sec, burst depth=10000 bytes
02:15:14:     peak rate =1250000 bytes/sec
02:15:14:     min unit=0 bytes, max unit=1514 bytes
02:15:14: ADSPEC              type 2 length 84:
02:15:14: version=0 length in words=19
02:15:14: General Parameters break bit=0 service length=8
02:15:14:                  IS Hops:1
02:15:14: Minimum Path Bandwidth (bytes/sec):1250000
02:15:14: Path Latency (microseconds):0
02:15:14: Path MTU:1500
02:15:14: Guaranteed Service break bit=0 service length=8
02:15:14: Path Delay (microseconds):192000
02:15:14: Path Jitter (microseconds):1200
02:15:14: Path delay since shaping (microseconds):192000
02:15:14: Path Jitter since shaping (microseconds):1200
02:15:14: Controlled Load Service break bit=0 service length=0
02:15:14:COPS:Sent 216 bytes on socket,
02:15:14:RSVP-POLICY:Message sent to PDP
02:15:14:COPS:Message event!
02:15:14:COPS:State of TCP is 4
02:15:14:In read function
02:15:14:COPS:Read block of 96 bytes, num=104 (len=104)
02:15:14:COPS:** RECEIVED MESSAGE **
    COPS HEADER:Version 1, Flags 1, Opcode 2 (DEC), Client-type:1, Length:104
    HANDLE (1/1) object. Length:8.    00 00 22 01
    CONTEXT (2/1) object. Length:8.  R-type:1.    M-type:1
    DECISION (6/1) object. Length:8.  COMMAND cmd:1, flags:0
    DECISION (6/3) object. Length:56.  REPLACEMENT 00 10 0E 01 61 62 63 64 65 66 67
68 69 6A 6B 6C 00 24 0C 02 00
00 00 07 01 00 00 06 7F 00 00 05 44 9C 40 00 46 1C 40 00 49 98
96 80 00 00 00 C8 00 00 01 C8
    CONTEXT (2/1) object. Length:8.  R-type:4.    M-type:1
    DECISION (6/1) object. Length:8.  COMMAND cmd:1, flags:0

02:15:14:Notifying client (callback code 2)
02:15:14:RSVP-COPS:COPS engine called us with reason2, handle 6202A104
02:15:14:RSVP-COPS:Received decision message
02:15:14:RSVP-POLICY:Received decision for Path message
02:15:14:RSVP-POLICY:Accept incoming message
02:15:14:RSVP-POLICY:Send outgoing message to Ethernet2/0
02:15:14:RSVP-POLICY:Replacement policy object for path-in context
02:15:14:RSVP-POLICY:Replacement TSPEC object for path-in context

```

```
02:15:14:RSVP-COPS:COPS report for Path message, 10.31.0.1_44->10.33.0.1_44
02:15:14:COPS:** SENDING MESSAGE **
    COPS HEADER:Version 1, Flags 1, Opcode 3 (RPT), Client-type:1, Length:24
    HANDLE (1/1) object. Length:8.    00 00 22 01
    REPORT (12/1) object. Length:8.    REPORT type COMMIT (1)

02:15:14:COPS:Sent 24 bytes on socket,
02:15:14:RSVP-POLICY:Report sent to PDP
02:15:14:Timer for connection entry is zero
02:15:14:RSVP-COPS:COPS report for Path message, 10.31.0.1_44->10.33.0.1_44
```

## Related Commands

Command	Description
<b>debug cops</b>	Displays debug messages for COPS processing.

## Glossary

This section defines acronyms and words that may not be readily understood.

**ACL**—Access Control List. List kept by the router to control access of flows to services by selecting packets according to the content of their header fields. The fields used are typically source address, destination address, DS field, protocol ID, source port, and/or destination port.

**CLI**—Command Language Interpreter. Cisco's command line interface for configuring and managing its routers.

**COPS**—Common Open Policy Service. A client/server protocol for controlling QoS policies.

**DS**—Differentiated Service. A paradigm for providing QoS in the Internet by employing a small, well-defined set of building blocks from which a variety of services can be built.

**IETF**—Internet Engineering Task Force. Organization that develops Internet standards.

**PDP**—Policy Decision Point. The server which makes policy decisions—called, therefore, the policy server. The PDP has global knowledge of network policies, and is consulted by network devices (like routers) that enforce the policies.

**PEP**—Policy Enforcement Point. The device on which policy decisions are carried out—usually a network node like a router or switch.

**Policy**—Any defined rule that determines the use of resources within the network. A policy can be based on a user, device, subnetwork, network, or application.

**Policy server**—The server (at least one in each QoS domain) that holds policies for reference by and decision over client routers and switches.

**PSB**—Path State Block. The block maintained by RSVP to store a path.

**QoS**—Quality of Service. The performance of a transmission across a network. To ensure that receivers get the quality they expect—a video image that is smooth rather than choppy, for example—various strategies have been developed that enable routers to give preference to one set of packets over others that arrive at the routers at the same moment. These strategies are known as Quality of Service features.

**QPM**—QoS Policy Manager. Cisco's policy server application for dynamically managing network traffic flows.

**RSB**—Reservation State Block. The block maintained by RSVP to store a reservation.

**RSVP**—Resource reSerVation Protocol. An IETF protocol used for signalling requests (setting up reservations) for Internet services by a customer before that customer is permitted to transmit data over that portion of the network.