



RSVP Application ID Support

First Published: February 27, 2006

Last Updated: February 19, 2007

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.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. 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 23.

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

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

Contents

- [Prerequisites for RSVP Application ID Support, page 2](#)
- [Restrictions for RSVP Application ID Support, page 2](#)
- [Information About RSVP Application ID Support, page 2](#)
- [How to Configure RSVP Application ID Support, page 5](#)
- [Configuration Examples for RSVP Application ID Support, page 16](#)
- [Additional References, page 20](#)
- [Command Reference, page 22](#)
- [Feature Information for RSVP Application ID Support, page 23](#)
- [Glossary, page 24](#)



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

© 2007 Cisco Systems, Inc. All rights reserved.

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 IP 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**

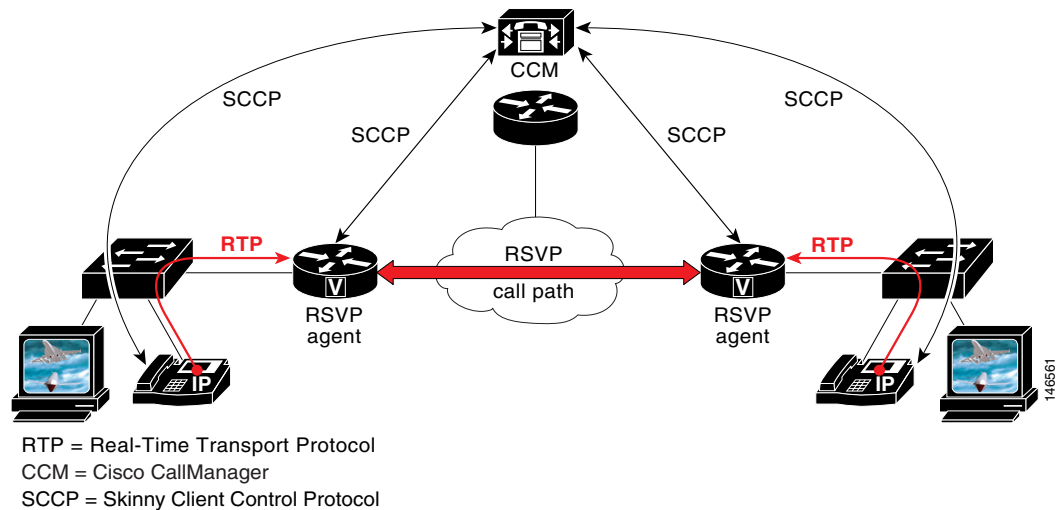
Before this feature, you could create access control lists (ACLs) that match on the differentiated services code points (DSCPs) of the IP header in an RSVP message. However, multiple applications could use the same DSCP; therefore, you could not uniquely identify applications in order to define separate 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 CallManager (CCM). Video requires much more bandwidth than voice, and if you do not separate the reservations, the video traffic could overwhelm the voice traffic.

CCM has been enhanced to use the RSVP Application ID Support feature. In this example, when CCM makes the RSVP reservation, CCM 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 CCM 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



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, CCM communicates with the RSVP agent and sends the parameters to reserve the necessary bandwidth.

When you want to make a voice or video call, the device signals CCM. CCM signals the RSVP agent, specifying the RSVP application ID that corresponds to the type of call, which is voice or video in this example. The RSVP agents establish the RSVP reservation across the network and tell CCM that the reservation has been made. CCM then completes the session establishment, and the Real-Time Transport

Protocol (RTP) traffic streams flow between the phones (or video devices). If the RSVP agents are unable to create the bandwidth reservations for the requested application ID, they communicate that information back to CCM, which signals this information back to you.

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 that has an RSVP bandwidth limit (as configured with the **maximum bandwidth group** submode command) and that limit has been reached, RSVP tries to preempt other lower-priority reservations admitted by that policy. When there are too few of these lower-priority reservations, RSVP rejects the incoming reservation request. Then RSVP looks at the interface bandwidth pool that you configured by using the **ip rsvp bandwidth** command. If that bandwidth limit has been reached, RSVP tries to preempt other lower-priority reservations on that interface to accommodate the new reservation request. At this point, RSVP does not consider which local policies admitted the reservations. When not enough bandwidth on that interface pool can be preempted, 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 offending 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 its neighbors.

If a received RSVP PATH or RESV message does not contain preemption priorities (as previously described) and you issued a global **ip rsvp policy preempt** command, and the message matches a local policy that contains a **preempt-priority** command, 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 then stored with the RSVP state in the router and forwarded to neighbors.

Controlling 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 CCM 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 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 to use with RSVP-aware software programs such as CCM or to 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 14](#) (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 The following two local policy configuration procedures are optional; however, you must choose one or both.

- [Configuring a Local Policy Globally, page 7](#) (optional)
- [Configuring a Local Policy on an Interface, page 8](#) (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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<pre>ip rsvp policy identity alias policy-locator locator</pre> <p>Example:</p> <pre>Router(config)# ip rsvp policy identity rsvp-voice policy-locator APP=Voice</pre>	<p>Defines RSVP application IDs to use as match criteria for local policies.</p> <ul style="list-style-type: none"> Enter a value for the <i>alias</i> 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). <p>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.</p> <ul style="list-style-type: none"> Enter a value for the <i>locator</i> 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	<pre>end</pre> <p>Example:</p> <pre>Router(config)# end</pre>	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

- enable**
- configure terminal**
- ip rsvp policy local {acl *acl1* [*acl2...acl8*] | default | identity *alias1* [*alias2...alias4*] | origin-as *as1* [*as2...as8*]}**
- Repeat Step 3 as needed to configure additional local policies.
- {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*]}**
- Repeat Step 5 as needed to configure additional submenu commands.
- end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	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. <ul style="list-style-type: none">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 submenu 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 submenu commands.
Step 6	Repeat Step 5 as needed to configure additional submenu commands.	(Optional) Configures additional submenu 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

- enable**
- configure terminal**
- interface** *type number*
- Repeat Step 3 as needed to configure additional interfaces.
- ip rsvp bandwidth** [*interface-kbps*] [*single-flow-kbps*]
- 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 submenu commands.
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface <i>type number</i> 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 [<i>interface-kbps</i>] [<i>single-flow-kbps</i>] Example: Router(config-if)# ip rsvp bandwidth 500 500	Enables RSVP on an interface. <ul style="list-style-type: none"> The optional <i>interface-kbps</i> and <i>single-flow-kbps</i> arguments specify the amount of bandwidth that can be allocated by RSVP flows or to a single flow, respectively. Values are from 1 to 1000,000.
Step 6	Repeat Step 5 as needed to configure bandwidth for additional interfaces.	(Optional) Configures bandwidth for additional interfaces.
Step 7	ip rsvp policy local { acl <i>acl1</i> [<i>acl2...acl8</i>] default identity <i>alias1</i> [<i>alias2...alias4</i>] origin-as <i>as1</i> [<i>as2...as8</i>]} 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. <ul style="list-style-type: none"> Enter the identity <i>alias1</i> 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.

Command or Action	Purpose
Step 9 <pre>{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]}</pre> Example: <pre>Router(config-rsvp-policy-local)# forward all</pre>	(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: <pre>Router(config-rsvp-policy-local)# end</pre>	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 11](#) (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	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>ip rsvp policy identity alias policy-locator locator</p> <p>Example: Router(config)# ip rsvp policy identity rsvp-voice policy-locator "APP=Voice"</p>	<p>Defines RSVP application IDs to use as match criteria for local policies.</p> <ul style="list-style-type: none"> Enter a value for the <i>alias</i> 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). <p>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.</p> <ul style="list-style-type: none"> Enter a value for the <i>locator</i> argument, which is a string that is signaled in RSVP messages and contains application IDs usually in X.500 Distinguished Name (DN) format. <p>Note Repeat this step as needed to configure additional application IDs.</p>
Step 4	Repeat step 3 to configure additional application IDs.	Configures additional application IDs.
Step 5	<p>end</p> <p>Example: Router(config)# end</p>	<p>Exits global configuration mode and returns to privileged EXEC mode.</p>

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

- enable**
- 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	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>ip rsvp sender-host <i>session-ip-address sender-ip-address</i> {tcp udp <i>ip-protocol</i>} <i>session-d-port sender-s-port bandwidth burst-size</i> [identity alias]</p> <p>Example: Router(config)# ip rsvp sender-host 10.0.0.7 10.0.0.1 udp 1 1 10 10 identity rsvp-voice</p>	<p>Enables a router to simulate a host generating RSVP PATH messages.</p> <ul style="list-style-type: none"> • 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). <p>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.</p>
Step 4	<p>end</p> <p>Example: Router(config)# end</p>	<p>Exits global configuration mode and returns to privileged EXEC mode.</p>

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 and/or a preemption priority value, the listener includes them in the RESV message sent in reply. See the “[Feature Information for RSVP Application ID Support](#)” section on [page 23](#) 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. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.

Command or Action	Purpose
<p>Step 3</p> <pre>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]</pre> <p>Example:</p> <pre>Router(config)# ip rsvp reservation-host 10.1.1.1 10.30.1.4 udp 20 30 se load 100 60 identity rsvp-voice</pre> <pre>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</pre>	<p>Enables a router to simulate a host generating RSVP RESV messages.</p> <ul style="list-style-type: none"> 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). <p>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.</p> <p>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.</p>
<p>Step 4</p> <pre>end</pre> <p>Example:</p> <pre>Router(config)# end</pre>	<p>Exits global configuration mode and returns to privileged EXEC mode.</p>

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	<p>enable</p> <p>Example: Router> enable</p>	<p>(Optional) Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted. <p>Note Skip this step if you are using the commands in user EXEC mode.</p>
Step 2	<p>show ip rsvp host {senders receivers} [group-name group-address]</p> <p>Example: Router# show ip rsvp host senders</p>	<p>Displays specific information for an RSVP host.</p> <p>Note Use this command only on routers from which PATH and RESV messages originate.</p>
Step 3	<p>show ip rsvp policy identity [regular-expression]</p> <p>Example: Router# show ip rsvp policy identity voice100</p>	<p>Displays selected RSVP identities in a router configuration.</p> <ul style="list-style-type: none"> The optional <i>regular-expression</i> argument allows pattern matching on the alias strings of the RSVP identities to be displayed. <p>Note For more information on regular expressions, see the “Related Documents” section on page 21.</p>
Step 4	<p>show ip rsvp policy local [detail] [interface name] [default acl acl origin-as as identity alias]</p> <p>Example: Router# show ip rsvp policy local identity voice100</p>	<p>Displays the local policies currently configured.</p> <ul style="list-style-type: none"> The optional detail keyword and the optional interface name keyword and argument combination can be used with any of the match criteria.
Step 5	<p>show ip rsvp reservation [detail] [filter [destination ip-addr hostname] [source ip-addr hostname] [dst-port port] [src-port port]]</p> <p>Example: Router# show ip rsvp reservation detail</p>	<p>Displays RSVP-related receiver information currently in the database.</p> <ul style="list-style-type: none"> 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. <p>Note The optional filter keyword is supported in Cisco IOS Releases 12.0S and 12.2S only.</p>
Step 6	<p>show ip rsvp sender [detail] [filter [destination ip-addr hostname] [source ip-addr hostname] [dst-port port] [src-port port]]</p> <p>Example: Router# show ip rsvp sender detail</p>	<p>Displays RSVP PATH-related sender information currently in the database.</p> <ul style="list-style-type: none"> The optional detail keyword displays additional output with information that includes which application ID was signaled in the PATH message. <p>Note The optional filter keyword is supported in Cisco IOS Releases 12.0 S and 12.2 S only.</p>
Step 7	<p>exit</p> <p>Example: Router# exit</p>	<p>Exits privileged EXEC mode and returns to user EXEC mode.</p>

Configuration Examples for RSVP Application ID Support

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

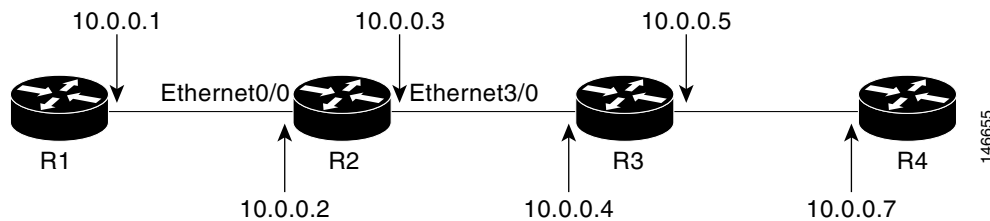
- [Configuring RSVP Application ID Support: Example, page 16](#)
- [Verifying RSVP Application ID Support: Example, page 18](#)

Configuring RSVP Application ID Support: Example

The four-router network in [Figure 2](#) contains the following configurations:

- [Configuring a Proxy Receiver on R4, page 16](#)
- [Configuring an Application ID and a Global Local Policy on R3, page 16](#)
- [Configuring an Application ID and Separate Bandwidth Pools on R2 for Per-Interface Local Policies, page 17](#)
- [Configuring an Application ID and a Static Reservation from R1 to R4, page 17](#)

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, page 18](#)
- [Verifying the Application ID and the Per-Interface Local Policies on R2, page 18](#)
- [Verifying the Application ID and the Reservation on R1, page 20](#)

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 related to RSVP	“Configuring RSVP” module
Cisco Unified Communications Manager (CallManager) and related features	“Overview of Cisco Unified Communications Manager and Cisco IOS Interoperability” module
Regular expressions	“Using the Cisco IOS Command-Line Interface” module

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
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	<p>http://www.cisco.com/techsupport</p>

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Quality of Service Solutions Command Reference* at http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.

- **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**

Feature Information for RSVP Application ID Support

Table 1 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 1 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 1 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.

CCM—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.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

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

© 2007 Cisco Systems, Inc. All rights reserved.

