RSVP Application ID Support

First Published: February 27, 2006
Last Updated: February 19, 2007

The RSVP Application ID Support feature introduces application-specific Resource Reservation Protocol (RSVP) reservations, which enhance the granularity for local policy match criteria so that you can manage quality of service (QoS) on the basis of application type.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for RSVP Application ID Support" section on page 58.

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 RSVP Application ID Support

You must configure RSVP on one or more interfaces on at least two neighboring routers that share a link within the network.

Restrictions for RSVP Application ID Support

- RSVP policies apply only to PATH, RESV, PATHERROR, and RESVERROR messages.
- Merging of global and interface-based local policies is not supported; therefore, you cannot match on multiple policies.

Information About RSVP Application ID Support

To use the RSVP Application ID Support feature, you should understand the following concepts:

- Feature Overview of RSVP Application ID Support, page 2
- Benefits of RSVP Application ID Support, page 5

Feature Overview of RSVP Application ID Support

This section provides the following information:

- How RSVP Functions, page 2
- Sample Solution, page 3
- Global and Per-Interface RSVP Policies, page 4
- How RSVP Policies Are Applied, page 4
- Preemption, page 4

How RSVP Functions

Multiple applications such as voice and video need RSVP support. RSVP admits requests until the bandwidth limit is reached. RSVP does not differentiate between the requests and is not aware of the type of application for which the bandwidth is requested.

As a result, RSVP can exhaust the allowed bandwidth by admitting requests that represent just one type of application, causing all subsequent requests to be rejected because of unavailable bandwidth. For example, a few video calls could prevent all or most of the voice calls from being admitted because the video calls require a large amount of bandwidth and not enough bandwidth remains to accommodate the voice calls. With this limitation, you would probably not deploy RSVP for multiple applications especially if voice happens to be one of the applications for which RSVP is required.

The solution is to allow configuration of separate bandwidth limits for individual applications or classes of traffic. Limiting bandwidth per application requires configuring a bandwidth limit per application and having each reservation flag the application to which the reservation belongs so that it can be admitted against the appropriate bandwidth limit.

Application and Sub Application Identity Policy Element for Use with RSVP (IETF RFC 2872) allows for creation of separate bandwidth reservation pools. For example, an RSVP reservation pool can be created for voice traffic, and a separate RSVP reservation pool can be created for video traffic. This prevents video traffic from overwhelming voice traffic.

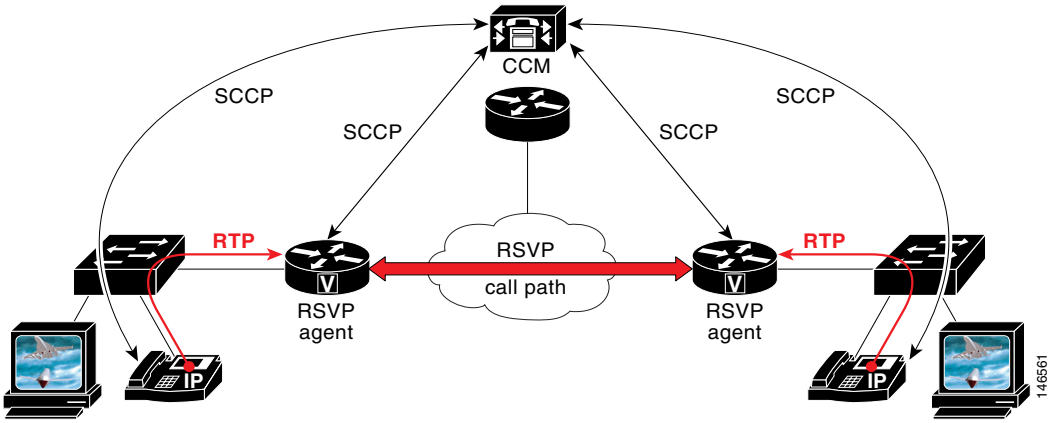
Note Before this feature, you could create access control lists (ACLs) that match on the differentiated services code points (DSCPs) of the IP header in an RSVP message. However, multiple applications could use the same DSCP; therefore, you could not uniquely identify applications in order to define separate policies for them.

Sample Solution

Figure 1 shows a sample solution in which application ID is used. In this example, bandwidth is allocated between the voice and video sessions that are being created by Cisco Unified Communications Manager. Video requires much more bandwidth than voice, and if you do not separate the reservations, the video traffic could overwhelm the voice traffic.

Cisco Unified Communications Manager has been enhanced to use the RSVP Application ID Support feature. In this example, when making the RSVP reservation, Cisco Unified Communications Manager has the ability to specify whether the reservation should be made against a video RSVP bandwidth pool or a voice RSVP bandwidth pool. If there is not enough bandwidth remaining in the requested pool, even though there is enough bandwidth in the total RSVP allocation, RSVP signals Cisco Unified Communications Manager that there is a problem with the reservation. Figure 1 shows some of the signaling and data traffic that is sent during the session setup.

Figure 1 Sample Solution Using RSVP Application ID Support



RTP = Real-Time Transport Protocol
CCM = Cisco CallManager
SCCP = Skinny Client Control Protocol

In this scenario, the IP phones and IP video devices do not directly support RSVP. In order to allow RSVP to reserve the bandwidth for these devices, the RSVP agent component in the Cisco IOS router creates the reservation. During the setup of the voice or video session, Cisco Unified Communications Manager communicates with the RSVP agent and sends the necessary parameters to reserve the appropriate bandwidth.

When a voice or video call is initiated on a device, the device signals Cisco Unified Communications Manager, which signals the RSVP agent, specifying the RSVP application ID that corresponds to the type of call (voice or video in this example). The RSVP agents establish the RSVP reservation across the network and notify Cisco Unified Communications Manager that the reservation is in place. Cisco Unified Communications Manager then completes session establishment and the Real-Time Transport Protocol (RTP) traffic streams flow between the devices. If the RSVP agents are unable to create the bandwidth reservations for the requested application ID, they communicate that information back to Cisco Unified Communications Manager, which signals this information back to the initiator.

Global and Per-Interface RSVP Policies

You can configure RSVP policies globally and on a per-interface basis. You can also configure multiple global policies and multiple policies per interface.

Global RSVP policies restrict how much RSVP bandwidth a router uses regardless of the number of interfaces. You should configure a global policy if your router has CPU restrictions, one interface, or multiple interfaces that do not require different bandwidth limits.

Per-interface RSVP policies allow you to configure separate bandwidth pools with varying limits so that no one application, such as video, can consume all the RSVP bandwidth on a specified interface at the expense of other applications, such as voice, which would be dropped. You should configure a per-interface policy when you need greater control of the available bandwidth.

How RSVP Policies Are Applied

RSVP searches for policies whenever an RSVP message is processed. The policy tells RSVP if any special handling is required for that message.

If your network configuration has global and per-interface RSVP policies, the per-interface policies are applied first meaning that RSVP looks for policy-match criteria in the order in which the policies were configured. RSVP searches for policy-match criteria in the following order:

- Nondefault interface policies
- Default interface policy
- Nondefault global policies
- Global default policy

If RSVP finds no policy-match criteria, it accepts all incoming messages. To change this decision from accept to reject, issue the **ip rsvp policy default-reject** command.

Preemption

Preemption happens when one reservation receives priority over another because there is insufficient bandwidth in an RSVP pool. There are two types of RSVP bandwidth pools: local policy pools and interface pools. Local policies can be global or interface-specific. RSVP performs admission control against these pools when a RESV message arrives.

If an incoming reservation request matches an RSVP local policy with an RSVP bandwidth limit that has been reached (as configured with the **bandwidth group** submode of the **maximum (local policy)** command), RSVP tries to preempt other lower-priority reservations admitted by that policy. When there are too few of these lower-priority reservations, then RSVP rejects the incoming reservation request. If there are enough lower-priority reservations that can be preempted to make room for the new call, then RSVP will next look at the interface bandwidth pool (configured with the **ip rsvp bandwidth** command). If that bandwidth limit has been reached, then RSVP tries to preempt other lower-priority reservations on that interface to accommodate the new reservation request. However, RSVP does not consider which local policies admitted the reservations—if there is not enough bandwidth on the interface bandwidth pool that can be preempted to make room for the new call, then RSVP rejects the new reservation even though the new reservation was able to obtain bandwidth from the local policy pool.

Preemption can also happen when you manually reconfigure an RSVP bandwidth pool of any type to a lower value such that the existing reservations using that pool no longer fit in the pool.

How Preemption Priorities Are Assigned and Signaled

If a received RSVP PATH or RESV message contains preemption priorities (signaled with an IETF RFC 3181 preemption priority policy element inside an IETF RFC 2750 POLICY_DATA object) and the priorities are higher than those contained in the matching local policy (if any), the message is rejected and a PATHERROR or RESVERROR message is sent in response. If the priorities are approved by the local policy, they are stored with the RSVP state in the router and forwarded to the router's neighbors.

If a received RSVP PATH or RESV message does not contain preemption priorities (as previously described), the **ip rsvp policy preempt** command is enabled globally, and the message matches a local policy that contains a **preempt-priority** command, then a POLICY_DATA object with a preemption priority element that contains the local policy's priorities is added to the message as part of the policy decision. These priorities are stored with the RSVP state in the router and forwarded to neighbors.

Controling Preemption

The **ip rsvp policy preempt** command controls whether or not a router preempts any reservations when required. When you issue this command, a RESV message that subsequently arrives on an interface can preempt the bandwidth of one or more reservations on that interface if the assigned setup priority of the new reservation is higher than the assigned hold priorities of the installed reservations.

Benefits of RSVP Application ID Support

The RSVP Application ID Support feature provides the following benefits:

- Allows RSVP to identify applications uniquely and to separate bandwidth pools to be created for different applications so that one application cannot consume all the available bandwidth, thereby forcing others to be dropped.
- Integrates with the RSVP agent and Cisco Unified Communications Manager to provide a solution for call admission control (CAC) and QoS for Voice over IP (VoIP) and video conferencing applications in networks with multitiered, meshed topologies using signaling protocols such as Skinny Client Control Protocol (SCCP) to ensure that a single application does not overwhelm the available reserved bandwidth.
- Functions with any endpoint that complies with RFC 2872 or RFC 2205.

How to Configure RSVP Application ID Support

You can configure application IDs and local policies for use with RSVP-aware software programs, such as Cisco Unified Communications Manager, or for use with non-RSVP-aware applications, such as static PATH and RESV messages.

This section contains the following procedures:

- Configuring RSVP Application IDs and Local Policies for RSVP-Aware Software Programs, page 6 (optional)
- Configuring RSVP Application IDs with Static Senders and Receivers for Non-RSVP-Aware Software Programs, page 10 (optional)
- Verifying the RSVP Application ID Support Configuration, page 15 (optional)

Configuring RSVP Application IDs and Local Policies for RSVP-Aware Software Programs

This section contains the following procedures:

- Configuring an Application ID, page 6 (required)

Note Although each of the following two local policy configuration procedures are noted as being optional, you must configure at least one of them (you can configure both if needed).

- Configuring a Local Policy Globally, page 8 (optional)
- Configuring a Local Policy on an Interface, page 9 (optional)

Configuring an Application ID

Perform this task to configure an application ID.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp policy identity** *alias* **policy-locator** *locator*
4. **Repeat Step 3 as needed to configure additional application IDs.**
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.

	Command or Action	Purpose
Step 3	**ip rsvp policy identity** *alias* **policy-locator** *locator* **Example:** `Router(config)# ip rsvp policy identity rsvp-voice policy-locator APP=Voice`	Defines RSVP application IDs to use as match criteria for local policies. • Enter a value for the *alias* argument, which is a string used within the router to reference the identity in RSVP configuration commands and show displays. The string can have as many as 64 printable characters (in the range 0x20 to 0x7E). **Note** If you use the " " or ? characters as part of the alias or locator string itself, you must type the CTRL/V key sequence before entering the embedded " " or ? characters. The alias is never transmitted to other routers. • Enter a value for the *locator* argument, which is a string that is signaled in RSVP messages and contains application IDs usually in X.500 Distinguished Name (DN) format. This can also be a regular expression. For more information on regular expressions, see the "Related Documents" section.
Step 4	`Repeat Step 3 as needed to configure additional application IDs.`	Defines additional application IDs.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

What to Do Next

Configure a local policy globally, on an interface, or both.

Configuring a Local Policy Globally

Perform this task to configure a local policy globally.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp policy local {acl** *acl1* [*acl2...acl8*] **| default | identity** *alias1* [*alias2...alias4*] **| origin-as** *as1* [*as2...as8*]**}**
4. Repeat Step 3 as needed to configure additional local policies.
5. {**accept | forward** [**all | path | path-error | resv | resv-error**] **| default | exit | fast-reroute | local-override | maximum** [**bandwidth** [**group** *x*] [**single** *y*] **| senders** *n*] **| preempt-priority** [**traffic-eng** *x*] *setup-priority* [*hold-priority*]}
6. **Repeat Step 5 as needed to configure additional submode commands.**
7. **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	**ip rsvp policy local** {**acl** *acl1* [*acl2...acl8*] | **default** | **identity** *alias1* [*alias2...alias4*] | **origin-as** *as1* [*as2...as8*]} **Example:** `Router(config)# ip rsvp policy local identity rsvp-voice`	Creates a local policy to determine how RSVP resources are used in a network and enters local policy configuration mode. • Enter the **identity** *alias1* keyword and argument combination to specify an application ID alias.
Step 4	`Repeat Step 3 as needed to configure additional local policies.`	(Optional) Configures additional local policies.
Step 5	{**accept** | **forward** [**all** | **path** | **path-error** | **resv** | **resv-error**] | **default** | **exit** | **fast-reroute** | **local-override** | **maximum** [**bandwidth** [**group** *x*] [**single** *y*] | **senders** *n*] | **preempt-priority** [**traffic-eng** *x*] *setup-priority* [*hold-priority*]} **Example:** `Router(config-rsvp-policy-local)# forward all`	(Optional) Defines the properties of the local policy that you are creating. (These are the submode commands.) **Note** This is an optional step. An empty policy rejects everything, which may be desired in some cases. See the **ip rsvp policy local** command for more detailed information on submode commands.
Step 6	`Repeat Step 5 as needed to configure additional submode commands.`	(Optional) Configures additional submode commands.
Step 7	**end** **Example:** `Router(config-rsvp-policy-local)# end`	Exits local policy configuration mode and returns to privileged EXEC mode.

Configuring a Local Policy on an Interface

Perform this task to configure a local policy on an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Repeat Step 3 as needed to configure additional interfaces.
5. **ip rsvp bandwidth** [*interface-kbps] [single-flow-kbps]*
6. Repeat Step 5 as needed to configure bandwidth for additional interfaces.
7. **ip rsvp policy local {acl** *acl1* [*acl2...acl8*] **| default | identity** *alias1* [*alias2...alias4*] **| origin-as** *as1* [*as2...as8*]**}**
8. Repeat Step 7 as needed to configure additional local policies.
9. {**accept | forward** [**all | path | path-error | resv | resv-error**] **| default | exit | fast-reroute | local-override | maximum** [**bandwidth** [**group** *x*] [**single** *y*] **| senders** *n*] **| preempt-priority** [**traffic-eng** *x*] *setup-priority* [*hold-priority*]}
10. Repeat Step 9 as needed to configure additional submode commands.
11. **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* **Example:** `Router(config)# interface Ethernet0/0`	Configures the interface type and number and enters interface configuration mode.
Step 4	`Repeat Step 3 as needed to configure additional interfaces.`	(Optional) Configures additional interfaces.

Step 5	`ip rsvp bandwidth [interface-kbps] [single-flow-kbps]`
	
	Example:
	`Router(config-if)# ip rsvp bandwidth 500 500`
		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 1000,000.

Step 6	`Repeat Step 5 as needed to configure bandwidth for additional interfaces.`	(Optional) Configures bandwidth for additional interfaces.

	Command or Action	Purpose
Step 7	**ip rsvp policy local** {**acl** *acl1* [*acl2...acl8*] | **default** | **identity** *alias1* [*alias2...alias4*] | **origin-as** *as1* [*as2...as8*]} **Example:** `Router(config-if)# ip rsvp policy local identity rsvp-voice`	Creates a local policy to determine how RSVP resources are used in a network. • Enter the **identity** *alias1* keyword argument combination to specify an application ID alias.
Step 8	`Repeat Step 7 as needed to configure additional local policies.`	(Optional) Configures additional local policies.
Step 9	{**accept** | **forward** [**all** | **path** | **path-error** | **resv** | **resv-error**] | **default** | **exit** | **fast-reroute** | **local-override** | **maximum** [**bandwidth** [**group** *x*] [**single** *y*] | **senders** *n*] | **preempt-priority** [**traffic-eng** *x*] *setup-priority* [*hold-priority*]} **Example:** `Router(config-rsvp-policy-local)# forward all`	(Optional) Defines the properties of the local policy that you are creating and enters local policy configuration mode. (These are the submode commands.) **Note** This is an optional step. An empty policy rejects everything, which may be desired in some cases. See the **ip rsvp policy local** command for more detailed information on submode commands.
Step 10	`Repeat Step 9 as needed to configure additional submode commands.`	(Optional) Configures additional submode commands.
Step 11	**end** **Example:** `Router(config-rsvp-policy-local)# end`	Exits local policy configuration mode and returns to privileged EXEC mode.

Configuring RSVP Application IDs with Static Senders and Receivers for Non-RSVP-Aware Software Programs

This section contains the following procedures:

- Configuring an Application ID, page 10 (required)
- Configuring a Static Sender with an Application ID, page 12 (optional)
- Configuring a Static Receiver with an Application ID, page 13 (optional)

Configuring an Application ID

Perform this task to configure an application ID.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp policy identity** *alias* **policy-locator** *locator*
4. **Repeat step 3 to configure additional application IDs.**
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	**ip rsvp policy identity** *alias* **policy-locator** *locator* **Example:** `Router(config)# ip rsvp policy identity rsvp-voice policy-locator "APP=Voice"`	Defines RSVP application IDs to use as match criteria for local policies. • Enter a value for the *alias* argument, which is a string used within the router to reference the identity in RSVP configuration commands and show displays. The string can have as many as 64 printable characters (in the range 0x20 to 0x7E). **Note** If you use the " " or ? characters as part of the alias or locator string itself, you must type the CTRL/V key sequence before entering the embedded " " or ? characters. The alias is never transmitted to other routers. • Enter a value for the *locator* argument, which is a string that is signaled in RSVP messages and contains application IDs usually in X.500 Distinguished Name (DN) format. **Note** Repeat this step as needed to configure additional application IDs.
Step 4	**Repeat step 3 to configure additional application IDs.**	Configures additional application IDs.
Step 5	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring a Static Sender with an Application ID

Perform this task to configure a static RSVP sender with an application ID to make the router proxy an RSVP PATH message containing an application ID on behalf of an RSVP-unaware sender application.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp sender-host** *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-d-port sender-s-port bandwidth burst-size* [**identity** *alias*]
4. **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	**ip rsvp sender-host** *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-d-port sender-s-port bandwidth burst-size* [**identity** *alias*] **Example:** `Router(config)# ip rsvp sender-host 10.0.0.7 10.0.0.1 udp 1 1 10 10 identity rsvp-voice`	Enables a router to simulate a host generating RSVP PATH messages. • The optional **identity** *alias* keyword and argument combination specifies an application ID alias. The string can have as many as 64 printable characters (in the range 0x20 to 0x7E). **Note** If you use the “ ” or ? characters as part of the alias string itself, you must type the CTRL/V key sequence before entering the embedded “ ” or ? characters. The alias is never transmitted to other routers.
Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring a Static Receiver with an Application ID

Perform this task to configure a static RSVP receiver with an application ID to make the router proxy an RSVP RESV message containing an application ID on behalf of an RSVP-unaware receiver application.

Note You can also configure a static listener to use with an application ID. If an incoming PATH message contains an application ID, preemption priority value, or both, the listener includes those values in the RESV message that is sent in reply. See the **"Feature Information for RSVP Application ID Support"** for more information.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp reservation-host** *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-d-port sender-s-port* {**ff** | **se** | **wf**} {**rate** | **load**} *bandwidth burst-size* [**identity** *alias*]
   or
   ip rsvp reservation *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-d-port sender-s-port next-hop-ip-address next-hop-interface* {**ff** | **se** | **wf**} {**rate** | **load**} *bandwidth burst-size* [**identity** *alias*]

Note Use the **ip rsvp reservation-host** command if the router is the destination or the **ip rsvp reservation** command to have the router proxy on behalf of a downstream host.

4. **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.

	Command or Action	Purpose

Step 3	**ip rsvp reservation-host** *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-d-port sender-s-port* {**ff** | **se** | **wf**} {**rate** | **load**} *bandwidth burst-size* [**identity** *alias*]
	or
	ip rsvp reservation *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-d-port sender-s-port next-hop-ip-address next-hop-interface* {**ff** | **se** | **wf**} {**rate** | **load**} *bandwidth burst-size* [**identity** *alias*]
	
	Example:
	`Router(config)# ip rsvp reservation-host 10.1.1.1 10.30.1.4 udp 20 30 se load 100 60 identity rsvp-voice`
	
	`Router(config)# ip rsvp reservation 10.1.1.1 0.0.0.0 udp 20 0 172.16.4.1 Ethernet1 wf rate 350 65 identity xyz`
		Enables a router to simulate a host generating RSVP RESV messages.
		• The optional **identity** *alias* keyword and argument combination specifies an application ID alias. The string can have as many as 64 printable characters (in the range 0x20 to 0x7E).
		Note If you use the “ ” or ? characters as part of the alias string itself, you must type the CTRL/V key sequence before entering the embedded “ ” or ? characters. The alias is never transmitted to other routers.
		Note Use the **ip rsvp reservation-host** command if the router is the destination or the **ip rsvp reservation** command to have the router proxy on behalf of a downstream host.

Step 4	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying the RSVP Application ID Support Configuration

Perform the following task to verify the configuration.

SUMMARY STEPS

1. **enable**

Note You can use the following commands in user EXEC or privileged EXEC mode.

2. **show ip rsvp host** {**senders** | **receivers**} [*group-name* | *group-address*]
3. **show ip rsvp policy identity** [*regular-expression*]
4. **show ip rsvp policy local** [**detail**] [**interface** *name*] [**default** | **acl** *acl* | **origin-as** *as* | **identity** *alias*]
5. **show ip rsvp reservation** [**detail**] [**filter** [**destination** *ip-addr* | *hostname*] [**source** *ip-addr* | *hostname*] [**dst-port** *port*] [**src-port** *port*]]
6. **show ip rsvp sender** [**detail**] [**filter** [**destination** *ip-addr* | *hostname*] [**source** *ip-addr* | *hostname*] [**dst-port** *port*] [**src-port** *port*]]
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Optional) Enables privileged EXEC mode. • Enter your password if prompted. **Note** Skip this step if you are using the commands in user EXEC mode.
Step 2	**show ip rsvp host** {**senders** | **receivers**} [*group-name* | *group-address*] **Example:** `Router# show ip rsvp host senders`	Displays specific information for an RSVP host. **Note** Use this command only on routers from which PATH and RESV messages originate.
Step 3	**show ip rsvp policy identity** [*regular-expression*] **Example:** `Router# show ip rsvp policy identity voice100`	Displays selected RSVP identities in a router configuration. • The optional *regular-expression* argument allows pattern matching on the alias strings of the RSVP identities to be displayed. **Note** For more information on regular expressions, see the "Related Documents" section.
Step 4	**show ip rsvp policy local** [**detail**] [**interface** *name*] [**default** | **acl** *acl* | **origin-as** *as* | **identity** *alias*] **Example:** `Router# show ip rsvp policy local identity voice100`	Displays the local policies currently configured. • The optional **detail** keyword and the optional **interface** *name* keyword and argument combination can be used with any of the match criteria.

	Command or Action	Purpose
Step 5	**show ip rsvp reservation** [**detail**] [**filter** [**destination** *ip-addr* | *hostname*] [**source** *ip-addr* | *hostname*] [**dst-port** *port*] [**src-port** *port*]] **Example:** `Router# show ip rsvp reservation detail`	Displays RSVP-related receiver information currently in the database. • The optional **detail** keyword displays additional output with information about where the policy originated as well as which application ID was signaled in the RESV message. **Note** The optional **filter** keyword is supported in Cisco IOS Releases 12.0S and 12.2S only.
Step 6	**show ip rsvp sender** [**detail**] [**filter** [**destination** *ip-addr* | *hostname*] [**source** *ip-addr* | *hostname*] [**dst-port** *port*] [**src-port** *port*]] **Example:** `Router# show ip rsvp sender detail`	Displays RSVP PATH-related sender information currently in the database. • The optional **detail** keyword displays additional output with information that includes which application ID was signaled in the PATH message. **Note** The optional **filter** keyword is supported in Cisco IOS Releases 12.0 S and 12.2 S only.
Step 7	**exit** **Example:** `Router# exit`	Exits privileged EXEC mode and returns to user EXEC mode.

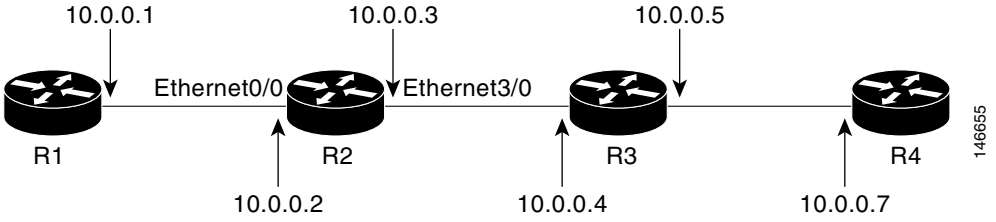
Configuration Examples for RSVP Application ID Support

This section provides configuration examples for the RSVP Application ID Support feature.

Configuring RSVP Application ID Support: Example

The four-router network in Figure 2 contains the following configurations:

Figure 2 Sample Network with Application Identities and Local Policies



Configuring a Proxy Receiver on R4

The following example configures R4 with a proxy receiver to create an RESV message to match the PATH message for the destination 10.0.0.7:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip rsvp listener 10.0.0.7 any any reply
Router(config)# end
```

Configuring an Application ID and a Global Local Policy on R3

The following example configures R3 with an application ID called video and a global local policy in which all RSVP messages are being accepted and forwarded:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip rsvp policy identity video policy-locator video
Router(config)# ip rsvp policy local identity video
Router(config-rsvp-policy-local)# forward all
Router(config-rsvp-policy-local)# end
```

Configuring an Application ID and Separate Bandwidth Pools on R2 for Per-Interface Local Policies

The following example configures R2 with an application ID called video, which is a wildcard regular expression to match any application ID that contains the substring video:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip rsvp policy identity video policy-locator .*Video.*
Router(config-rsvp-id)# end
```

The following example configures R2 with a local policy on ingress Ethernet interface 0/0:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.0.0.2 255.0.0.0
Router(config-if)# no cdp enable
Router(config-if)# ip rsvp bandwidth 200
Router(config-if)# ip rsvp policy local identity video
Router(config-rsvp-policy-local)# maximum senders 10
Router(config-rsvp-policy-local)# maximum bandwidth group 100
Router(config-rsvp-policy-local)# maximum bandwidth single 10
Router(config-rsvp-policy-local)# forward all
Router(config-rsvp-policy-local)# end
```

The following example configures R2 with a local policy on egress Ethernet interface 3/0:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface Ethernet3/0
Router(config-if)# ip address 10.0.0.3 255.0.0.0
Router(config-if)# no cdp enable
Router(config-if)# ip rsvp bandwidth 200
Router(config-if)# ip rsvp policy local identity video
Router(config-rsvp-policy-local)# maximum senders 10
Router(config-rsvp-policy-local)# maximum bandwidth group 100
Router(config-rsvp-policy-local)# maximum bandwidth single 10
Router(config-rsvp-policy-local)# forward all
Router(config-rsvp-policy-local)# end
```

Note PATH messages arrive on ingress Ethernet interface 0/0 and RESV messages arrive on egress Ethernet interface 3/0.

Configuring an Application ID and a Static Reservation from R1 to R4

The following example configures R1 with an application ID called video and initiates a host generating a PATH message with that application ID:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip rsvp policy identity video policy-locator "GUID=www.cisco.com,
APP=Video, VER=1.0"
Router(config)# ip rsvp sender-host 10.0.0.7 10.0.0.1 udp 1 1 10 10 identity video
Router(config)# end
```

Verifying RSVP Application ID Support: Example

This section contains the following verification examples:

Verifying the Application ID and the Global Local Policy on R3

The following example verifies that a global local policy has been configured on R3 with an application ID called Video:

```
Router# show ip rsvp policy local detail

Global:
  Policy for ID(s): Video

    Preemption Scope: Unrestricted.
    Local Override:   Disabled.
    Fast ReRoute:     Accept.
    Handle:           23000404.

                          Accept              Forward
    Path:                 Yes                 Yes
    Resv:                 Yes                 Yes
    PathError:            Yes                 Yes
    ResvError:            Yes                 Yes

                          Setup Priority      Hold Priority
    TE:                   N/A                 N/A
    Non-TE:               N/A                 N/A

                          Current             Limit
    Senders:              1                   N/A
    Receivers:            1                   N/A
    Conversations:        1                   N/A
    Group bandwidth (bps): 10K                N/A
    Per-flow b/w (bps):   N/A                 N/A


Generic policy settings:
    Default policy: Accept all
    Preemption:     Disabled
```

Verifying the Application ID and the Per-Interface Local Policies on R2

The following example verifies that an application ID called Video has been created on R2:

```
Router# show ip rsvp policy identity

Alias: Video
  Type:    Application ID
  Locator: .*Video.*
```

The following example verifies that per-interface local policies have been created on Ethernet interface 0/0 and Ethernet interface 3/0 on R2:

```
Router# show ip rsvp policy local detail

Ethernet0/0:
  Policy for ID(s): Video

    Preemption Scope: Unrestricted.
    Local Override:   Disabled.
    Fast ReRoute:     Accept.
    Handle:           26000404.

                          Accept               Forward
    Path:                 Yes                  Yes
    Resv:                 Yes                  Yes
    PathError:            Yes                  Yes
    ResvError:            Yes                  Yes

                          Setup Priority       Hold Priority
    TE:                   N/A                  N/A
    Non-TE:               N/A                  N/A

                          Current              Limit
    Senders:              1                    10
    Receivers:            0                    N/A
    Conversations:        0                    N/A
    Group bandwidth (bps): 0                   100K
    Per-flow b/w (bps):   N/A                  10K


Ethernet3/0:
  Policy for ID(s): Video

    Preemption Scope: Unrestricted.
    Local Override:   Disabled.
    Fast ReRoute:     Accept.
    Handle:           5A00040A.

                          Accept               Forward
    Path:                 Yes                  Yes
    Resv:                 Yes                  Yes
    PathError:            Yes                  Yes
    ResvError:            Yes                  Yes

                          Setup Priority       Hold Priority
    TE:                   N/A                  N/A
    Non-TE:               N/A                  N/A

                          Current              Limit
    Senders:              0                    10
    Receivers:            1                    N/A
    Conversations:        1                    N/A
    Group bandwidth (bps): 10K                 100K
    Per-flow b/w (bps):   N/A                  10K


Generic policy settings:
    Default policy: Accept all
    Preemption:     Disabled
```

Note Notice in the above display that the ingress interface has only its senders counter incremented because the PATH message is checked there. However, the egress interface has its receivers, conversations, and group bandwidth counters incremented because the reservation is checked on the incoming interface, which is the egress interface on R2.

Verifying the Application ID and the Reservation on R1

The following example verifies that a PATH message containing the application ID called Video has been created on R1:

```
Router# show ip rsvp sender detail

PATH Session address: 10.0.0.7, port: 1. Protocol: UDP
  Sender address: 10.0.0.1, port: 1
     Inbound from: 10.0.0.1 on interface:
  Traffic params - Rate: 10K bits/sec, Max. burst: 10K bytes
                   Min Policed Unit: 0 bytes, Max Pkt Size 4294967295 bytes
  Path ID handle: 02000402.
  Incoming policy: Accepted. Policy source(s): Default
    Application ID: 'GUID=www.cisco.com, APP=Video, VER=1.0'
  Status: Proxied
  Output on Ethernet0/0. Policy status: Forwarding. Handle: 01000403
    Policy source(s): Default
```

Note You can issue the **debug ip rsvp dump path** and the **debug ip rsvp dump resv** commands to get more information about a sender and the application ID that it is using.

The following example verifies that a reservation with the application ID called Video has been created on R1:

```
Router# show ip rsvp reservation detail

RSVP Reservation. Destination is 10.0.0.7, Source is 10.0.0.1,
  Protocol is UDP, Destination port is 1, Source port is 1
  Next Hop is 10.0.0.2, Interface is Ethernet0/0
  Reservation Style is Fixed-Filter, QoS Service is Guaranteed-Rate
  Resv ID handle: 01000405.
  Created: 10:07:35 EST Thu Jan 12 2006
  Average Bitrate is 10K bits/sec, Maximum Burst is 10K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  Status:
  Policy: Forwarding. Policy source(s): Default
    Application ID: 'GUID=www.cisco.com, APP=Video, VER=1.0'
```

Additional References

The following sections provide references related to the RSVP Application ID Support 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*
QoS configuration tasks	*Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4
Cisco CallManager and related features	*Cisco Unified Communications Manager and Cisco IOS Interoperability Features Roadmap*
Error messages	*Cisco IOS Software System Messages*
Regular expressions	*Regular Expressions*

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 (RSVP)
RFC 2872	Application and Sub Application Identity Policy Element for Use with RSVP
RFC 3181	Signaled Preemption Priority Policy Element
RFC 3182	Identity Representation for RSVP

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 new or modified.

- ip rsvp listener
- ip rsvp policy identity
- ip rsvp policy local
- ip rsvp reservation
- ip rsvp reservation-host
- ip rsvp sender
- ip rsvp sender-host
- maximum (local policy)
- show ip rsvp host
- show ip rsvp policy identity
- show ip rsvp policy local

ip rsvp listener

To configure a Resource Reservation Protocol (RSVP) router to listen for PATH messages, use the **ip rsvp listener** command in global configuration mode. To disable listening, use the **no** form of this command.

ip rsvp listener *dst* {**udp | tcp | any |** *number*} {**any |** *dst-port*} {**announce | reply | reject**}

no ip rsvp listener *dst* {**udp | tcp | any |** *number*} {**any |** *dst-port*} {**announce | reply | reject**}

Syntax Description

dst	IP address of the receiving interface.
udp	UDP for the receiving interface.
tcp	TCP for the receiving interface.
any	Protocol for the receiving interface.
number	Source port number from 0 to 255; the protocol is IP.
any	Destination port for the receiving interface.
dst-port	Port number from 0 to 65535 for the receiving interface.
announce	Receiver announces the arrival of the flow at its destination, but does not send a RESV message in response.
reply	Sender requests a reply when the flow is received and sends a RESV message when a matching PATH message arrives.
reject	Router sends a PATHERROR (reject) message in response to an incoming PATH message that matches specified listener parameters.

Command Default

This command is disabled by default; therefore, no listeners are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.4(6)T	Support for RSVP application identity (ID) was added.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Use the **ip rsvp listener** command to allow a router to send a matching RESV message when a PATH message arrives with the desired destination address, port, and protocol. This command copies the application ID and preemption priority value, if present, from the PATH message and includes them in the RESV message.

This command is similar to the **ip rsvp reservation** and **ip rsvp reservation-host** commands. However, they do not allow you to specify more than one port or protocol per command; so you may have to enter many commands to proxy for a set of ports and protocols. In contrast, the **ip rsvp listener** command allows you to use a wildcard for a set of ports and protocols by using just that one command.

You can use the **debug ip rsvp api** command to look for a matching PATH message, but no RESV message will be sent.

Examples

In the following example, the sender is requesting that the receiver reply with a RESV message for the flow if the PATH message destination is 192.168.2.1:

```
Router# configure terminal
Router(config)# ip rsvp listener 192.168.2.1 any any reply
```

Related Commands

Command	Description
ip rsvp reservation	Enables a router to simulate receiving and forwarding RSVP RESV messages.
ip rsvp reservation-host	Enables a router to simulate a host generating RSVP RESV messages.
show ip rsvp listeners	Displays configured RSVP listeners.

ip rsvp policy identity

To define Resource Reservation Protocol (RSVP) application identities (IDs), use the **ip rsvp policy identity** command in global configuration mode. To delete RSVP application IDs, use the **no** form of this command.

ip rsvp policy identity *alias* **policy-locator** *locator*

no ip rsvp policy identity *alias* [**policy-locator** *locator*]

Syntax Description

alias	A string used within the router to reference the identity in RSVP configuration commands and **show** displays. The string can have as many as 64 printable characters (in the range 0x20 to 0x7E). **Note** If you use the " " or ? characters as part of the alias or locator string itself, you must type the CTRL/V key sequence before entering the embedded " "or ? characters. The alias is never transmitted to other routers.
policy-locator *locator*	A string that is signaled in RSVP messages and contains application IDs in X.500 Distinguished Name (DN) format. (See the "**Usage Guidelines"** section for detailed information.)

Command Default

This command is disabled by default; therefore, no RSVP application identities are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

You can use RSVP identities as criteria for matching RSVP PATH and RESV messages to local policies. Identities can also be used to configure static senders and receivers. When you use an RSVP identity as the match criterion for a local policy, RSVP treats the *policy locato*r string as a type of pattern-matching string known as a regular expression. Regular expressions allow you to configure a single identity for use with a local policy that can match multiple X.500 DNs. Regular expressions, by default, are not exact matches unless you add appropriate control characters to the expression to force it to be an exact match.

In Cisco IOS software, the *locator* is the primary piece of information that the router uses to find the correct policy to apply to RSVP messages that contain application IDs. This string assumes the format of an X.500 DN and includes the following attributes as recommended in RFC 2872:

- APP = Application identifier, a required attribute.
- VER = Version number of the application, a required attribute.
- SAPP = Subapplication identifier, an optional attribute. An arbitrary number of subapplication elements can be included.

- GUID = Global unique identifier, an optional attribute.

Here are some examples:

- APP = CCM, VER = 1.1, SAPP = Voice
- GUID = http://www.cisco.com/apps, APP = VideoConference, VER = 1.2.3

You can create a maximum of 100 identities on a router. If you attempt to create more, the command fails and the following error message is generated: “RSVP error: maximum number of identities already created”.

When you use the **ip rsvp policy identity** command, be aware of the following behavior:

- If you specify *alias* or *locator* strings that are empty or invalid, the command is rejected and an error message is generated.
- Cisco IOS software automatically adds quotes to the *alias* or *locator* strings in the configuration if quotes are required.
- If you specify the optional **policy-locator** keyword in the **no** version of this command, the command is rejected if *locator* does not match the configured *locator* string for the *alias* being deleted.
- If you specify an *alias* that is missing, empty, or contains invalid characters, the command is rejected and an error message is generated.
- RSVP does not check the *locator* string to see if it is a valid X.500 DN; therefore, the *locator* string can be anything that you want. (Future versions of Cisco IOS software may force RSVP messages to contain valid X.500 DNs.)

Command Restrictions

- User identities are not supported in the Cisco IOS 12.4(6)T release.
- You cannot configure a single router with more than 100 identities at a time.

Examples

Exact Application ID Match

The following example shows an application ID for RSVP messages containing a locator string whose contents are the exact string “APP=Voice”:

```
Router# configure terminal
Router(config)# ip rsvp policy identity “rsvp-voice” policy-locator “^APP=Voice$”
Router(config-rsvp-id)# end
```

Wildcard (or Partial) Application ID Match

The following example shows an application ID that is a partial match for RSVP messages containing a locator string with the substring “APP=Voice” anywhere in the signaled application ID:

```
Router# configure terminal
Router(config)# ip rsvp policy identity “rsvp-voice” policy-locator ".*APP=Voice.*"
Router(config-rsvp-id)# end
```

Related Commands

Command	Description
ip rsvp policy local	Creates a local procedure that determines the use of RSVP resources in a network.

Command	Description
show ip rsvp policy identity	Displays selected RSVP identities in a router configuration.
show ip rsvp policy local	Displays selected local policies that have been configured.

ip rsvp policy local

To determine how to perform authorization on Resource Reservation Protocol (RSVP) requests and enter local policy configuration mode, use the **ip rsvp policy local** command in global configuration or interface configuration mode. To disable this feature, use the **no** form of this command.

ip rsvp policy local {acl *acl1* [*acl2...acl8*] **| default | identity** *alias1* [*alias2...alias4*] **| origin-as** *as1* [*as2...as8*]**}**

no ip rsvp policy local {acl *acl1* [*acl2...acl8*] **| default | identity** *alias1* [*alias2...alias4*] **| origin-as** *as1* [*as2...as8*]**}**

Syntax Description

acl *acl1* [*acl2...acl8*]	Specifies an access control list (ACL). Values for each ACL are 1 to 199. **Note** You must associate at least one ACL with an ACL-based policy. However, you can associate as many as eight.
default	Used when an RSVP message does not match any ACL, identity, or autonomous system.
identity *alias1* [*alias2...alias4*]	Specifies an application ID alias for an application ID previously configured using the **ip rsvp policy identity** command. **Note** You must associate at least one alias with an application-ID-based policy. However, you can associate as many as four.
origin-as *as1* [*as2...as8*]	Specifies an autonomous system. Values for each autonomous system are 1 to 65535. **Note** You must associate at least one autonomous system with an autonomous-system-based policy. However, you can associate as many as eight.

Command Default

This command is disabled by default; therefore, no local policies are configured.

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.0(29)S	The **origin-as** *as* keyword and argument combination and new submode commands were added.
12.0(30)S	This command was modified so that you can no longer use 0 as the protocol when you configure an ACL.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.

12.4(6)T	The command was modified as follows: • Interface configuration mode was added to support per-interface local policies. • **The identity** *alias* keyword and argument combination was added. • The **maximum** submode command was changed to support RESV messages.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **ip rsvp policy local** command to determine how to perform authorization on RSVP requests.

Note Before entering the **origin-as** *as* keyword and argument combination, you must have Border Gateway Protocol (BGP) running; otherwise, an RSVP warning message appears stating that the autonomous-system-based policy will be ineffective.

You can use all types of match criteria with non-Traffic-Engineering (TE) reservations. You can use all types of match criteria except application ID with TE reservations because TE PATH and RESV messages sent by Cisco routers do not contain application IDs.

There are four types of local policies—one default local policy, one or more ACL-based policies, one or more autonomous-system-based policies, and one or more application-ID-based policies. The default policy is used when an RSVP message does not match any ACL-, autonomous-system-, or application-ID-based policies.

You can configure a mixture of local policy types including ACL, autonomous system, application ID, or default on the same interface or globally. Policies have the following priority (from highest to lowest):

- Nondefault interface policies
- Default interface policy
- Nondefault global policies
- Global default policy

Note If you configure an ACL to use with a TE tunnel, do not use 0 as the protocol because RSVP cannot accept any messages since they do not match the ACL.

Policy-Match Criteria

Note You cannot specify a policy-match criteria more than once using the **ip rsvp policy local** command.

An ACL-based policy must have at least one ACL associated with it, but it can optionally have up to eight ACLs. The ACLs can be standard or extended IP ACLs. They are matched against source/destination addresses/ports based on RSVP objects inside RSVP signaling messages as described below.

- ACL source address—Matched against the source address in the SENDER_TEMPLATE object in RSVP messages. If this object is not present, the source address in the IP header is used.
- ACL destination address—Matched against the destination address in the SESSION object in RSVP messages. If this object is not present, the destination address in the IP header is used.

- ACL source port—Matched against the source port in the SENDER_TEMPLATE object in RSVP messages. If this object is not present, the source port of 0 is used.
- ACL destination port—Matched against the destination port in the SESSION object in RSVP messages. If this object is not present, the destination port of 0 is used.
- ACL IP protocol—Matched against the IP protocol in the SESSION object in RSVP messages. If this object is not present, the IP protocol of 0 is used. If the IP protocol is for a TE session, then the ACL IP protocol should be UDP.
- ACL differentiated services code point (DSCP) values—Matched against the DSCP value in the IP header of the RSVP message.

Note These same policy-match criteria apply when you create ACLs for the **debug ip rsvp filter** command except the command does not use DSCP and the protocol is ignored for TE sessions.

An autonomous-system-based policy must have at least one autonomous system associated with it, but it can optionally have up to eight autonomous systems. They are matched against the incoming interface/source IP address contained in RSVP objects inside RSVP signaling messages, not on the IP headers of the RSVP messages.

An application-ID-based policy must have at least one application ID associated with it, but it can optionally have up to four application IDs. They are matched against the incoming interface/source IP address contained in RSVP objects inside RSVP signaling messages, not on the IP headers of the RSVP messages.

Command Restrictions

- You cannot configure more than 300 local policies per router. This limit is independent of policy location (global or per interface) or match criteria such as application IDs, access control lists, or autonomous systems.
- You cannot configure a single local policy with more than four RSVP identities.

CLI Submodes

Once you type the **ip rsvp policy local** command, you enter the local policy CLI submode where you define the properties of the local policy that you are creating.

Note The local policy that you create automatically rejects all RSVP messages unless you enter a submode command that instructs RSVP on the types of messages to accept or forward.

The submode commands are as follows:

- **accept**—Accepts, but does not forward RSVP messages.

  accept {**all** | **path** | **path-error** | **resv** | **resv-error**}

  - **all**—Accepts all incoming RSVP messages.
  - **path**—Accepts incoming PATH messages that meet the match criteria for this policy, which includes ACL(s), autonomous system(s), application ID(s), or default(s). If you omit this command, incoming PATH messages that meet the policy-match criteria are rejected and a PATHERROR message is sent in reply. However, the PATHERROR reply is also subject to local policy.
  - **path-error**—Accepts incoming PATHERROR messages that meet the match criteria for this policy. If you omit this command, incoming, including locally-generated, PATHERROR messages that meet the policy-match criteria are rejected.

  - **resv**—Accepts incoming RESV messages that meet the match criteria for this policy and performs any required admission control. If you omit this command, incoming RESV messages that meet the policy-match criteria are rejected and a RESVERROR message is sent in reply. However, the RESVERROR reply is also subject to local policy.

    The default bandwidth for a policy is unlimited. Therefore, if the policy has no configured bandwidth, a RESV message is always accepted by the local policy because any bandwidth request is less than or equal to unlimited. However, the RESV message may subsequently fail admission control if there is insufficient bandwidth in the RSVP pool on the input interface to which the RESV message applies. (See the **ip rsvp bandwidth** command for more information.) If the bandwidth requested by the RESV messages is too large, a RESVERROR message that is also subject to local policy is transmitted to the RESV sender.
  - **resv-error**—Accepts incoming RESVERROR messages that meet the policy-match criteria for this policy. If you omit this command, the incoming, including locally-generated, RESVERROR messages that meet the policy-match criteria are rejected.

- **default**—Sets a command to its defaults.
- **exit**—Exits local policy configuration mode.
- **fast-reroute**—Allows TE LSPs that request Fast Reroute service. The default value is accept.
- **forward**—Accepts and forwards RSVP messages.

  forward {**all** | **path** | **path-error** | **resv** | **resv-error**}

  - **all**—Accepts and forwards all RSVP messages.
  - **path**—Accepts and forwards PATH messages that meet the match criteria for this policy. If you omit this command, PATH messages that meet the policy-match criteria are not forwarded to the next (downstream) hop.
  - **path-error**—Accepts and forwards PATHERROR messages that meet the match criteria for this policy. If you omit this command, the PATHERROR messages that meet the match criteria are not forwarded to the previous (upstream) hop. You may want to reject outbound PATHERROR messages if you are receiving PATH messages from an untrusted node because someone could be trying to port-scan for RSVP. If you reply with a PATHERROR message, the untrusted node knows that you support RSVP and your IP address. Such information could be used to attempt RSVP-based attacks.
  - **resv**—Accepts and forwards RESV messages that meet the match criteria for this policy. If you omit this command, RESV messages that meet the match criteria are not forwarded to the previous (upstream) hop.
  - **resv-error**—Accepts and forwards RESVERROR messages that meet the match criteria for this policy. If you omit this command, the RESVERROR messages that meet the match criteria are not forwarded to the next (downstream) hop. You may want to reject outbound RESVERROR messages if you are receiving RESV messages from an untrusted node because someone could be trying to port-scan for RSVP. If you reply with a RESVERROR message, then the untrusted node knows that you support RSVP and your IP address. Such information could be used to attempt RSVP-based attacks.

- **local-override**—Overrides any other policy sources by enforcing this local policy. Finalizes any decisions by this policy. If local-override is omitted, RSVP holds onto the local policy decision to see if another local or remote policy exists that will make a decision on the RSVP message, and only if there is no other policy decision will the local policy decision be enforced.
- **maximum** [**bandwidth** [**group** *x*] [**single** *y*] | **senders** *n*]—Sets the limits for resources.

  - **bandwidth** [**group** *x*] [**single** *y*]—Indicates bandwidth limits for RSVP reservations. The **group** keyword specifies the amount of bandwidth that can be requested by all reservations covered by this policy. The **single** keyword specifies the maximum bandwidth that can be requested by any specific RSVP reservation covered by this policy. The *x* and *y* values are in kbps and can range from 1 to 10,000,000 (similar in concept to the existing interface mode **ip rsvp bandwidth** command). Absence of a bandwidth command implies that there is no policy limit on bandwidth requests.

    Previously, the **maximum bandwidth** command applied only to PATH messages. However, as part of the application ID enhancement, this command now applies only to RESV messages. This change has the following benefits:

    Allows the local policy bandwidth limit to be used by RSVP's admission control process for both shared and nonshared reservations. Previous releases that performed group bandwidth checks on PATH messages could not account for bandwidth sharing, and, as a result, you had to account for sharing by creating a larger maximum group bandwidth for the policy.

    Allows a local policy to trigger preemption during the admission control function if there is insufficient policy bandwidth to meet the needs of an incoming RESV message.

  - **senders** *n*—Limits the number of RSVP senders affected by this policy that can be active at the same time on this router. The value for *n* ranges from 1 to 50,000 with a default of 1000.

Note If you do not configure the **ip rsvp policy preempt** command, the **maximum** command may be rejected, resulting in the following error message: "**RSVP error: insufficient preemptable bandwidth" if there are reservations admitted against the policy, and you try to reduce the group bandwidth to less than the amount of admitted bandwidth on the policy**.

- **no**—Negates a command or sets its defaults.
- **preempt-priority** [**traffic-eng** *x*] *setup-priority* [*hold-priority*]—Specifies the RSVP QoS priorities to be inserted into PATH and RESV messages if they were not signaled from an upstream or downstream neighbor or local client application, and the maximum setup or hold priority that RSVP QoS or MPLS/TE sessions can signal. A PATHERROR, RESVERROR, or local application error is returned if these limits are exceeded.

  The *x* value indicates the upper limit of the priority for TE reservations. The range of *x* values is 0 to 7 in which the smaller the number, the higher the reservation's priority. For non-TE reservations, the range of *x* values is 0 to 65535 in which the higher the number, the higher the reservation's priority.

  The *setup-priority* argument indicates the priority of a reservation when it is initially installed. The optional *hold-priority* argument indicates the priority of a reservation after it has been installed; if omitted, it defaults to the *setup-priority*. Values for the *setup-priority* and *hold-priority* arguments range from 0 to 7 where 0 is considered the highest priority.

  If the incoming message has a preemption priority that requests a priority higher than the policy allows, the message is rejected. Use the **tunnel mpls traffic-eng priority** command to configure preemption priority for TE tunnels.

  A single policy can contain a **preempt-priority traffic-eng** and a **preempt-priority** command, which may be useful if the policy is bound to an ACL that identifies a subnet containing a mix of TE and non-TE endpoints or midpoints.

Note If you exit local policy configuration mode without entering any submode commands, the policy that you have created rejects *all* RSVP messages.

Per-Interface Local Policies

All the local policy submode commands are also supported on a per-interface basis. You simply enter Cisco IOS interface configuration mode for the selected interface and type in any number and mix of the submode commands.

Per-interface local policies take precedence over global local policies. However, if there is a default local policy configured for an interface, the router does not try to match any RSVP messages arriving on that interface to any of the global local policies. Policies have the following priority (from highest to lowest):

- Nondefault interface policies
- Default interface policy
- Nondefault global policies
- Global default policy

There are some important points to note about per-interface local policies:

- Per-interface local policies do not take the place of the **ip rsvp bandwidth** command. The **ip rsvp bandwidth** command indicates if RSVP is enabled on an interface as well as the size of the RSVP bandwidth pool. The **ip rsvp bandwidth** pool is used by the admission control function of RSVP; per-interface policies are used by the policy control function of RSVP. Policy control is the third phase of RSVP message processing, which consists of validation, authentication, policy control (authorization), and admission control.
- The sum of the group bandwidth of all the local policies assigned to an interface can be greater than the maximum total bandwidth configured in the **ip rsvp bandwidth** command. However, the **ip rsvp bandwidth** command makes the final decision as to whether there is sufficient bandwidth to admit the reservation.

Examples

ACL-, Default-, and Autonomous-System-Based Policies

In the following example, any RSVP nodes in the 192.168.101.0 subnet can initiate or respond to reservation requests, but all other nodes can respond to reservation requests only. This means that any 192.168.101.x node can send and receive PATH, PATHERROR, RESV, or RESVERROR messages. All other nodes can send only RESV or RESVERROR messages, and all reservations for autonomous system 1 are rejected.

```
Router# configure terminal
Router(config)# access-list 104 permit ip 192.168.101.0 0.0.0.255 any
Router(config)# ip rsvp policy local acl 104
Router(config-rsvp-policy-local)# forward all
Router(config-rsvp-policy-local)# exit
Router(config)# ip rsvp policy local default
Router(config-rsvp-policy-local)# forward resv
Router(config-rsvp-policy-local)# forward resverror
Router(config-rsvp-policy-local)# exit
Router(config)# ip rsvp policy local origin-as 1
Router(config-rsvp-policy-local)# end
```

Application-ID-Based Policy

RSVP matches incoming RSVP messages with IDs to configured IDs and policies. The following example displays a global RSVP local policy that limits voice calls to 200 kbps for the whole router regardless of which interface the RSVP signaling occurs on:

```
Router# configure terminal
Router(config)# ip rsvp policy identity rsvp-voice policy-locator "GUID=www.cisco.com,
APP=Voice"
Router(config)# ip rsvp policy local identity rsvp-voice
Router(config-rsvp-local-policy)# forward all
Router(config-rsvp-local-policy)# maximum bandwidth group 200
Router(config-rsvp-local-policy)# end
```

Per-Interface Application ID-Based Policy

The following example displays a local policy that limits all RSVP voice calls on serial interface 2/0/0 to a total of 200 kbps:

```
Router# configure terminal
Router(config)# ip rsvp policy identity rsvp-voice policy-locator APP=Voice
Router(config)# interface serial2/0/0
Router(config-if)# ip rsvp policy local identity rsvp-voice
Router(config-rsvp-local-policy)# forward all
Router(config-rsvp-local-policy)# maximum bandwidth group 200
Router(config-rsvp-local-policy)# exit
Router(config-if)# ip rsvp policy local default
Router(config-rsvp-local-policy)# forward all
Router(config-rsvp-local-policy)# maximum bandwidth group 50
Router(config-rsvp-local-policy)# end
```

Related Commands

Command	Description
ip rsvp policy preempt	Enables RSVP to take bandwidth from lower-priority reservations and give it to new, higher-priority reservations.
show ip rsvp policy	Displays the configured local policies.
show ip rsvp policy cops	Displays the policy server addresses, ACL IDs, and current state of the router's TCP connections to COPS servers.
show ip rsvp policy local	Displays selected local policies that have been configured.
tunnel mpls traffic-eng priority	Configures the setup and reservation priority for an MPLS Traffic Engineering tunnel.

ip rsvp reservation

To enable a router to simulate receiving Resource Reservation Protocol (RSVP) RESV messages from a downstream host, use the **ip rsvp reservation** command in global configuration mode. To disable this function, use the **no** form of this command.

ip rsvp reservation *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-d-port sender-s-port next-hop-ip-address next-hop-interface* {**ff** | **se** | **wf**} {**rate** | **load**} *bandwidth burst-size* [**identity** *alias*]

no ip rsvp reservation *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-d-port sender-s-port next-hop-ip-address next-hop-interface* {**ff** | **se** | **wf**} {**rate** | **load**} *bandwidth burst-size* [**identity** *alias*]

Syntax Description

session-ip-address	For unicast sessions, this is the address of the intended receiver; for multicast sessions, this is the IP multicast address of the session.
sender-ip-address	IP address of the sender.
tcp | **udp** | *ip-protocol*	TCP, UDP, or IP protocol in the range from 0 to 255.
session-d-port *sender-s-port*	*The session-d-port* argument is the destination port. The *sender-s-port* argument is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If the destination is zero, the source must be zero, and the implication is that ports are not checked. If the destination is nonzero, the source must be nonzero (except for **wf** reservations, for which the source port is always ignored and can therefore be zero).
next-hop-ip-address	Hostname or address of the receiver or the router closest to the receiver.
next-hop-interface	Next-hop interface or subinterface type and number. Interface type can be **ethernet**, **loopback**, **null**, or **serial**.
ff | **se** | **wf**	Reservation style: • Fixed Filter (**ff**) is single reservation. • Shared Explicit (**se**) is shared reservation, limited scope. • Wildcard Filter (**wf**) is shared reservation, unlimited scope.
rate | **load**	QoS guaranteed bit rate service or controlled load service.
bandwidth	Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000.
burst-size	Maximum burst size (kbps of data in queue). The range is from 1 to 65535.
identity alias	(Optional) Specifies an application ID alias. An alias is a string that can have as many as 64 printable characters (in the range 0x20 to 0x7E). **Note** If you use the " " or ? characters as part of the alias or locator string itself, you must type the CTRL/V key sequence before entering the embedded " " or ? characters. The alias is never transmitted to other routers.

Command Default

The router does not simulate receiving RSVP RESV messages.

Command Modes Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.4(6)T	The optional **identity** *alias* keyword and argument combination was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines Use the **ip rsvp reservation** command to make the router simulate receiving RSVP RESV messages from a downstream host and to proxy RSVP RESV messages for that host. By giving a local (loopback) next-hop address and next-hop interface, you can also use this command to proxy RSVP for the router that you are configuring or you can use the **ip rsvp reservation-host** command.

An alias must reference an RSVP identity that you created by using the **ip rsvp identity** command. The policy-locator string associated with this identity is signaled in the RESV message. This identity overrides any application ID that is contained in the matching PATH message.

If the matching PATH message has an application ID, but you have not specified an application ID using the **ip rsvp reservation** command, the RESV message will not contain an application ID. However, the RESV message proxied by the **ip rsvp listener** command does put the matching PATH message application ID into the proxied RESV message.

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

```
Router(config)# ip rsvp reservation 239.250.0.2 172.16.1.1 udp 20 30 172.16.4.1 Ethernet1
se load 100 60

Router(config)# ip rsvp reservation 239.250.0.2 172.16.2.1 tcp 20 30 172.16.4.1 Ethernet1
se load 150 65
```

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

```
Router(config)# ip rsvp reservation 239.250.0.3 0.0.0.0 udp 20 0 172.16.4.1 Ethernet1 wf
rate 300 60 identity xyz

Router(config)# ip rsvp reservation 239.1.1.1 0.0.0.0 udp 20 0 172.16.4.1 Ethernet1 wf
rate 350 65 identity xyz
```

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

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp identity	Defines RSVP application IDs.
ip rsvp neighbor	Enables a router to control who its authorized neighbors are.

Command	Description
ip rsvp reservation-host	Enables a router to simulate a host generating RSVP RESV messages.
ip rsvp sender	Enables a router to simulate receiving RSVP PATH messages.
ip rsvp sender-host	Enables a router to simulate a host generating RSVP PATH messages.
show ip rsvp installed	Displays RSVP-related bandwidth information.
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp neighbor	Displays current RSVP neighbors.
show ip rsvp policy identity	Displays selected RSVP identities in a router configuration.
show ip rsvp reservation	Displays RSVP RESV-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.

ip rsvp reservation-host

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

ip rsvp reservation-host *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-d-port sender-s-port* {**ff** | **se** | **wf**} {**rate** | **load**} *bandwidth burst-size* [**identity** *alias*]

no ip rsvp reservation-host *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-d-port sender-s-port* {**ff** | **se** | **wf**} {**rate** | **load**} *bandwidth burst-size* [**identity** *alias*]

Syntax Description

session-ip-address	For unicast sessions, this is the address of the intended receiver. IP multicast addresses cannot be used with this argument. It must be a logical address configured on an interface on the router that you are configuring.
sender-ip-address	IP address of the sender.
tcp | **udp** | *ip-protocol*	TCP, UDP, or IP protocol in the range from 0 to 255.
session-d-port *sender-s-port*	*The session-d-port* argument is the destination port. The *sender-s-port* argument is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If the destination is zero, the source must be zero, and the implication is that ports are not checked. If the destination is nonzero, the source must be nonzero (except for **wf** reservations, for which the source port is always ignored and can therefore be zero).
ff | **se** | **wf**	Reservation style: • Fixed Filter (**ff**) is single reservation. • Shared Explicit (**se**) is shared reservation, limited scope. • Wildcard Filter (**wf**) is shared reservation, unlimited scope.
rate | **load**	QoS guaranteed bit rate service or controlled load service.
bandwidth	Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000.
burst-size	Maximum burst size (kbps of data in queue). The range is from 1 to 65535.
identity alias	(Optional) Specifies an application ID alias. An alias is a string that can have as many as 64 printable characters (in the range 0x20 to 0x7E). **Note** If you use the " " or ? characters as part of the alias or locator string itself, you must type the CTRL/V key sequence before entering the embedded " " or ? characters. The alias is never transmitted to other routers.

Command Default

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

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.
12.4(6)T	The optional **identity** *alias* keyword and argument combination was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **ip rsvp reservation-host** command to make a router simulate a host generating its own RSVP RESV messages. This command is similar to the **ip rsvp reservation** command, which can cause a router to generate RESV messages on behalf of another host. The main differences between the **ip rsvp reservation-host** and **ip rsvp reservation** commands follow:

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

An alias must reference an RSVP identity that you created by using the **ip rsvp identity** command. The policy-locator string associated with this identity is signaled in the RESV message. This identity overrides any application ID that is contained in the matching PATH message.

If the matching PATH message has an application ID, but you have not specified an application ID using the **ip rsvp reservation-host** command, the RESV message does not contain an application ID. However, the RESV message proxied by the **ip rsvp listener** command does put the matching PATH message application ID into the proxied RESV message.

Examples

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

```
Router(config)# ip rsvp reservation-host 10.1.1.1 10.30.1.4 udp 20 30 se load 100 60
identity xyz

Router(config)# ip rsvp reservation-host 10.40.2.2 10.22.1.1 tcp 20 30 se load 150 65
identity xyz
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp identity	Defines RSVP application IDs.
ip rsvp neighbor	Enables a router to control who its authorized RSVP neighbors are.
ip rsvp reservation	Enables a router to simulate receiving RSVP RESV messages.
ip rsvp sender	Enables a router to simulate receiving RSVP PATH messages.
ip rsvp sender-host	Enables a router to simulate a host generating RSVP PATH messages.
show ip rsvp installed	Displays RSVP-related bandwidth information.

Command	Description
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp neighbor	Displays current RSVP neighbors.
show ip rsvp policy identity	Displays selected RSVP identities in a router configuration.
show ip rsvp reservation	Displays RSVP RESV-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.

ip rsvp sender

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

ip rsvp sender *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-d-port sender-s-port previous-hop-ip-address previous-hop-interface bandwidth burst-size* [**identity** *alias*]

no ip rsvp sender *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-d-port sender-s-port previous-hop-ip-address previous-hop-interface bandwidth burst-size* [**identity** *alias*]

Syntax Description

session-ip-address	For unicast sessions, this is the address of the intended receiver; for multicast sessions, it is the IP multicast address of the session.
sender-ip-address	IP address of the sender.
tcp | **udp** | *ip-protocol*	TCP, UDP, or IP protocol in the range from 0 to 255.
session-d-port *sender-s-port*	*The session-d-port* argument is the destination port. The *sender-s-port* argument is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If the destination is zero, the source must be zero, and the implication is that ports are not checked. If the destination is nonzero, the source must be nonzero.
previous-hop-ip-address	Address of the sender or the router closest to the sender.
previous-hop-interface	Previous-hop interface or subinterface. Interface type can be **ethernet**, **loopback**, **null**, or **serial**.
bandwidth	Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000.
burst-size	Maximum burst size (kbps of data in queue). The range is from 1 to 65535.
identity *alias*	(Optional) Specifies an application ID alias. An alias is a string that can have as many as 64 printable characters (in the range 0x20 to 0x7E). **Note** If you use the " " or ? characters as part of the alias or locator string itself, you must type the CTRL/V key sequence before entering the embedded " " or ? characters. The alias is never transmitted to other routers.

Command Default

The router does not simulate receiving RSVP PATH messages.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was introduced.
12.4(6)T	The optional **identity** *alias* keyword and argument combination was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **ip rsvp sender** command to make the router simulate that it is receiving RSVP PATH messages from an upstream host and to proxy RSVP PATH messages from that host. By including a local (loopback) previous-hop address and previous-hop interface, you can also use this command to proxy RSVP for the router that you are configuring.

An alias must reference an RSVP identity that you created by using the **ip rsvp identity** command. The policy-locator string associated with this identity is supplied in the PATH message.

Examples

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

```
Router(config)# ip rsvp sender 239.250.0.1 172.16.2.1 udp 20 30 172.16.2.1 loopback 1 50 5
identity xyz

Router(config)# ip rsvp sender 239.250.0.2 172.16.2.1 udp 20 30 172.16.2.1 loopback 1 50 5
identity xyz
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp identity	Defines RSVP application IDs.
ip rsvp neighbor	Enables a router to control who its authorized RSVP neighbors are.
ip rsvp reservation	Enables a router to simulate receiving RSVP RESV messages.
ip rsvp reservation-host	Enables a router to simulate a host generating RSVP RESV messages.
ip rsvp sender-host	Enables a router to simulate a host generating RSVP PATH messages.
show ip rsvp installed	Displays RSVP-related bandwidth information.
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp neighbor	Displays current RSVP neighbors.
show ip rsvp policy identity	Displays selected RSVP identities in a router configuration.
show ip rsvp reservation	Displays RSVP RESV-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.

ip rsvp sender-host

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

ip rsvp sender-host *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-d-port sender-s-port bandwidth burst-size* [**identity** *alias*]

no ip rsvp sender-host *session-ip-address sender-ip-address* {**tcp** | **udp** | *ip-protocol*} *session-d-port sender-s-port bandwidth burst-size* [**identity** *alias*]

Syntax Description

session-ip-address	For unicast sessions, this is the address of the intended receiver; for multicast sessions, it is the IP multicast address of the session.
sender-ip-address	IP address of the sender. It must be a logical address configured on an interface on the router that you are configuring.
tcp | **udp** | *ip-protocol*	TCP, UDP, or IP protocol in the range from 0 to 255.
session-d-port *sender-s-port*	*The session-d-port argument* is the destination port. The *sender-s-port* argument is the source port. Port numbers are specified in all cases, because the use of 16-bit ports following the IP header is not limited to UDP or TCP. If the destination is zero, the source must be zero, and the implication is that ports are not checked. If the destination is nonzero, the source must be nonzero.
bandwidth	Average bit rate, in kbps, to reserve up to 75 percent of the total on the interface. The range is from 1 to 10000000.
burst-size	Maximum burst size (kbps of data in queue). The range is from 1 to 65535.
identity *alias*	(Optional) Specifies an application ID alias. An alias is a string that can have as many as 64 printable characters (in the range 0x20 to 0x7E). **Note** If you use the " " or ? characters as part of the string itself, you must type the CTRL/V key sequence before entering the embedded " " or ? characters. The alias is never transmitted to other routers.

Command Default

The router does not simulate RSVP PATH message generation.

Command Modes

Global configuration

Command History

Release	Modification
12.0	This command was introduced.
12.4(6)T	The optional **identity** *alias* keyword and argument combination was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **ip rsvp sender-host** command to make a router simulate a host generating its own RSVP PATH messages. This command is similar to the **ip rsvp sender** command, which can cause a router to generate RSVP PATH messages on behalf of another host. The main differences between the **ip rsvp sender-host** and **ip rsvp sender** commands follow:

- When you enter the **ip rsvp sender-host** command, the *sender-ip-address* argument must be a local address configured on an interface of the router.
- Because the message is assumed to originate from the router that you are configuring, you do not specify a previous-hop or incoming interface for the RSVP PATH message when entering the **ip rsvp sender-host** command.
- Use the **ip rsvp sender-host** command for debugging and testing purposes because you cannot use it to proxy RSVP for non-RSVP-capable hosts.

An alias must reference an RSVP identity that you created by using the **ip rsvp identity** command. The policy-locator string associated with this identity is signaled in the RESV message. This identity overrides any application ID that is contained in the matching PATH message.

Examples

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

```
Router(config)# ip rsvp sender-host 10.0.0.7 10.0.0.1 udp 1 1 10 10 identity xyz
```

Related Commands

Command	Description
ip rsvp bandwidth	Enables RSVP for IP on an interface.
ip rsvp identity	Defines RSVP application IDs.
ip rsvp neighbor	Enables a router to control who its authorized neighbors are.
ip rsvp reservation	Enables a router to simulate receiving RSVP RESV messages.
ip rsvp reservation-host	Enables a router to simulate a host generating RSVP RESV messages.
ip rsvp sender	Enables a router to simulate receiving RSVP PATH messages.
show ip rsvp installed	Displays RSVP-related bandwidth information.
show ip rsvp interface	Displays RSVP-related interface information.
show ip rsvp neighbor	Displays current RSVP neighbors.
show ip rsvp policy identity	Displays selected RSVP identities in a router configuration.
show ip rsvp reservation	Displays RSVP RESV-related receiver information currently in the database.
show ip rsvp sender	Displays RSVP PATH-related sender information currently in the database.

maximum (local policy)

To set the limits for Resource Reservation Protocol (RSVP) resources, use the **maximum** command in local policy configuration mode. To delete the limits, use the **no** form of this command.

maximum [**bandwidth** [**group** *x*] [**single** *y*] | **senders** *n*]

no maximum [**bandwidth** [**group** *x*] [**single** *y*] | **senders** *n*]

Syntax Description

bandwidth	(Optional) Indicates bandwidth limits for RSVP reservations.
group *x*	(Optional) Specifies the amount of bandwidth, in kbps, that can be requested by all the reservations covered by a local policy. The *x* value ranges from 1 to 10000000.
single *y*	(Optional) Specifies the maximum bandwidth, in kbps, that can be requested by any specific RSVP reservation covered by a local policy. The *y* value ranges from 1 to 10000000.
senders *n*	(Optional) Limits the number of RSVP senders affected by a local policy that can be active at the same time on a router. The value for *n* ranges from 1 to 50000; the default is 1000.

Command Default

No maximum bandwidth limit is set and no RSVP senders are configured.

Command Modes

Local policy configuration

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.4(6)T	This command was modified to apply to RESV messages.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Previously, the **maximum bandwidth** command applied only to PATH messages. However, as part of the application ID enhancement, this command now applies only to RESV messages. This change has the following benefits:

- Allows the local policy bandwidth limit to be used by RSVP's admission control process for both shared and nonshared reservations. Previous releases that performed group bandwidth checks on PATH messages could not account for bandwidth sharing and, as a result, you had to account for sharing by creating a larger maximum group bandwidth for the policy.
- Allows a local policy to trigger preemption during the admission control function if there is insufficient policy bandwidth to meet the needs of an incoming RESV message.

Examples

The following example specifies the maximum bandwidth for a group of reservations and for a single reservation, respectively:

```
Router(config-rsvp-local-policy)# maximum bandwidth group 500
Router(config-rsvp-local-policy)# maximum bandwidth single 50
```

Related Commands

Command	Description
ip rsvp policy local	Determines how to perform authorization on RSVP requests.

show ip rsvp host

To display specific information for a Resource Reservation Protocol (RSVP) host, use the **show ip rsvp host** command in user EXEC or privileged EXEC mode.

show ip rsvp host {**senders** | **receivers**} [*group-name* | *group-address*]

Syntax Description

senders	RSVP-related sender information currently in the database.
receivers	RSVP-related receiver information currently in the database.
group-name	(Optional) Hostname of the source or destination.
group-address	(Optional) IP address of the source or destination.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.4(6)T	The command output was modified to display RSVP identity information when configured.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **show ip rsvp host** command to display static RSVP senders and receivers. If a router has any local host receivers or senders that have RSVP identities configured, the application IDs that they use are also displayed.

Examples

In the following example from the **show ip rsvp host senders** command, no RSVP identities are configured for the local sender:

```
Router# show ip rsvp host senders

To              From            Pro DPort Sport Prev Hop      I/F      BPS
192.168.104.3 192.168.104.1 UDP 1     1                              10K
  Mode(s): Host CLI
```

Table 1 describes the significant fields shown in the display.

Table 1 show ip rsvp host senders (No RSVP Identities Configured) Field Descriptions

Field	Description
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. IP protocol such as TCP or UDP.

Table 1 show ip rsvp host senders (No RSVP Identities Configured) Field Descriptions

Field	Description
DPort	Destination port number. Code 1 indicates IP protocol such as TCP or UDP.
Sport	Source port number. Code 1 indicates IP protocol such as TCP or UDP.
Prev Hop	IP address of the previous hop. Blank means no previous hop.
I/F	Interface of the previous hop.
BPS	Reservation rate, in bits per second (bps).
Mode(s)	Any of the following strings: • Host—The router is acting as the host system or RSVP endpoint for this reservation. • LSP-Tunnel—The reservation is for a Traffic Engineering (TE) tunnel. • MIB—The reservation was created via an SNMP SET directive from a remote management station. • CLI—The reservation was created via a local RSVP CLI command. • Host CLI—A combination of the host and CLI strings meaning that the static sender being displayed was created by the **ip rsvp sender-host** CLI command.

In the following example from the **show ip rsvp host senders** command, an RSVP identity is configured for the local sender and more information displays:

```
Router# show ip rsvp host senders

To            From          Pro DPort Sport Prev Hop      I/F      BPS
192.168.104.3 192.168.104.1 UDP 1     1                            10K
  Mode(s): Host CLI
  Identity: voice100
    Locator: GUID=www.cisco.com,APP=voice,VER=100.0
    ID Type: Application
```

Table 2 describes the significant fields shown in the display.

Table 2 show ip rsvp host senders (RSVP Identity Configured) Field Descriptions

Field	Description
To	IP address of the receiver.
From	IP address of the sender.
Pro	Protocol code. IP protocol such as TCP or UDP.
DPort	Destination port number. Code 1 indicates IP protocol such as TCP or UDP.
Sport	Source port number. Code 1 indicates IP protocol such as TCP or UDP.

Table 2 show ip rsvp host senders (RSVP Identity Configured) Field Descriptions (continued)

Field	Description
Prev Hop	IP address of the previous hop. Blank means no previous hop.
I/F	Interface of the previous hop.
BPS	Reservation rate in bits per second (bps).
Mode(s)	Any of the following strings: • Host—The router is acting as the host system or RSVP endpoint for this reservation. • LSP-Tunnel—The reservation is for a Traffic Engineering (TE) tunnel. • MIB—The reservation was created via an SNMP SET directive from a remote management station. • CLI—The reservation was created via a local RSVP CLI command. • Host CLI—A combination of the host and CLI strings meaning that the static sender being displayed was created by the **ip rsvp sender-host** CLI command.
Identity	The alias string for the RSVP application ID.
Locator	The application ID that is being signaled in the RSVP PATH message for this statically-configured sender.
ID Type	Types of identities. RSVP defines two types: application IDs (Application) and user IDs (User). Cisco IOS software currently supports Application only.

Related Commands

Command	Description
ip rsvp sender-host	Enables a router to simulate a host generating an RSVP PATH message.

show ip rsvp policy identity

To display selected Resource Reservation Protocol (RSVP) identities in a router configuration, use the **show ip rsvp policy identity** command in user EXEC or privileged EXEC mode.

show ip rsvp policy identity [*regular-expression*]

Syntax Description

regular-expression	(Optional) String of text that allows pattern matching on the alias strings of the RSVP identities to be displayed.

Command Default

All configured RSVP identities are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Use the **show ip rsvp policy identity** command with the optional *regular-expression* argument to perform pattern matching on the alias strings of the RSVP identities to be displayed. Use this filtering capability to search for a small subset of RSVP identities in a configuration with a large number of identities.

Omit the *regular-expression* argument to display all the configured identities.

Examples

In the following example from the **show ip rsvp policy identity** command, all the configured identities are displayed:

```
Router# show ip rsvp policy identity

Alias: voice1
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=1.0
Alias: voice10
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=10.0
Alias: voice100
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=100.0
Alias: voice1000
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=1000.0
```

Table 3 describes the significant fields shown in the display.

Table 3 show ip rsvp policy identity Field Descriptions

Field	Description
Alias	Name of the alias string. The string can have as many as 64 printable characters (in the range 0x20 to 0x7E). The string has no maximum length and must contain printable characters (in the range 0x20 to 0x7E). **Note** If you use the " " or ? characters as part of the string itself, you must type the CTRL/V key sequence before entering the embedded " " or ? characters. The alias is never transmitted to other routers.
Type	Types of identities. RSVP defines two types: application IDs and user IDs. Cisco IOS software currently supports application IDs only.
Locator	Information used by a router to find the correct policy to apply to RSVP messages that contain application IDs.

In the following example from the **show ip rsvp policy identity** command, all the identities whose aliases contain voice100 display:

```
Router# show ip rsvp policy identity voice100

Alias: voice100
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=100.0
Alias: voice1000
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=1000.0
```

In the following example from the **show ip rsvp policy identity** command, all the identities whose aliases contain an exact match on voice100 are displayed:

```
Router# show ip rsvp policy identity ^voice100$

Alias: voice100
  Type:    Application ID
  Locator: GUID=www.cisco.com,APP=voice,VER=100.0
```

Related Commands

Command	Description
ip rsvp listener	Configures an RSVP router to listen for PATH messages.
ip rsvp policy identity	Defines RSVP application IDs.
ip rsvp policy local	Determines how to perform authorization on RSVP requests.
ip rsvp reservation	Enables a router to simulate receiving RSVP RESV messages.
ip rsvp sender	Enables a router to simulate receiving RSVP PATH messages.

show ip rsvp policy local

To display the local policies that are currently configured, use the **show ip rsvp policy local** command in user EXEC or privileged EXEC mode.

show ip rsvp policy local [**detail**] [**interface** *type number*] [**default** | **acl** *acl* | **origin-as** *as* | **identity** *alias*]

Syntax Description

detail	(Optional) Displays additional information about the configured local policies including preempt-priority and local-override.
interface *type name*	(Optional) Specifies an interface.
default	(Optional) Displays additional information about the default policy.
acl *acl*	(Optional) Specifies an access control list (ACL). Values are 1 to 199.
origin-as *as*	(Optional) Specifies an autonomous system. Values are 1 to 65535.
identity *alias*	(Optional) Specifies an application identity (ID) alias.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.0(29)S	The **origin-as** *as* keyword and argument combination was added, and the *acl* argument became optional.
12.4(6)T	The **identity** *alias* and the **interface** *type number* keyword and argument combinations were added, and the output was modified to include application ID information.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.

Usage Guidelines

Use the **show ip rsvp policy local** command to display information about the selected local policies that are currently configured. You can use the **default** keyword and/or the **interface** *type number* keyword and argument combination with one or more of the match criteria.

If you omit the **acl** *acl,* the **origin-as** *as,* or the **identity** *alias* keyword and argument combinations, all local policies currently configured appear.

If you use the ACL, the autonomous system, or the application-ID options as match criteria, you can specify only one. However, that parameter can be any ACL, autonomous system, or application ID of any local policy that you have created. If you have multiple local policies with a common match criteria, using that parameter displays all local policies that meet the match criteria. On the other hand, if you have created local policies each with multiple ACLs, autonomous systems, or application IDs as the match criteria, you cannot use that parameter to show only a specific policy. You must omit the match criteria and show all the local policies.

Examples

The following sample output from the **show ip rsvp policy local** command **displays** global and per-interface local policies based on RSVP identities (application IDs) that have been configured:

```
Router# show ip rsvp policy local

  A=Accept    F=Forward

  Global:
    Path:AF Resv:AF PathErr:AF ResvErr:AF ACL(s):101
    Path:AF Resv:AF PathErr:AF ResvErr:AF AS(es):3
    Path:AF Resv:AF PathErr:AF ResvErr:AF ID:voice
    Path:AF Resv:AF PathErr:AF ResvErr:AF ID:video

  Serial2/0/0:
    Path:AF Resv:AF PathErr:AF ResvErr:AF ID:voice
    Path:AF Resv:AF PathErr:AF ResvErr:AF ID:video

  Serial2/0/1:
    Path:AF Resv:AF PathErr:AF ResvErr:AF ID:conference
    Path:AF Resv:AF PathErr:AF ResvErr:AF ID:iptv
    Path:-- Resv:-- PathErr:-- ResvErr:-- Default

Generic policy settings:
    Default policy: Accept all
    Preemption:     Disabled
```

Table 4 describes the significant fields shown in the display.

Table 4 show ip rsvp policy local Field Descriptions

Field	Description
A=Accept F=Forward	State of RSVP messages. • Accept—Messages being accepted. • Forward—Messages being forwarded.
Global	Location of the local policy. Global—Local policy configured for the entire router.
Path, Resv, PathErr, ResvErr, ACL(s), AS(es), ID, Default	Types of RSVP messages being accepted and forwarded and the match criteria for the local policies configured. Blank (--) means that messages of the specified type are neither accepted nor forwarded.
Interface	Location of the local policy. Serial2/0/0—Local policy configured for a specific interface on the router.

Table 4 show ip rsvp policy local Field Descriptions (continued)

Field	Description
Path, Resv, PathErr, ResvErr, ACL(s), AS(es), ID	Types of RSVP messages being accepted and forwarded and the types of local policies configured. Blank (--) means that messages of the specified type are neither accepted nor forwarded.
Generic policy settings	Policy settings that are not specific to any local or remote policy. • Default policy: Accept all means that all RSVP messages are accepted and forwarded. Reject all means that all RSVP messages are rejected. • Preemption: Disabled means that RSVP should not implement any preemption decisions required by a particular local or remote policy. Enabled means that RSVP should implement any preemption decisions required by a particular local or remote policy.

The following sample output from the **show ip rsvp policy local detail** command **shows** the location of the local policy (such as whether the policy is configured globally or for a specific interface, and the settings for preemption scope and maximum bandwidth. Preemption priorities and sender and receiver limits also appear even if they are set to their defaults.

```
Router# show ip rsvp policy local detail

Global:
  Policy for ID: voice

    Preemption Scope: Unrestricted.
    Local Override:   Disabled.
    Fast ReRoute:     Accept.
    Handle:           02000409.

                          Accept              Forward
    Path:                 Yes                 Yes
    Resv:                 Yes                 Yes
    PathError:            Yes                 Yes
    ResvError:            Yes                 Yes

                          Setup Priority      Hold Priority
    TE:                   N/A                 N/A
    Non-TE:               N/A                 N/A

                          Current             Limit
    Senders:              0                   40
    Receivers:            0                   N/A
    Conversations:        0                   N/A
    Group bandwidth (bps): 0                  200K
    Per-flow b/w (bps):   N/A                 10M


  Policy for ID: video

    Preemption Scope: Unrestricted.
    Local Override:   Disabled.
    Fast ReRoute:     Accept.
    Handle:           0200040A.
```

```
                          Accept               Forward
    Path:                 Yes                  Yes
    Resv:                 Yes                  Yes
    PathError:            Yes                  Yes
    ResvError:            Yes                  Yes

                          Setup Priority       Hold Priority
    TE:                   2                    2
    Non-TE:               5                    4

                          Current              Limit
    Senders:              2                    10
    Receivers:            2                    10
    Conversations:        2                    10
    Group bandwidth (bps): 100K                200K
    Per-flow b/w (bps):   N/A                  10M


Ethernet2/1:
  Policy for ID: voice

    Preemption Scope: Unrestricted.
    Local Override:   Disabled.
    Fast ReRoute:     Accept.
    Handle:           0200040B.

                          Accept               Forward
    Path:                 Yes                  Yes
    Resv:                 Yes                  Yes
    PathError:            Yes                  Yes
    ResvError:            Yes                  Yes

                          Setup Priority       Hold Priority
    TE:                   2                    2
    Non-TE:               5                    4

                          Current              Limit
    Senders:              2                    10
    Receivers:            2                    10
    Conversations:        2                    10
    Group bandwidth (bps): 100K                200K
    Per-flow b/w (bps):   N/A                  10M


Generic policy settings:
    Default policy: Accept all
    Preemption:     Disabled
```

Table 5 describes the significant fields shown in the display.

Table 5 show ip rsvp policy local detail Field Descriptions

Field	Description
Global	Location of the local policy. Global—Local policy configured for the entire router.
Policy for ID	A global local policy defined for an application ID alias named voice.

Table 5 show ip rsvp policy local detail Field Descriptions (continued)

Field	Description
Preemption Scope	Describes which classes of RSVP quality of service (QoS) reservations can be preempted by other classes of RSVP QoS reservations on the same interface. Unrestricted means that a reservation using an application ID such as voice can preempt any other class of reservation on the same interface as that reservation, even other nonvoice reservations.
Local Override	Overrides any remote policy by enforcing the local policy in effect. • Disabled—Not active. • Enabled—Active.
Fast ReRoute	State of Fast ReRoute for Multiprotocol Label Switching (MPLS)/Traffic Engineering (TE) label switched paths (LSPs). • Accept—Messages being accepted. • Do not accept—Messages requesting Fast Reroute service are not being accepted.
Handle	Internal database ID assigned to the security association by RSVP for bookkeeping purposes.
Accept, Forward	State of RSVP messages.
Path, Resv, PathError, ResvError	Types of RSVP messages being accepted and forwarded. • Yes—Messages are being accepted and forwarded. • No—Messages are not being accepted or forwarded.
Setup Priority, Hold Priority	Preemption priorities. Setup Priority indicates the priority of a reservation when it is initially installed. Hold Priority indicates the priority of a reservation after it has been installed. N/A means preemption priorities are not configured.
TE	The preemption priority of TE reservations. Values for Setup Priority and Hold Priority range from 0 to 7 where 0 is considered the highest priority.
Non-TE	The preemption priority of non-TE reservations. Values for Setup Priority and Hold Priority range from 0 to 65535 where 65535 is considered the highest priority.
Current, Limit	The present number and the highest number of these parameters allowed.
Senders	The number of current PATH states accepted and/or approved by this policy.
Receivers	The number of current RESV states accepted by this policy.
Conversations	The number of active bandwidth requests approved by the local policy.
Group bandwidth (bps)	Amount of bandwidth configured for a class of reservations in bits per second (bps).

Table 5 show ip rsvp policy local detail Field Descriptions (continued)

Field	Description
Per-flow b/w (bps)	Amount of bandwidth configured for each reservation in bits per second (bps).
Interface	Location of the local policy. Ethernet2/1—Local policy configured for a specific interface on the router.
Generic policy settings	Policy settings that are not specific to the local policy. • Default policy: Accept all means that all RSVP messages are accepted and forwarded. Reject all means that all RSVP messages are rejected. • Preemption: Disabled means that RSVP should not implement any preemption decisions required by a particular local or remote policy. Enabled means that RSVP should implement any preemption decisions required by a particular local or remote policy.

Related Commands

Command	Description
ip rsvp policy local	Determines how to perform authorization on RSVP requests.

Feature Information for RSVP Application ID Support

Table 6 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 6 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 6 Feature Information for RSVP Application ID Support

Feature Name	Releases	Feature Information
RSVP Application ID Support	12.4(6)T, 12.2(33)SRB	The RSVP Application ID Support feature introduces application-specific reservations, which enhance the granularity for local policy-match criteria so that you can manage quality of service (QoS) on the basis of application type.

Glossary

ACL—access control list. An ACL consists of individual filtering rules grouped together in a single list. It is generally used to provide security filtering, although it may be used to provide a generic packet classification facility.

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

application identity (ID)—A string that can be inserted in a policy element in a POLICY_DATA object of an RSVP message to identify the application and associate it with the RSVP reservation request, thus allowing routers along the path to make appropriate decisions based on the application information.

autonomous system—A collection of networks that share the same routing protocol and that are under the same system administration.

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

Cisco Unified Communications Manager—Formerly known as Cisco CallManager. The software-based, call-processing component of the Cisco IP telephony solution. The software extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, Voice-over-IP (VoIP) gateways, and multimedia applications.

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.

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

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.

RSVP agent—Implements a Resource Reservation Protocol (RSVP) agent on Cisco IOS voice gateways that support Cisco CallManager 5.0.

RTP—Real-Time Transport Protocol. An Internet protocol for transmitting real-time data such as voice and video.

router—A network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another on the basis of network layer information.

TE—traffic engineering. The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.

Note See *Internetworking Terms and Acronyms* for terms not included in this glossary.