QoS: RSVP Configuration Guide, Cisco IOS XE Release 3S (Cisco ASR 1000)

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

RSVP Aggregation

The RSVP Aggregation feature allows the Resource Reservation Protocol (RSVP) state to be reduced within an RSVP/DiffServ network by aggregating many smaller reservations into a single, larger reservation at the edge.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for RSVP Aggregation

You must configure at least two aggregating nodes (provider edge [PE] devices), one interior node (provider [P] device) and two end user nodes (customer edge [CE] devices) within your network.

You must configure your network to support the following Cisco IOS features:

- RSVP
- Class Based Weighted Fair Queuing (CBWFQ)
- RSVP Scalability Enhancements

Note You configure these features because Cisco IOS Release 12.2(33)SRC supports control plane aggregation only. Dataplane aggregation must be achieved by using the RSVP Scalability Enhancements.

Restrictions for RSVP Aggregation

Functionality Restrictions

The following functionality is not supported:

- Multilevel aggregation
- Multiple, adjacent aggregation regions
- Dynamic resizing of aggregate reservations
- Policing of end-to-end (E2E) reservations by the aggregator
- Policing of aggregate reservations by interior devices
- Differentiated Services Code Point (DSCP) marking by the aggregator
- Equal Cost Multiple Paths (ECMP) load-balancing within the aggregation region
- RSVP Fast Local Repair in case of a routing change resulting in a different aggregator or deaggregator, admission control is performed on E2E PATH refresh
- Multicast RSVP reservations
- RSVP policy servers including Common Open Policy Server (COPS)
- Dataplane aggregation

The following functionality is supported:

- Multiple, non-adjacent aggregation regions
- Control plane aggregation

Note RSVP/DiffServ using CBWFQ provides the dataplane aggregation.

Configuration Restrictions

- Sources should not send marked packets without an installed reservation.
- Sources should not send marked packets that exceed the reserved bandwidth.
- Sources should not send marked packets to a destination other than the reserved path.
- All RSVP capable devices within an aggregation region regardless of role must support the aggregation feature to recognize the RFC 3175 RSVP message formats properly.
- E2E reservations must be present to establish dynamic aggregates; aggregates cannot be established manually.
- Aggregates are established at a fixed bandwidth regardless of the number of current E2E reservations being aggregated.
- Aggregators and deaggregators must be paired to avoid blackholing of E2E reservations because of dynamic aggregate establishment.

Note Blackholing means that the reservation is never established. If an E2E reservation crosses from an exterior to an interior interface, the E2E reservation turns into an RSVP-E2E-IGNORE protocol packet. If there is no corresponding deaggregator, a device where this RSVP-E2E-IGNORE reservation crosses an interior to an exterior interface, then the RSVP-E2E-IGNORE reservation is never restored to an E2E reservation. The RSVP-E2E-IGNORE reservation eventually reaches its destination, which is the RSVP receiver; however, the RSVP receiver does not know what to do with the RSVP-E2E-IGNORE reservation and discards the packet.

Information About RSVP Aggregation

Feature Overview of RSVP Aggregation

High Level Overview

The establishment of a single RSVP reservation requires a large amount of resources including memory allocated for the associated data structures, CPU for handling signaling messages, I/O operations for datapath programming, interprocess communication, and signaling message transmission.

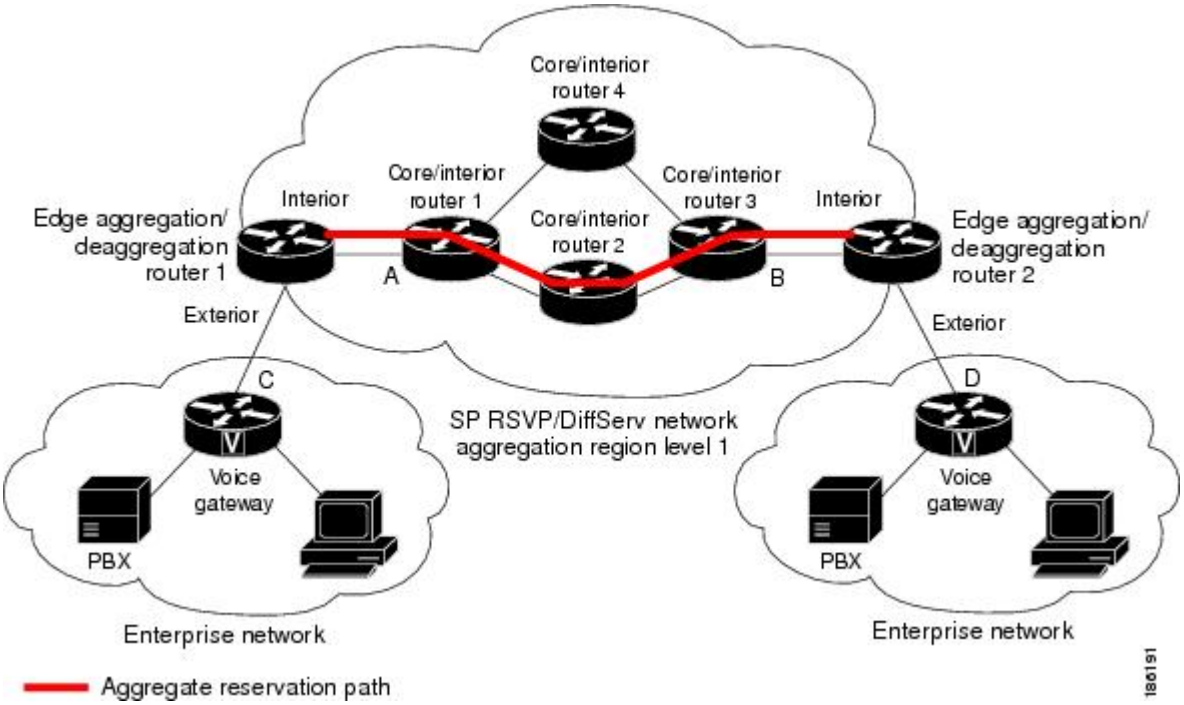
When a large number of small reservations are established, the resources required for setting and maintaining these reservations may exceed a node's capacity to the point where the node's performance is significantly degraded or it becomes unusable. The RSVP Aggregation feature addresses this scalability issue by introducing flow aggregation.

Flow aggregation is a mechanism wherein RSVP state can be reduced within a core device by aggregating many smaller reservations into a single, larger reservation at the network edge. This preserves the ability to perform connection admission control on core device links within the RSVP/DiffServ network while reducing signaling resource overhead.

How Aggregation Functions

Common segments of multiple end-to-end (E2E) reservations are aggregated over an aggregation region into a larger reservation that is called an aggregate reservation. An aggregation region is a connected set of nodes that are capable of performing RSVP aggregation as shown in the figure below.

Figure 1 RSVP Aggregation Network Overview



There are three types of nodes within an aggregation region:

- Aggregator--Aggregates multiple E2E reservations.
- Deaggregator--Deaggregates E2E reservations; provides mapping of E2E reservations onto aggregates.
- Interior--Neither aggregates or deaggregates, but is an RSVP core router that understands RFC 3175 formatted RSVP messages. Core/interior routers 1 through 4 are examples shown in the figure above.

There are two types of interfaces on the aggregator/deaggregator nodes:

- Exterior interface--The interface is not part of the aggregate region.
- Interior interface--The interface is part of the aggregate region.

Any router that is part of the aggregate region must have at least one interior interface and may have one or more exterior interfaces. Depending on the types of interfaces spanned by an IPv4 flow, a node can be an aggregator, a deaggregator, or an interior router with respect to that flow.

- Aggregate RSVP DiffServ Integration Topology, page 4

Aggregate RSVP DiffServ Integration Topology

RSVP aggregation further enhances RSVP scalability within an RSVP/DiffServ network as shown in the figure above by allowing the establishment of aggregate reservations across an aggregation region. This allows for aggregated connection admission control on core/interior device interfaces. Running RSVP on the core/interior devices allows for more predictable bandwidth use during normal and failure scenarios.

The voice gateways are running classic RSVP, which means RSVP is keeping a state per flow and also classifying, marking, and scheduling packets on a per-flow basis. The edge/aggregation devices are running RSVP with scalability enhancements for admission control on the exterior interfaces connected to the voice gateways and running RSVP aggregation on the interfaces connected to core/interior devices 1 and 3. The core/interior devices in the RSVP/DiffServ network are running RSVP for the establishment of the aggregate reservations. The edge and core/interior devices inside the RSVP/DiffServ network also implement a specific per hop behavior (PHB) for a collection of flows that have the same DSCP.

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

The interior interfaces on the edge/aggregation/deaggregation devices (labeled A and B) connected to core/interior devices 1 and 3 are running RSVP aggregation. They are performing admission control only per flow against the RSVP bandwidth of the aggregate reservation for the corresponding DSCP.

Admission control is performed at the deaggregator because it is the first edge node to receive the returning E2E RSVP RESV message. CBWFQ is performing the classification, policing, and scheduling functions on all nodes within the RSVP/DiffServ network including the edge devices.

Aggregate reservations are dynamically established over an aggregation region when an E2E reservation enters an aggregation region by crossing from an exterior to an interior interface; for example, when voice gateway C initiates an E2E reservation to voice gateway D. The aggregation is accomplished by "hiding" the E2E RSVP messages from the RSVP nodes inside the aggregation region. This is achieved with a new IP protocol, RSVP-E2E-IGNORE, that replaces the standard RSVP protocol in E2E PATH, PATHTEAR, and RESVCONF messages. This protocol change to RSVP-E2E-IGNORE is performed by the aggregator when the message enters the aggregation region and later restored back to RSVP by the deaggregator when the message exits the aggregation region. Thus, the aggregator and deaggregator pairs for a given flow are dynamically discovered during the E2E PATH establishment.

The deaggregator device 2 is responsible for mapping the E2E PATH onto an aggregate reservation per the configured policy. If an aggregate reservation with the corresponding aggregator device 1 and a DSCP is established, the E2E PATH is forwarded. Otherwise a new aggregate at the requisite DSCP is established, and then the E2E PATH is forwarded. The establishment of this new aggregate is for the fixed bandwidth parameters configured at the deaggregator device 2. Aggregate PATH messages are sent from the aggregator to the deaggregator using RSVP's normal IP protocol. Aggregate RESV messages are sent back from the deaggregator to the aggregator, thus establishing an aggregate reservation on behalf of the set of E2E flows that use this aggregator and deaggregator. All RSVP capable interior nodes process the aggregate reservation request following normal RSVP processing including any configured local policy.

The RSVP-E2E-IGNORE messages are ignored by the core/interior devices, no E2E reservation states are created, and the message is forwarded as IP. As a consequence, the previous hop/next hop (PHOP/ NHOP) for each RSVP-E2E-IGNORE message received at the deaggregator or aggregator is the aggregator or deaggregator node. Therefore, all messages destined to the next or previous hop (RSVP error messages, for example) do not require the protocol to be changed when they traverse the aggregation region.

By setting up a small number of aggregate reservations on behalf of a large number of E2E flows, the number of states stored at core/interior devices and the amount of signal processing within the aggregation region is reduced.

In addition, by using differentiated services mechanisms for classification and scheduling of traffic supported by aggregate reservations rather than performing per aggregate reservation classification and scheduling, the amount of classification and scheduling state in the aggregation region is further reduced. This reduction is independent of the number of E2E reservations and the number of aggregate reservations in the aggregation region. One or more RSVP/DiffServ DSCPs are used to identify the traffic covered by aggregate reservations, and one or more RSVP/DiffServ per hop behaviors (PHBs) are used to offer the required forwarding treatment to this traffic. There may be more than one aggregate reservation between

the same pair of devices, each representing different classes of traffic and each using a different DSCP and a different PHB.

Integration with RSVP Features

RSVP aggregation has been integrated with many RSVP features, including the following:

- RSVP Fast Local Repair
- RSVP Local Policy Support
- RSVP Refresh Reduction and Reliable Messaging

Benefits of RSVP Aggregation

Enhanced Scalability

Aggregating a large number of small reservations into one reservation requires fewer resources for signaling, setting, and maintaining the reservation thereby increasing scalability.

Enhanced Bandwidth Usage within RSVP/DiffServ Core Network

Aggregate reservations across an RSVP/DiffServ network allow for more predictable bandwidth use of core links across RSVP/DiffServ PHBs. Aggregate reservations can use RSVP fast local repair and local policy preemption features for determining bandwidth use during failure scenarios.

How to Configure RSVP Aggregation

Configuring RSVP Scalability Enhancements

Perform these tasks on all nodes within the aggregation region including aggregators, deaggregators, and interior nodes.

Enabling RSVP on an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *subslot* / *port*
4. **ip rsvp bandwidth** [*interface-kbps* [*single-flow-kbps*[**bc1** *kbps* | **sub-pool** *kbps*]/| **percent** *percent-bandwidth* [*single-flow-kbps*]]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type slot* / *subslot* / *port* **Example:** Router(config)# interface gigabitEthernet 0/0/0	Configures the interface type and enters interface configuration mode.
Step 4	**ip rsvp bandwidth** [*interface-kbps* [*single-flow-kbps*[**bc1** *kbps* | **sub-pool** *kbps*]/| **percent** *percent-bandwidth* [*single-flow-kbps*]] **Example:** Router(config-if)# ip rsvp bandwidth 500 500	Enables RSVP bandwidth 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 10000000. **Note** Repeat this command for each interface that you want to enable.
Step 5	**end** **Example:** Router(config-if)# **end**	(Optional) Returns to privileged EXEC mode.

Setting the Resource Provider

Note Resource provider was formerly called QoS provider.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp bandwidth** [*interface-kbps* [*single-flow-kbps*[**bc1** *kbps* | **sub-pool** *kbps*]*]*| **percent** *percent-bandwidth* [*single-flow-kbps*]]
4. **ip rsvp resource-provider** [**none** | **wfq-interface** | **wfq-pvc**]
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 bandwidth** [*interface-kbps* [*single-flow-kbps*[**bc1** *kbps* | **sub-pool** *kbps*]*]*| **percent** *percent-bandwidth* [*single-flow-kbps*]] **Example:** Router(config-if)# ip rsvp bandwidth 500 500	Configures the interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**ip rsvp resource-provider** [**none** | **wfq-interface** | **wfq-pvc**] **Example:** Router(config-if)# ip rsvp resource-provider none	Sets the resource provider. • Enter the optional **none** keyword to set the resource provider to none regardless of whether one is configured on the interface. **Note** Setting the resource provider to **none** instructs RSVP to *not* associate any resources, such as weighted fair queueing (WFQ) queues or bandwidth, with a reservation. • Enter the optional **wfq-interface** keyword to specify WFQ as the resource provider on the interface. • Enter the optional **wfq-pvc** keyword to specify WFQ as the resource provider on the permanent virtual circuit (PVC) or connection.
Step 5	**end** **Example:** Router(config-if)# **end**	(Optional) Returns to privileged EXEC mode.

Disabling Data Packet Classification

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *subslot* / *port*
4. **ip rsvp data-packet classification none**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type slot* / *subslot* / *port* **Example:** Router(config)# interface gigabitEthernet 0/0/0	Configures the interface type and enters interface configuration mode.
Step 4	**ip rsvp data-packet classification none** **Example:** Router(config-if)# ip rsvp data-packet classification none	Disables data packet classification.
Step 5	**end** **Example:** Router(config-if)# **end**	(Optional) Returns to privileged EXEC mode.

Configuring Class and Policy Maps

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** [**type** {**stack** | **access-control**| **port-filter**| **queue-threshold**}] [**match-all**| **match-any**] *class-map-name*
4. **match access-group** {*access-group* | **name** *access-group-name*}
5. **exit**
6. **policy-map** [**type access-control**] *policy-map-name*
7. **class** {*class-name* | **class-default**}
8. **priority** {*bandwidth-kbps* | **percent** *percentage*} [*burst*]
9. **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	**class-map** [**type** {**stack** | **access-control**| **port-filter**| **queue-threshold**}] [**match-all**| **match-any**] *class-map-name* **Example:** Router(config)# class-map match-all voice	Creates a class map to be used for matching packets to a specified class and enters class-map configuration mode. • The optional **type stack** keywords enable the flexible packet matching (FPM) functionality to determine the correct protocol stack in which to examine. **Note** If the appropriate protocol header description files (PHDFs) have been loaded onto the router (via the **load protocol**command), a stack of protocol headers can be defined so the filter can determine which headers are present and in what order. • The optional **type access-control** keywords determine the exact pattern to look for in the protocol stack of interest. **Note** You must specify a stack class map (via the **type stack** keywords) before you can specify an access-control class map (via the type **access-control** keywords). • The optional **type port-filter** keywords create a port-filter class-map that enables the TCP/UDP port policing of control plane packets. **Note** When enabled, these keywords provide filtering of traffic destined to specific ports on the control plane host subinterface. • The optional **type queue-threshold** keywords enable queue thresholding that limits the total number of packets for a specified protocol that is allowed in the control plane IP input queue. This feature applies only to control plane host subinterface. • The optional **match-all** | **match-any** keywords determine how packets are evaluated when multiple match criteria exist. Packets must either meet all of the match criteria (**match-all**) or one of the match criteria (**match-any**) in order to be considered a member of the class.

	Command or Action	Purpose
Step 4	**match access-group** {*access-group* | **name** *access-group-name*} **Example:** Router(config-cmap)# match access-group 100	Specifies the numbered access list against whose contents packets are checked to determine if they match the criteria specified in the class map. **Note** After you create the class map, you configure its match criteria. Here are some of the commands that you can use: • ◦ **match access-group** ◦ **match input-interface** ◦ **match mpls experimental** ◦ **match protocol**
Step 5	**exit** **Example:** Router(config-cmap)# exit	Exits to global configuration mode.
Step 6	**policy-map** [**type access-control**] *policy-map-name* **Example:** Router(config)# policy-map wfq-voip	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy and enters policy-map configuration mode. • The optional **type access-control** keywords determine the exact pattern to look for in the protocol stack of interest.
Step 7	**class** {*class-name* | **class-default**} **Example:** Router(config-pmap-c)# class voice	Specifies the class so that you can configure or modify its policy. Enters policy-map class configuration mode. • Enter the *class name* or use the **class-default**keyword.
Step 8	**priority** {*bandwidth-kbps* | **percent** *percentage*} [*burst*] **Example:** Router(config-pmap-c)# priority 24	(Optional) Prioritizes a class of traffic belonging to a policy map. • The optional *burst* argument specifies the burst size in bytes. The burst size configures the network to accommodate temporary bursts of traffic. The default burst value, which is computed as 200 milliseconds of traffic at the configured bandwidth rate, is used when the *burst* argument is not specified. The range of the burst is from 32 to 2000000 bytes.
Step 9	**end** **Example:** Router(config--pmap-c)# **end**	(Optional) Returns to privileged EXEC mode.

Attaching a Policy Map to an Interface

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type slot* / *subslot* / *port* **Example:** Router(config)# interface gigabitEthernet 0/0/0	Configures the interface type and enters interface configuration mode.
Step 4	**service-policy** [**type access-control**] {**input**	**output**} *policy-map-name* **Example:** Router(config-if)# service-policy output POLICY-ATM	Specifies the name of the policy map to be attached to the input or output direction of the interface. **Note** Policy maps can be attached in the input or output direction of an interface. The direction and the router to which the policy map should be attached vary according to the network configuration. When using the **service-policy** command to attach the policy map to an interface, be sure to choose the router and the interface direction that are appropriate for the network configuration. • The optional **type access-control** keywords determine the exact pattern to look for in the protocol stack of interest. • Enter the *policy-map name*.

	Command or Action	Purpose
Step 5	**end** **Example:** Router(config-if)# **end**	(Optional) Returns to privileged EXEC mode.

Configuring Interfaces with Aggregation Role

Perform this task on aggregator and deaggregators to specify which interfaces are facing the aggregation region.

Note You do not need to perform this task on interior routers; that is, nodes having interior interfaces only.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *subslot* / *port*
4. **ip rsvp aggregation role interior**
5. Repeat Step 4 as needed to configure additional aggregator and deaggregator interfaces.
6. **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 slot* / *subslot* / *port* **Example:** Router(config)# interface gigabitEthernet 0/0/0	Configures the interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**ip rsvp aggregation role interior** **Example:** Router(config-if)# ip rsvp aggregation role interior	Enables RSVP aggregation on an aggregator or deaggregator's interface.
Step 5	Repeat Step 4 as needed to configure additional aggregator and deaggregator interfaces.	Configures additional aggregator and deaggregator interfaces.
Step 6	**end** **Example:** Router(config-if)# end	(Optional) Returns to privileged EXEC mode.

Configuring Aggregation Mapping on a Deaggregator

Note Typically, an edge router acts as both an aggregator and deaggregator because of the unidirectional nature of RSVP reservations. Most applications require bidirectional reservations. Therefore, these parameters are used by a deaggregator when mapping E2E reservations onto aggregates during the dynamic aggregate reservation process.

You should configure an access control list (ACL) to define a group of RSVP endpoints whose reservations will be aggregated onto a single aggregate reservation session identified by the specified DSCP. Then for each ACL, define a map configuration.

Note In classic (unaggregated) RSVP, a session is identified in the reservation message session object by the destination IP address and protocol information. In RSVP aggregation, a session is identified by the destination IP address and DSCP within the session object of the aggregate RSVP message. E2E reservations are mapped onto a particular aggregate RSVP session identified by the E2E reservation session object alone or a combination of the session object and sender template or filter spec.

Extended ACLs

The ACLs used within the **ip rsvp aggregation ip map** command match the RSVP message objects as follows for an extended ACL:

- Source IP address and port match the RSVP PATH message sender template or RSVP RESV message filter spec; this is the IP source or the RSVP sender.
- Destination IP address and port match the RSVP PATH/RESV message session object IP address; this is the IP destination address or the RSVP receiver.
- Protocol matches the RSVP PATH/RESV message session object protocol; if protocol = IP, then it matches the source or destination address as above.

Standard ACLs

The ACLs used within the **ip rsvp aggregation ip map** command match the RSVP message objects as follows for a standard ACL:

- IP address matches the RSVP PATH message sender template or RSVP RESV message filter spec; this is the IP source address or the RSVP sender.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp aggregation ip map** {**access-list** {*acl-number*} | **any**} **dscp** *value*
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 aggregation ip map** {**access-list** {*acl-number*}	**any**} **dscp** *value* **Example:** Router(config)# **ip rsvp aggregation ip map any dscp af41**	Configures RSVP aggregation rules that tell a router how to map E2E reservations onto aggregate reservations. • The keywords and arguments specify additional information such as DSCP values.
Step 4	**end** **Example:** Router(config)# end	(Optional) Returns to privileged EXEC mode.

Configuring Aggregate Reservation Attributes on a Deaggregator

Perform this task on a deaggregator to configure the aggregate reservation attributes (also called token bucket parameters) on a per-DSCP basis.

Note Typically, an edge device acts as both an aggregator and deaggregator because of the unidirectional nature of RSVP reservations. Most applications require bidirectional reservations. Therefore, these parameters are used by a deaggregator when mapping E2E reservations onto aggregates during the dynamic aggregate reservation process.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp aggregation ip reservation dscp** *value* [**aggregator** *agg-ip-address*] **traffic-params static rate** *data-rate* [**burst** *burst-size*] [**peak** *peak-rate*]
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**ip rsvp aggregation ip reservation dscp** *value* [**aggregator** *agg-ip-address*] **traffic-params static rate** *data-rate* [**burst** *burst-size*] [**peak** *peak-rate*] **Example:** Device(config)# **ip rsvp aggregation ip reservation dscp af11 aggregator 10.10.10.10 traffic-params static rate 10 burst 8 peak 10**	Configures RSVP aggregate reservation attributes (also called token bucket parameters) on a per-DSCP basis. • The keywords and arguments specify additional information.
Step 4	**end** **Example:** Device(config)# end	(Optional) Returns to privileged EXEC mode.

Configuring an RSVP Aggregation Device ID

Perform this task on aggregators and deaggregators to configure an RSVP aggregation device ID.

Note Both aggregators and deaggregators need to be identified with a stable and routable IP address. This is the RFC 3175 device ID, which is also the IP address of the loopback interface with the lowest number. If there is no loopback interface configured or all those configured are down, then there will be no device ID assigned for the aggregating/deaggregating function and aggregate reservations will not be established.

Note The device ID may change if the associated loopback interface goes down or its IP address is removed. In this case, the E2E and aggregate sessions are torn down. If a new device ID is determined, new E2E and aggregate sessions will use the new device ID.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface loopback** *number*
4. **ip address** *ip-address subnet-mask/prefix*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**interface loopback** *number* **Example:** Device(config)# interface loopback 1	Creates a loopback interface and enters interface configuration mode. • Enter a value for the *number* argument. The range is 0 to 2147483647.

	Command or Action	Purpose
Step 4	**ip address** *ip-address subnet-mask/prefix* **Example:** Device(config-if)# ip address 192.168.50.1 255.255.255.0	Configures an IP address and subnet mask or prefix on the loopback interface.
Step 5	**end** **Example:** Device(config-if)# end	(Optional) Returns to privileged EXEC mode.

Enabling RSVP Aggregation

Perform this task on aggregators and deaggregators to enable RSVP aggregation globally after you have completed all the previous aggregator and deaggregator configurations.

Note This task registers a device to receive RSVP-E2E-IGNORE messages. It is not necessary to perform this task on interior devices because they are only processing RSVP aggregate reservations. If you do so, you may decrease performance because the interior device will then unnecessarily process all the RSVP-E2E-IGNORE messages.

Note If you enable RSVP aggregation globally on an interior device, then you should configure all interfaces as interior.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp aggregation ip**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**ip rsvp aggregation ip** **Example:** Device(config)# ip rsvp aggregation ip	Enables RSVP aggregation globally on an aggregator or deaggregator.
Step 4	**end** **Example:** Device(config)# end	(Optional) Returns to privileged EXEC mode.

Configuring RSVP Local Policy

Perform this task to apply a local policy to an RSVP aggregate reservation.

Note In classic (unaggregated) RSVP, a session is identified in the reservation message session object by the destination IP address and protocol information. In RSVP aggregation, a session is identified by the destination IP address and DSCP within the session object of the aggregate RSVP message. The **dscp-ip** keyword matches the DSCP within the session object.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp policy local** {**acl** *acl1*[*acl2...acl8*] | **dscp-ip** *value1* [*value2 ... value8*] | **default** | **identity** *alias1* [*alias2...alias4*] | **origin-as** *as1*[*as2...as8*]}
4. {**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*]}
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 local** {**acl** *acl1*[*acl2...acl8*] | **dscp-ip** *value1* [*value2 ... value8*] | **default** | **identity** *alias1* [*alias2...alias4*] | **origin-as** *as1*[*as2...as8*]} **Example:** Router(config)# ip rsvp policy local **dscp-ip 46**	Creates a local policy to determine how RSVP resources are used in a network and enters local policy configuration mode. • Enter the **dscp-ip** *value*keyword and argument combination to specify a DSCP for matching the session object DCSP within the aggregate reservations. Values can be the following: ◦ 0 to 63--Numerical. The default value is 0. ◦ af11 to af43--Assured forwarding (AF). ◦ cs1 to cs7--Type of service (ToS) precedence. ◦ default--Default DSCP. ◦ ef--Expedited Forwarding (EF). **Note** You must associate at least one DSCP with a DSCP-based policy. However, you can associate as many as eight.
Step 4	{**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 dscp-ip 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 5	**end** **Example:** Router(config-rsvp-policy-local)# end	(Optional) Exits local policy configuration mode and returns to privileged EXEC mode.

Verifying the RSVP Aggregation Configuration

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

SUMMARY STEPS

1. **enable**
2. **show ip rsvp aggregation ip** [**endpoints** | **interface** [*if-name*] | **map** [**dscp** *value*]| **reservation** [**dscp** *value*[**aggregator** *ip-address*]]
3. **show ip rsvp aggregation ip endpoints** [**role**{**aggregator**| **deaggregator**}] [*ip-address*] [**dscp** *value*] [**detail**]
4. **show ip rsvp** [**atm-peak-rate-limit**| **counters**| **host**| **installed**| **interface**| **listeners**| **neighbor**| **policy**| **precedence**| **request**| **reservation**| **sbm**| **sender**| **signalling**| **tos**]
5. **show ip rsvp reservation** [**detail**] [**filter**[**destination** *ip-address* | *hostname*] [**dst-port** *port-number*] [**source** *ip-address* | *hostname*][**src-port** *port-number*]]
6. **show ip rsvp sender** [**detail**] [**filter**[**destination** *ip-address* | *hostname*] [**dst-port** *port-number*] [**source** *ip-address* | *hostname*][**src-port** *port-number*]]
7. **show ip rsvp installed** [*interface-type interface-number*] [**detail**]
8. **show ip rsvp interface** [**detail**] [*interface-type interface-number*]
9. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	(Optional) Enables privileged EXEC mode. • Enter your password if prompted. **Note** Skip this step if you are using the **show** commands in user EXEC mode.
Step 2	**show ip rsvp aggregation ip** [**endpoints**	**interface** [*if-name*]	**map** [**dscp** *value*]| **reservation** [**dscp** *value*[**aggregator** *ip-address*]] **Example:** Device# show ip rsvp aggregation ip	(Optional) Displays RSVP summary aggregation information. • The optional keywords and arguments display additional information.
Step 3	**show ip rsvp aggregation ip endpoints** [**role**{**aggregator**| **deaggregator**}] [*ip-address*] [**dscp** *value*] [**detail**] **Example:** Device# show ip rsvp aggregation ip endpooints	(Optional) Displays RSVP information about aggregator and deaggregator devices for currently established aggregate reservations. • The optional keywords and arguments display additional information.

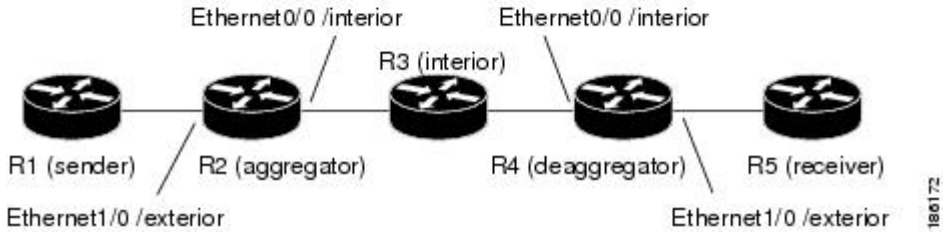
	Command or Action	Purpose
Step 4	**show ip rsvp** [**atm-peak-rate-limit**| **counters**| **host**| **installed**| **interface**| **listeners**| **neighbor**| **policy**| **precedence**| **request**| **reservation**| **sbm**| **sender**| **signalling**| **tos**] **Example:** Device# show ip rsvp	(Optional) Displays specific information for RSVP categories. • The optional keywords display additional information.
Step 5	**show ip rsvp reservation** [**detail**] [**filter**[**destination** *ip-address* | *hostname*] [**dst-port** *port-number*] [**source** *ip-address* | *hostname*][**src-port** *port-number*]] **Example:** Device# show ip rsvp reservation detail	(Optional) Displays RSVP-related receiver information currently in the database. • The optional keywords and arguments display additional information. **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-address* | *hostname*] [**dst-port** *port-number*] [**source** *ip-address* | *hostname*][**src-port** *port-number*]] **Example:** Device# show ip rsvp sender detail	(Optional) Displays RSVP PATH-related sender information currently in the database. • The optional keywords and arguments display additional information. **Note** The optional **filter** keyword is supported in Cisco IOS Releases 12.0S and 12.2S only.
Step 7	**show ip rsvp installed** [*interface-type interface-number*] [**detail**] **Example:** Device# show ip rsvp installed detail	(Optional) Displays RSVP-related installed filters and corresponding bandwidth information. • The optional keywords and arguments display additional information.
Step 8	**show ip rsvp interface** [**detail**] [*interface-type interface-number*] **Example:** Device# show ip rsvp interface detail	(Optional) Displays RSVP-related interface information. • The optional keywords and arguments display additional information.
Step 9	**end** **Example:** Device# end	(Optional) Exits privileged EXEC mode and returns to user EXEC mode.

Configuration Examples for RSVP Aggregation

Examples Configuring RSVP Aggregation

The figure below shows a five-router network in which RSVP aggregation is configured.

Figure 2 Sample RSVP Aggregation Network



Configuring RSVP and DiffServ Attributes on an Interior Router

The following example configures RSVP/DiffServ attributes on an interior router (R3 in the figure above).

- GigabitEthernet interface 0/0/0 is enabled for RSVP and the amount of bandwidth available for reservations is configured.
- A resource provider is configured and data packet classification is disabled because RSVP aggregation supports control plane aggregation only.

Router# **configure terminal**

```
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface GigabitEthernet 0/0/0

Router(config-if)# ip rsvp bandwidth 400

Router(config-if)# ip rsvp resource-provider none

Router(config-if)# ip rsvp data-packet classification none

Router(config-if)# end
```

Configuring RSVP Aggregation on an Aggregator or Deaggregator

The following example configures RSVP aggregation attributes on an aggregator or deaggregator (R2 and R4 in the figure above):

- Loopback 1 is configured to establish an RSVP aggregation router ID.
- Ethernet interface 0/0 is enabled for RSVP and the amount of bandwidth available for reservations is configured.
- Ethernet interface 0/0 on an aggregator or deaggregator is configured to face an aggregation region.
- A resource provider is configured and data packet classification is disabled because RSVP aggregation supports control plane aggregation only.

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface Loopback 1
Router(config)# ip address 192.168.50.1 255.255.255.0
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# ip rsvp bandwidth 400
Router(config-if)# ip rsvp aggregation role interior
Router(config-if)# ip rsvp resource-provider none
Router(config-if)# ip rsvp data-packet classification none
Router(config-if)# end
```

Configuring RSVP Aggregation Attributes and Parameters

The following example configures additional RSVP aggregation attributes, including a global rule for mapping all E2E reservations onto a single aggregate with DSCP AF41 and the token bucket parameters for aggregate reservations, because dynamic resizing is not supported. This configuration is only required on nodes performing the deaggregation function (R4 in the figure above).

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# ip rsvp aggregation ip map any dscp af41

Router(config)# ip rsvp aggregation ip reservation dscp af41 aggregator 10.10.10.10 traffic-params static
rate 10 burst 8 peak 10

Router(config)# end
```

Configuring an Access List for a Deaggregator

In the following example, access list 1 is defined for all RSVP messages whose RSVP PATH message sender template source address is in the 10.1.0.0 subnet so that the deaggregator (R4 in the figure above) maps those reservations onto an aggregate reservation for the DSCP associated with the AF41 PHB:

```
Router# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)# access-list 1 permit 10.1.0.0 0.0.255.255

Router(config)# ip rsvp aggregation ip map access-list 1 dscp af41

Router(config)# end
```

Configuring RSVP Aggregation

After you configure your RSVP aggregation attributes, you are ready to enable aggregation globally.

When you enable aggregation on a router, the router can act as an aggregator or a deaggregator. To perform aggregator and deaggregator functions, the RSVP process must see messages with the RSVP-E2E-IGNORE protocol type (134) on a router; otherwise, the messages are forwarded as data by the router's data plane. The **ip rsvp aggregation ip** command enables RSVP to identify messages with the RSVP-E2E-IGNORE protocol.

Note This registers a router to receive RSVP-E2E-IGNORE messages. It is not necessary to configure this command on interior nodes that are only processing RSVP aggregate reservations and forwarding RSVP-E2E-IGNORE messages as IP datagrams). Since the router is loaded with an image that supports aggregation, the router will process aggregate (RFC 3175 formatted) messages correctly. Enabling aggregation on an interior mode may decrease performance because the interior node will then unnecessarily process all RSVP-E2E-IGNORE messages.

Note If you enable aggregation on an interior node, you must configure all its interfaces as interior. Otherwise, all the interfaces have the exterior role, and any E2E PATH (E2E-IGNORE) messages arriving at the router are discarded.

In summary, there are two options for an interior router (R3 in the figure above):

- No RSVP aggregation configuration commands are entered.
- RSVP aggregation is enabled and all interfaces are configured as interior.

Configuring RSVP Local Policy

You can configure a local policy optionally on any RSVP capable node. In this example, a local policy is configured on a deaggregator to set the preemption priority values within the RSVP RESV aggregate messages based upon matching the DSCP within the aggregate RSVP messages session object. This allows the bandwidth available for RSVP reservations to be used first by reservations of DSCP EF over DSCP AF41 on interior or aggregation nodes. Any aggregate reservation for another DSCP will have a preemption priority of 0, the default.

Note Within the RSVP RESV aggregate message at the deaggregator, this local policy sets an RFC 3181 "Signaled Preemption Priority Policy Element" that can be used by interior nodes or the aggregator that has **ip rsvp preemption** enabled.

The following example sets the preemption priority locally for RSVP aggregate reservations during establishment on an interior router (R3 in the figure above):

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip rsvp policy local dscp-ip ef
Router(config-rsvp-local-policy)# 5 5
Router(config-rsvp-local-policy)# exit
Router(config)# ip rsvp policy local dscp-ip af41
Router(config-rsvp-local-policy)# 2 2
Router(config-rsvp-local-policy)# end
```

Example Verifying the RSVP Aggregation Configuration

Verifying RSVP Aggregation and Configured Reservations

The following example verifies that RSVP aggregation is enabled and displays information about the reservations currently established and configured map and reservation policies:

```
Router# show ip rsvp aggregation ip
RFC 3175 Aggregation:  Enabled
  Level: 1
  Default QoS service: Controlled-Load
  Number of signaled aggregate reservations:  2
  Number of signaled E2E reservations:        8
  Number of configured map commands:          4
  Number of configured reservation commands:  1
```

Verifying Configured Interfaces and Their Roles

The following example displays the configured interfaces and whether they are interior or exterior in regard to the aggregation region:

```
Router# show ip rsvp aggregation ip interface
Interface Name      Role
------------------- --------
Ethernet0/0         interior
Serial2/0           exterior
Serial3/0           exterior
```

Verifying Aggregator and Deaggregator Reservations

The following example displays information about the aggregators and deaggregators when established reservations are present:

```
Router# show ip rsvp aggregation ip endpoints detail
Role  DSCP Aggregator      Deaggregator    State  Rate    Used    QBM PoolID
----- ---- --------------- --------------- ------ ------- ------- ----------
Agg   46   10.3.3.3         10.4.4.4        ESTABL 100K    100K    0x00000003
  Aggregate Reservation for the following E2E Flows (PSBs):
To            From          Pro DPort Sport  Prev Hop       I/F      BPS
10.4.4.4      10.1.1.1      UDP 1     1      10.23.20.3     Et1/0    100K
  Aggregate Reservation for the following E2E Flows (RSBs):
To            From          Pro DPort Sport  Next Hop       I/F      Fi Serv BPS
10.4.4.4      10.1.1.1      UDP 1     1      10.4.4.4       Se2/0    FF RATE 100K
  Aggregate Reservation for the following E2E Flows (Reqs):
To            From          Pro DPort Sport  Next Hop       I/F      Fi Serv BPS
10.4.4.4      10.1.1.1      UDP 1     1      10.23.20.3     Et1/0    FF RATE 100K
```

Additional References

The following sections provide references related to the RSVP Aggregation feature.

Related Documents

Related Topic	Document Title
RSVP commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
QoS features including signaling, classification, and congestion management	"Quality of Service Overview" module
Information on RSVP local policies	"RSVP Local Policy Support" module
Information on RSVP scalability enhancements	"RSVP Scalability Enhancements" 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, software 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)--Version 1 Functional Specification*
RFC 2209	*Resource ReSerVation Protocol (RSVP)--Version 1 Message Processing Rules*
RFC 3175	*Aggregation of RSVP for IPv4 and IPv6 Reservations*
RFC 3181	*Signaled Preemption Priority Policy Element*
RFC 4804	Aggregation of Resource ReSerVation Protocol (RSVP) Reservations over MPLS TE/DS-TE Tunnels

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for RSVP Aggregation

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 1 Feature Information for RSVP Aggregation

Feature Name	Releases	Feature Information
RSVP Aggregation	Cico IOS XE Release 2.6 Cisco IOS XE Release 3.8S	The RSVP Aggregation feature allows the Resource Reservation Protocol (RSVP) state to be reduced within an RSVP/DiffServ network by aggregating many smaller reservations into a single, larger reservation at the edge. The following commands were introduced or modified: **debug ip rsvp aggregation**, **debug qbm**, **ip rsvp aggregation ip**, **ip rsvp aggregation ip map**, **ip rsvp aggregation**, **ip reservation dscp traffic-params static rate**, **ip rsvp aggregation ip role interior**, **ip rsvp policy local**, **show ip rsvp**, **show ip rsvp aggregation ip**, **show ip rsvp aggregation ip endpoints**, **show ip rsvp installed**, **show ip rsvp interface**, **show ip rsvp policy local**, **show ip rsvp request**, **show ip rsvp reservation**, **show ip rsvp sender**, **show qbm client**, **show qbm pool**. In Cisco IOS XE Release 3.8S, support was added for the Cisco ASR 903 Router.

Glossary

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

aggregate --AnRSVP flow that represents multiple end-to-end (E2E) flows; for example, a Multiprotocol Label Switching Traffic Engineering (MPLS-TE) tunnel may be an aggregate for many E2E flows.

aggregation region --An area where E2E flows are represented by aggregate flows, with aggregators and deaggregators at the edge; for example, an MPLS-TE core, where TE tunnels are aggregates for E2E flows. An aggregation region contains a connected set of nodes that are capable of performing RSVP aggregation.

aggregator --The device that processes the E2E PATH message as it enters the aggregation region. This device is also called the TE tunnel head-end device; it forwards the message from an exterior interface to an interior interface.

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

deaggregator --The device that processes the E2E PATH message as it leaves the aggregation region. This device is also called the TE tunnel tail-end device; it forwards the message from an interior interface to an exterior interface.

E2E --end-to-end. An RSVP flow that crosses an aggregation region, and whose state is represented in aggregate within this region, such as a classic RSVP unicast flow crossing an MPLS-TE core.

LSP --label-switched path. A configured connection between two devices, in which label switching is used to carry the packets. The purpose of an LSP is to carry data packets.

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 that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams that they want to receive.

state --Information that a device must maintain about each LSP. The information is used for rerouting tunnels.

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.

tunnel --Secure communications path between two peers, such as two devices.

RSVP Application ID Support

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

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for RSVP Application ID Support

You must configure Resource Reservation Protocol (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

Feature Overview of RSVP Application ID Support

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 (Internet Engineering Task Force (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 the introduction of the RSVP Application ID Support feature, provision was made to create Access Control Lists (ACLs) that matched 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

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

CUCM uses the RSVP Application ID Support feature. In this example, when CUCM makes the RSVP reservation, CUCM can specify whether the reservation should be made against a video RSVP bandwidth pool or a voice RSVP bandwidth pool. If not enough bandwidth remains in the requested pool, even though there is enough bandwidth in the total RSVP allocation, RSVP signals CUCM that there is a problem with the reservation. The figure below shows some of the signaling and data traffic that is sent during the session setup.

IMAGE MISSING; embedded not referenced

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. While setting up the voice or video session, CUCM 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 CUCM. CUCM 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 communicate to CUCM that the reservation has been made. CUCM 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 CUCM, 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 informs 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; that is, the 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, use 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, page 36
- Controlling Preemption, page 36

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 device 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 device and forwarded to neighbors.

Controlling Preemption

The **ip rsvp policy preempt** command controls whether 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 CUCM to provide a solution for call admission control (CAC) and QoS for VoIP and video conferencing applications in networks with multitiered, meshed topologies using signaling protocols such as Signaling Connection Control Part (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 CUCM or to use with non-RSVP-aware applications such as static PATH and RESV messages.

Configuring RSVP Application ID for RSVP-Aware Software Programs

Configuring an RSVP 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 ? character. 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.
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, page 38

What to Do Next

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

Configuring a Local Policy Globally

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp policy local** {**acl** *acl1*[*acl2...acl8*] | **dscp-ip** *value1*[*value2...value8*]| **default** | **identity** *alias1* [*alias2...alias4*] | **origin-as** *as1*[*as2...as8*]}
4. Repeat Step 3 as needed to configure additional local policies.
5. Enter the submode commands as required.
6. **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*] | **dscp-ip** *value1*[*value2...value8*]| **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	Enter the submode commands as required.	(Optional) Defines the properties of the local policy that you are creating. **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 detailed information on submode commands.
Step 6	**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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *subslot* / *port*
4. Repeat Step 3 as needed to configure a local policy on additional interfaces.
5. **ip rsvp bandwidth** [*interface-kbps* [*single-flow-kbps*[**bc1** *kbps* | **sub-pool** *kbps*]*]*| **percent** *percent-bandwidth* [*single-flow-kbps*]]
6. Repeat Step 5 as needed to configure bandwidth for additional interfaces.
7. **ip rsvp policy local** {**acl** *acl1*[*acl2...acl8*] | **dscp-ip** *value1*[*value2...value8*]| **default** | **identity** *alias1* [*alias2...alias4*] | **origin-as** *as1*[*as2...as8*]}
8. Repeat Step 7 as needed to configure additional local policies.
9. Enter the submode commands as required.
10. **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 slot* / *subslot* / *port* **Example:** Router(config)# interface gigabitEthernet 0/0/0	Configures the interface type and number and enters interface configuration mode.
Step 4	Repeat Step 3 as needed to configure a local policy on additional interfaces.	(Optional) Configures additional interfaces.
Step 5	**ip rsvp bandwidth** [*interface-kbps* [*single-flow-kbps*[**bc1** *kbps* | **sub-pool** *kbps*]*]*| **percent** *percent-bandwidth* [*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 1000000.

	Command or Action	Purpose
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** *acl1*[*acl2...acl8*] | **dscp-ip** *value1*[*value2...value8*]| **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	Enter the submode commands as required.	(Optional) Defines the properties of the local policy that you are creating and enters local policy configuration mode. **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 detailed information on submode commands.
Step 10	**end** **Example:** Router(config-rsvp-policy-local)# end	Exits local policy configuration mode and returns to privileged EXEC mode.

Configuring RSVP Application ID for Non-RSVP-Aware Software Programs

Configuring an Application ID

Refer to the Configuring an RSVP Application ID, page 37.

Configuring a Static RSVP 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 sende r-host** *session-ip-address sender-ip-address* {*ip-protocol* |**tcp** | **udp**} *session-dest-port sender-source-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 sende r-host** *session-ip-address sender-ip-address* {*ip-protocol* |**tcp**	**udp**} *session-dest-port sender-source-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 ? character as part of the alias string itself, you must type the CTRL-V key sequence before entering the embedded " " or ? character. 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 RSVP 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, page 52for more information.

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.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - **ip rsvp reservation-host** *session-ip-address sender-ip-address* {*ip-protocol*| **tcp** | **udp**} *session-dest-port sender-source-port*{**ff** | **se** | **wf**}{**load** | **rate**} *bandwidth burst-size*[**identity** *alias*]
   -
   - **ip rsvp reservation** *session-ip-address sender-ip-address* {*ip-protocol* | **tcp** | **udp**} *session-dest-port sender-source-port next-hop-ip-address next-hop-interface*{**ff** | **se** | **wf**}{**load** | **rate**} *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.

	Command or Action	Purpose
Step 3	Do one of the following: • **ip rsvp reservation-host** *session-ip-address sender-ip-address* {*ip-protocol*| **tcp** | **udp**} *session-dest-port sender-source-port*{**ff** | **se** | **wf**} {**load** | **rate**} *bandwidth burst-size*[**identity** *alias*] • • **ip rsvp reservation** *session-ip-address sender-ip-address* {*ip-protocol* | **tcp** | **udp**} *session-dest-port sender-source-port next-hop-ip-address next-hop-interface*{**ff** | **se** | **wf**} {**load** | **rate**} *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 **Example:** **Example:** 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 ? character as part of the alias string itself, you must type the CTRL-V key sequence before entering the embedded " " or ? character. 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

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

SUMMARY STEPS

1. **enable**
2. **show ip rsvp host** {**receivers**| **senders**}[*hostname* | *group-address*]
3. **show ip rsvp policy identity** [*regular-expression*]
4. **show ip rsvp policy local** [**detail**] [**interface** *type slot* / *subslot* / *port*] [**acl** *acl-number*| **dscp-ip** *value*| **default** | **identity** *alias* | **origin-as** *as*]
5. **show ip rsvp reservation** [**detail**] [**filter** [**destination** *address*] [**dst-port** *port-number*] [**source** *address*] [**src-port** *port-number*]]
6. **show ip rsvp sender** [**detail**] [**filter** [**destination** *address*] [**dst-port** *port-number*] [**source** *address*] [**src-port** *port-number*]]
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** {**receivers**	**senders**}[*hostname*	*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.
Step 4	**show ip rsvp policy local** [**detail**] [**interface** *type slot* / *subslot* / *port*] [**acl** *acl-number*| **dscp-ip** *value*| **default**	**identity** *alias*	**origin-as** *as*] **Example:** Router# show ip rsvp policy local identity voice100	Displays the local policies currently configured. • The optional **detail** keyword and the optional **interface** *type slot* / *subslot* / *port* keyword and argument combination can be used with any of the match criteria.

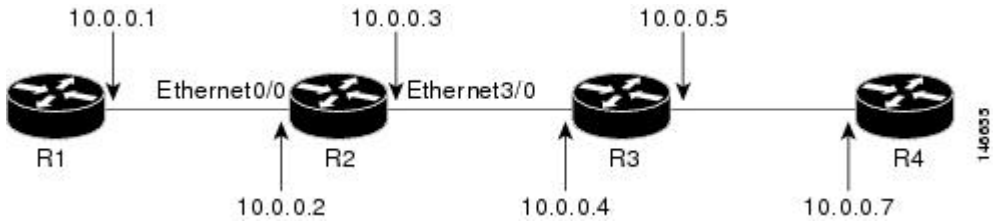
	Command or Action	Purpose
Step 5	**show ip rsvp reservation** [**detail**] [**filter** [**destination** *address*] [**dst-port** *port-number*] [**source** *address*] [**src-port** *port-number*]] **Example:** Router# show ip rsvp reservation detail	Displays RSVP-related receiver information currently in the database. • The optional **detail** keyword displays additional output with information about where the policy originated and which application ID was signaled in the RESV message.
Step 6	**show ip rsvp sender** [**detail**] [**filter** [**destination** *address*] [**dst-port** *port-number*] [**source** *address*] [**src-port** *port-number*]] **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.
Step 7	**end** **Example:** Router# end	Exits privileged EXEC mode and returns to user EXEC mode.

Configuration Examples for RSVP Application ID Support

Example Configuring RSVP Application ID Support

The configurations for four-router network shown in the figure below are in the following sections:

Figure 3 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:

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

Device(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:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip rsvp policy identity video policy-locator video
Device(config)# ip rsvp policy local identity video
Device(config-rsvp-policy-local)# forward all
Device(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 Gigabit Ethernet interface 0/0/0:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitEthernet 0/0/0
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 Gigabit Ethernet interface 3/0/0:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitEthernet 3/0/0
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 Gigabit Ethernet interface 0/0/0 and RESV messages arrive on egress Gigabit Ethernet interface 3/0/0.

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:

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

Example Verifying RSVP Application ID Support

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 Gigabit Ethernet interface 0/0/0 and Gigabit Ethernet interface 3/0/0 on R2:

```
Router# show ip rsvp policy local detail
gigabitEthernet 0/0/0:
  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

giabitEthernet 3/0/0:
  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 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 gigabitEthernet 0/0/0. Policy status: Forwarding. Handle: 01000403
    Policy source(s): Default
```

Note You can use 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 gigabitEthernet 0/0/0
  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
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

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 United 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 XE software 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 and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for RSVP Application ID Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 2 Feature Information for RSVP Application ID Support

Feature Name	Releases	Feature Information
RSVP Application ID Support	Cisco IOS XE Release 2.6 Cisco IOS XE Release 3.8S	The RSVP Application ID Support feature introduces application-specific reservations, which enhance the granularity for local policy-match criteria so that you can manage QoS on the basis of application type. The following commands were introduced 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**. In Cisco IOS XE Release 3.8S, support was added for the Cisco ASR 903 Router.

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.

CUCM--Cisco Unified Communications Manager. 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 Unified Communications Manager.

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.

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

RSVP Fast Local Repair

The RSVP Fast Local Repair feature provides quick adaptation to routing changes occurring in global and Virtual Routing and Forwarding (VRF) domains, without the overhead of the refresh period to guarantee the quality of service (QoS) for data flows. With fast local repair (FLR), Resource Reservation Protocol (RSVP) speeds up its response to routing changes from 30 seconds to a few seconds.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for RSVP FLR

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

Restrictions for RSVP FLR

- RSVP FLR applies only when RSVP is used to set up resource reservations for IPv4 unicast flows; IPv4 multicast flows are not supported.

- RSVP FLR does not apply to traffic engineering (TE) tunnels and, therefore, does not affect TE sessions.
- RSVP FLR does not support message bundling.

Information About RSVP FLR

Feature Overview of RSVP FLR

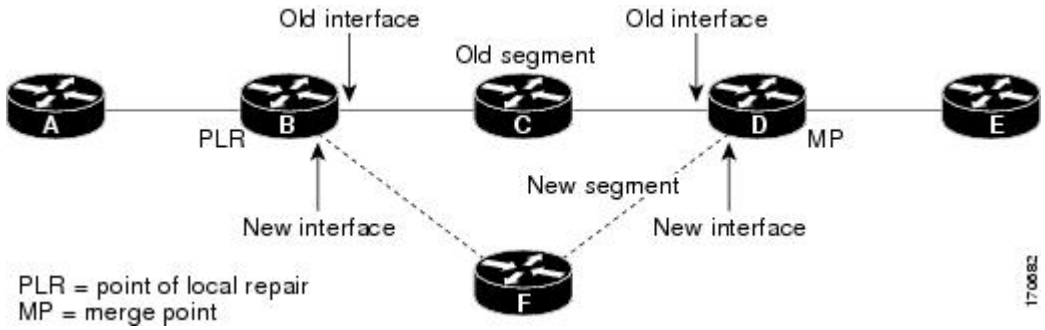
RSVP FLR provides for dynamic adaptation when routing changes occur in global or VRF routing domains. When a route changes, the next PATH and RESV message refreshes establish path and reservation states along the new route. Depending on the configured refresh interval, this reroute happens in tens of seconds. However, during this time, the QoS of flows is not guaranteed because congestion may occur while data packets travel over links where reservations are not yet in place.

In order to provide faster adaptation to routing changes, without the overhead of a refresh period, RSVP registers with the Routing Information Base (RIB) and receives notifications when routes change, thereby triggering state refreshes for the affected destinations. These triggered refreshes use the new route information and, as a result, install reservations over the new path.

When routes change, RSVP has to reroute all affected paths and reservations. Without FLR, the reroute happens when refresh timers expire for the path states. With real-time applications such as VoIP and video on demand (VoD), the requirement changes and the reroute must happen, within three seconds from the triggering event such as link down or link up.

The figure below illustrates the FLR process.

Figure 4 Overview of RSVP FLR



Initial RSVP states are installed for an IPv4 unicast flow over Routers A, B, C, D, and E. Router A is the source or headend, and Router E is the destination or tailend. The data packets are destined to an address of Router E. Assume that a route change occurs, and the new path taken by the data packets is from Router A to Router B to Router F to Router D to Router E; therefore, the old and new paths differ on the segments between Routers B and D. The Router B to Router C to Router D segment is the old segment, and the Router B to Router F to Router D segment is the new segment.

A route may change because of a link or node failure, or if a better path becomes available.

RSVP at Router B detects that the route change affects the RSVP flow and initiates the FLR procedure. The node that initiates an FLR repair procedure, Router B in the figure above, is the point of local repair (PLR).

The node where the new and old segments meet, Router D in the figure above, is the merge point (MP). The interfaces at the PLR and the MP that are part of the old segment are the old interfaces, and the interfaces that are part of the new segment are the new interfaces.

If a route has changed because of a failure, the PLR may not be the node that detects the failure. For example, it is possible that the link from Router C to Router D fails, and although Router C detects the failure, the route change at Router B is the trigger for the FLR procedure. Router C, in this case, is also referred to as the node that detects the failure.

The support for FLR in VRF domains means that RSVP can get a route change notification, even if there is a route change in any VRF domains, because RSVP FLR was previously supported only in the global routing domain.

Benefits of RSVP FLR

Faster Response Time to Routing Changes

FLR reduces the time that it takes for RSVP to determine that a physical link has gone down and that the data packets have been rerouted. Without FLR, RSVP may not recognize the link failure for 30 seconds when all of the sessions are impacted by having too much traffic for the available bandwidth. With FLR, this time can be significantly reduced to a few seconds.

After detecting the failure, RSVP recomputes the admission control across the new link. If the rerouted traffic fits on the new link, RSVP reserves the bandwidth and guarantees the QoS of the new traffic.

If admission control fails on the new route, RSVP does not explicate tear down the flow, but instead sends a RESVERROR message toward the receiver. If a proxy receiver is running, then RSVP sends a PATHERROR message toward the headend, in response to the RESVERROR message, indicating the admission failure. In both cases, with and without a proxy receiver, the application tears down the failed session either at the headend or at the final destination.

Until this happens, the data packets belonging to this session still flow over the rerouted segment although admission has failed and QoS is affected.

The support of FLR in VRF domains means that if there is a route change in any routing domain, RSVP can use FLR to adapt to the routing change, because RSVP FLR was previously supported only in the global routing domain.

How to Configure RSVP FLR

You can configure the RSVP FLR parameters in any order that you want.

- Configuring the RSVP FLR Wait Time, page 58
- Configuring the RSVP FLR Repair Rate, page 59
- Configuring the RSVP FLR Notifications, page 60
- Verifying the RSVP FLR Configuration, page 61

Configuring the RSVP FLR Wait Time

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *subslot* / *port*
4. **ip rsvp bandwidth** [*interface-kbps* [*single-flow-kbps*[**bc1** *kbps* | **sub-pool** *kbps*]/| **percent** *percent-bandwidth* [*single-flow-kbps*]]
5. **ip rsvp signalling fast-local-repair wait-time** *interval*
6. **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 slot* / *subslot* / *port* **Example:** Router(config)# interface gigabitEthernet 0/0/0	Configures the interface type and enters interface configuration mode.
Step 4	**ip rsvp bandwidth** [*interface-kbps* [*single-flow-kbps*[**bc1** *kbps* | **sub-pool** *kbps*]/| **percent** *percent-bandwidth* [*single-flow-kbps*]] **Example:** Router(config-if)# ip rsvp bandwidth 7500 7500	Enables RSVP on an interface. • The optional *interface-kbps* and *single-flow-kbps* arguments specify the amount of bandwidth that can be allocated by RSVP flows or to a single flow, respectively. Values are from 1 to 10000000. • The optional **sub-pool**and *kbps*keyword and argument specify subpool traffic and the amount of bandwidth that can be allocated by RSVP flows. Values are from 1 to 10000000. **Note** Repeat this command for each interface on which you want to enable RSVP.

	Command or Action	Purpose
Step 5	**ip rsvp signalling fast-local-repair wait-time** *interval* **Example:** Router(config-if)# **ip rsvp signalling fast-local-repair wait-time 100**	Configures the delay that RSVP uses before starting an FLR procedure. • Values for the *interval* argument are 1 to 2500 milliseconds (ms); the default is 0.
Step 6	**end** **Example:** Router(config-if)# **end**	(Optional) Returns to privileged EXEC mode.

Configuring the RSVP FLR Repair Rate

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp signalling fast-local-repair rate** rate
4. **exit**

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 signalling fast-local-repair rate** rate **Example:** Router(config)# **ip rsvp signalling fast-local-repair rate 100**	Configures the repair rate that RSVP uses for an FLR procedure. • Values for the *rate* argument are 1 to 2500 messages per second; the default is 400.
Step 4	**exit** **Example:** Router(config)# **exit**	(Optional) Returns to privileged EXEC mode.

Configuring the RSVP FLR Notifications

Perform this task to configure the number of RSVP FLR notifications.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp signalling fast-local-repair notifications** *number*
4. **exit**

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 signalling fast-local-repair notifications** *number* **Example:** Router(config)# **ip rsvp signalling fast-local-repair notifications 100**	Configures the number of per flow notifications that RSVP processes during an FLR procedure before it suspends. • Values for the *number*argument are 10 to 10000; the default is 1000.
Step 4	**exit** **Example:** Router(config)# **exit**	(Optional) Returns to privileged EXEC mode.

Verifying the RSVP FLR Configuration

Perform this task to verify the RSVP FLR configuration. You can use these commands in any order.

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

SUMMARY STEPS

1. **enable**
2. **show ip rsvp signalling fast-local-repair** [**statistics** [**detail**]]
3. **show ip rsvp interface** [**detail**] [*interface-type interface-number*]
4. **show ip rsvp**
5. **show ip rsvp sender** [**detail**] [**filter** [**destination** *ip-address* | *hostname*] [**dst-port** *port-number*] [**source** *ip-address* | *hostname*] [**src-port** *port-number*]]
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	(Optional) Enables privileged EXEC mode. • Enter your password if prompted. **Note** Omit this step if you are using the **show** commands in user EXEC mode.

	Command or Action	Purpose
Step 2	**show ip rsvp signalling fast-local-repair** [**statistics** [**detail**]] **Example:** Router# show ip rsvp signalling fast-local-repair statistics detail	Displays FLR-specific information that RSVP maintains. • The optional **statistics** and **detail** keywords display additional information about the FLR parameters.
Step 3	**show ip rsvp interface** [**detail**] [*interface-type interface-number*] **Example:** Router# show ip rsvp interface gigabit**ethernet 0/0/0**	Displays RSVP-related information. • The optional **detail** keyword displays additional information including FLR parameters.
Step 4	**show ip rsvp** **Example:** Router# show ip rsvp	Displays general RSVP-related information.
Step 5	**show ip rsvp sender** [**detail**] [**filter** [**destination** *ip-address* | *hostname*] [**dst-port** *port-number*] [**source** *ip-address* | *hostname*] [**src-port** *port-number*]] **Example:** Router# show ip rsvp sender detail	Displays RSVP PATH-related sender information currently in the database. • The optional **detail** keyword displays additional output including the FLR parameters.
Step 6	**exit** **Example:** Router# exit	(Optional) Exits privileged EXEC mode and returns to user EXEC mode.

Configuration Examples for RSVP FLR

Example Configuring RSVP FLR

The configuration options for RSVP FLR are the following:

- Wait time

- Number of notifications
- Repair rate

Note You can configure these options in any order.

Configuring the Wait Time

The following example configures gigabitEthernet interface 0/0/0 with a bandwidth of 200 kbps and a wait time of 1000 ms:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# ip rsvp bandwidth 200
Router(config-if)# ip rsvp signalling fast-local-repair wait-time 1000
Router(config-if)# end
```

Configuring the Number of Notifications

The following example configures the number of flows that are repaired before suspending to 100:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip rsvp signalling fast-local-repair notifications 100
Router(config)# exit
```

Configuring the Repair Rate

The following example configures a repair rate of 100 messages per second:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip rsvp signalling fast-local-repair rate 100
Router(config)# exit
```

Example Verifying the RSVP FLR Configuration

Verifying the Details for FLR Procedures

The following example displays detailed information about FLR procedures:

```
Router# show ip rsvp signalling fast-local-repair statistics detail
Fast Local Repair: enabled
  Max repair rate (paths/sec): 10
  Max processed   (paths/run): 10
FLR Statistics:
  FLR 1: DONE
    Start Time: 05:18:54 IST Mon Nov 5 2007
    Number of PSBs repaired:          2
    Used Repair Rate (msgs/sec):      10
    RIB notification processing time: 0(us).
    Time of last PSB refresh:         5025(ms).
```

```
Time of last Resv received:      6086(ms).
Time of last Perr received:      0(us).
Suspend count: 0
FLR Pacing Unit: 100 msec.
Affected neighbors:
  Nbr Address   Interface    Relative Delay Values (msec)      VRF
  10.1.2.12     Et0/3        [5000  ,..., 5000  ]      vrf1
  10.1.2.12     Et1/3        [5000  ,..., 5000  ]      vrf2
```

Verifying Configuration Details for a Specific Interface

The following example from the **show ip rsvp interface detail** command displays detailed information, including FLR, for the gigabitEthernet 0/0/0 interface:

```
Router# show ip rsvp interface detail gigabitethernet 0/0/0
 Et1/0:
   RSVP: Enabled
   Interface State: Up
   Bandwidth:
     Curr allocated: 9K bits/sec
     Max. allowed (total): 300K bits/sec
     Max. allowed (per flow): 300K bits/sec
     Max. allowed for LSP tunnels using sub-pools (pool 1): 0 bits/sec
     Set aside by policy (total): 0 bits/sec
   Traffic Control:
     RSVP Data Packet Classification is ON via CEF callbacks
   Signalling:
     DSCP value used in RSVP msgs: 0x30
     Number of refresh intervals to enforce blockade state: 4
   FLR Wait Time (IPv4 flows):
     Repair is delayed by 1000 msec.
   Authentication: disabled
     Key chain:   <none>
     Type:        md5
     Window size: 1
     Challenge:   disabled
   Hello Extension:
     State: Disabled
```

Verifying Configuration Details Before During and After an FLR Procedure

The following is sample output from the **showiprsvpsenderdetail** command before an FLR procedure has occurred:

```
Router# show ip rsvp sender detail
PATH:
  Destination 192.168.101.21, Protocol_Id 17, Don't Police , DstPort 1
  Sender address: 10.10.10.10, port: 1
  Path refreshes:
    arriving: from PHOP 172.3.31.34 on Et0/0 every 30000 msecs
  Traffic params - Rate: 9K bits/sec, Max. burst: 9K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
  Path ID handle: 01000401.
  Incoming policy: Accepted. Policy source(s): Default
  Status:
  Output on gigabitEthernet 0/0/0. Policy status: Forwarding. Handle: 02000400
    Policy source(s): Default
  Path FLR: Never repaired
```

The following is sample output from the **showiprsvpsenderdetail** command at the PLR during an FLR procedure:

```
Router# show ip rsvp sender detail
PATH:
  Destination 192.168.101.21, Protocol_Id 17, Don't Police , DstPort 1
  Sender address: 10.10.10.10, port: 1
```

```
  Path refreshes:
    arriving: from PHOP 172.16.31.34 on Et0/0 every 30000 msecs
  Traffic params - Rate: 9K bits/sec, Max. burst: 9K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
  Path ID handle: 01000401.
  Incoming policy: Accepted. Policy source(s): Default
  Status:
  Path FLR: PSB is currently being repaired...try later
  PLR - Old Segments: 1
   Output on Ethernet1/0, nhop 172.5.36.34
   Time before expiry: 2 refreshes
   Policy status: Forwarding. Handle: 02000400
     Policy source(s): Default
```

The following is sample output from the **showiprsvpsenderdetail** command at the MP during an FLR procedure:

```
Router# show ip rsvp sender detail
PATH:
  Destination 192.168.101.21, Protocol_Id 17, Don't Police , DstPort 1
  Sender address: 10.10.10.10, port: 1
  Path refreshes:
    arriving: from PHOP 172.16.37.35 on Et1/0 every 30000 msecs
Traffic params - Rate: 9K bits/sec, Max. burst: 9K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
  Path ID handle: 09000406.
  Incoming policy: Accepted. Policy source(s): Default
  Status: Proxy-terminated
  Path FLR: Never repaired
  MP - Old Segments: 1
   Input on Serial2/0, phop 172.16.36.35
   Time before expiry: 9 refreshes
```

The following is sample output from the **showiprsvpsenderdetail** command at the PLR after an FLR procedure:

```
Router# show ip rsvp sender detail
PATH:
  Destination 192.168.101.21, Protocol_Id 17, Don't Police , DstPort 1
  Sender address: 10.10.10.10, port: 1
  Path refreshes:
    arriving: from PHOP 172.16.31.34 on Et0/0 every 30000 msecs
  Traffic params - Rate: 9K bits/sec, Max. burst: 9K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
  Path ID handle: 05000401.
  Incoming policy: Accepted. Policy source(s): Default
  Status:
  Output on Serial3/0. Policy status: Forwarding. Handle: 3B000406
    Policy source(s): Default
  Path FLR: Started 12:56:16 EST Thu Nov 16 2006, PSB repaired 532(ms) after.
        Resv/Perr: Received 992(ms) after.
```

Additional References

The following sections provide references related to the RSVP FLR feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Related Topic	Document Title
RSVP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
QoS features including signaling, classification, and congestion management	"Quality of Service Overview" 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 software 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--Version 1 Functional Specification*
RFC 2209	*Resource ReSerVation Protocol--Version 1 Messaging Processing Rules*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for RSVP FLR

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 3 Feature Information for RSVP FLR

Feature Name	Releases	Feature Information
RSVP Fast Local Repair	Cisco IOS XE Release 2.6 Cisco IOS XE Release 3.8S	The RSVP Fast Local Repair feature provides quick adaptation to routing changes without the overhead of the refresh period to guarantee QoS for data flows. With FLR, RSVP speeds up its response to routing changes from 30 seconds to a few seconds. The following commands were introduced or modified: **clear ip rsvp signalling fast-local-repair statistics**, **ip rsvp signalling fast-local-repair notifications**, **ip rsvp signalling fast-local-repair rate**, **ip rsvp signalling fast-local-repair wait-time**, **show ip rsvp**, **show ip rsvp interface**, **show ip rsvp sender**, **show ip rsvp signalling fast-local-repair**. In Cisco IOS XE Release 3.8S, support was added for the Cisco ASR 903 Router.

Glossary

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

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

message pacing-- A system for managing volume and timing that permits messages from multiple sources to be spaced apart over time. RSVP message pacing maintains, on an outgoing basis, a count of the messages that it has been forced to drop because the output queue for the interface used for the message pacing was full.

MP --merge point. The node where the new and old FLR segments meet.

PLR --point of local repair. The node that initiates an FLR procedure.

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 that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams that they want to receive.

VRF--virtual routing and forwarding. VRF is a VPN routing and forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.

RSVP Interface-Based Receiver Proxy

The RSVP Interface-Based Receiver Proxy feature lets you configure a proxy router by outbound interface instead of configuring a destination address for each flow going through the same interface.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for RSVP Interface-Based Receiver Proxy

You must configure an IP address and enable Resource Reservation Protocol (RSVP) on one or more interfaces on at least two neighboring routers that share a link within the network.

Restrictions for RSVP Interface-Based Receiver Proxy

- Filtering using access control lists (ACLs), application IDs, or other mechanisms is not supported.
- A provider edge (PE) router cannot switch from being a proxy node to a transit node for a given flow during the lifetime of the flow.

Information About RSVP Interface-Based Receiver Proxy

Feature Overview of RSVP Interface-Based Receiver Proxy

The RSVP Interface-Based Receiver Proxy feature allows you to use RSVP to signal reservations and guarantee bandwidth on behalf of a receiver that does not support RSVP by terminating the PATH message and generating a RESV message in the upstream direction on an RSVP-capable router on the path to the endpoint. An example is a video-on-demand flow from a video server to a set-top box, which is a computer that acts as a receiver and decodes the incoming video signal from the video server.

Because set-top boxes may not support RSVP natively, you cannot configure end-to-end RSVP reservations between a video server and a set-top box. Instead, you can enable the RSVP interface-based receiver proxy on the router that is closest to that set-top box.

The router terminates the end-to-end sessions for many set-top boxes and performs admission control on the outbound (or egress) interface of the PATH message, where the receiver proxy is configured, as a proxy for Call Admission Control (CAC) on the router-to-set-top link. The RSVP interface-based receiver proxy determines which PATH messages to terminate by looking at the outbound interface to be used by the traffic flow.

You can configure an RSVP interface-based receiver proxy to terminate PATH messages going out a specified interface with a specific action (reply with RESV, or reject). The most common application is to configure the receiver proxy on the edge of an administrative domain on interdomain interfaces. The router then terminates PATH messages going out the administrative domain while still permitting PATH messages transitioning through the router within the same administrative domain to continue downstream.

The router terminates the end-to-end sessions for many set-top boxes, with the assumption that the links further downstream (for example, from the DSLAM to the set-top box) never become congested or, more likely, in the case of congestion, that the voice and video traffic from the router gets the highest priority and access to the bandwidth.

Benefits of RSVP Interface-Based Receiver Proxy

Before the RSVP Interface-Based Receiver Proxy feature was introduced, you had to configure a receiver proxy for every separate RSVP stream or set-top box. The RSVP Interface-Based Receiver Proxy feature allows you to configure the proxy by outbound interface. For example, if there were 100 set-top boxes downstream from the proxy router, you had to configure 100 proxies. With this enhancement, you configure only the outbound interfaces. In addition, the receiver proxy is guaranteed to terminate the reservation only on the last hop within the core network. Nodes that may function as transit nodes for some PATH messages but should proxy others depending on their placement in the network can perform the correct functions on a flow-by-flow basis.

How to Configure RSVP Interface-Based Receiver Proxy

- Verifying the RSVP Interface-Based Receiver Proxy Configuration, page 73

Enabling RSVP on an Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface type** *slot* / *subslot* / *port*
4. **ip rsvp bandwidth** [*interface-kbps* [*single-flow-kbps*[**bc1** *kbps* | **sub-pool** *kbps*]/| **percent** *percent-bandwidth* [*single-flow-kbps*]]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface type** *slot* / *subslot* / *port* **Example:** Router(config)# interface gigabitEthernet0/0/0	Configures the interface type and enters interface configuration mode.

Command or Action	Purpose
Step 4 **ip rsvp bandwidth** [*interface-kbps* [*single-flow-kbps*[**bc1** *kbps* | **sub-pool** *kbps*]*]*| **percent** *percent-bandwidth* [*single-flow-kbps*]]	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. Range is from 1 to 10000000. • The optional **sub-pool**and *sub-pool-kbps*keyword and argument specify subpool traffic and the amount of bandwidth that can be allocated by RSVP flows. Range is from 1 to 10000000. **Note** Repeat this command for each interface on which you want to enable RSVP.
Example: **Example:** **Example:** **Example:** **Example:** **Example:** **Example:** **Example:** **Example:** Router(config-if)# ip rsvp bandwidth 7500 7500	
Step 5 **end**	(Optional) Returns to privileged EXEC mode.
Example: Router(config-if)# **end**	

Configuring a Receiver Proxy on an Outbound Interface

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface type** *slot* / *subslot* / *port*
4. **ip rsvp listener outbound** {**reply** | **reject**}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface type** *slot* / *subslot* / *port* **Example:** Router(config)# interface gigabitEthernet 0/0/0	Configures the interface type and enters interface configuration mode.
Step 4	**ip rsvp listener outbound** {**reply**	**reject**} **Example:** Router(config-if)# ip rsvp listener outbound reject	Configures an RSVP router to listen for PATH messages sent through a specified interface. • Enter the **reply** keyword or the **reject** keyword to specify the response that you want to PATH messages.
Step 5	**end** **Example:** Router(config-if)# **end**	(Optional) Returns to privileged EXEC mode.

Verifying the RSVP Interface-Based Receiver Proxy Configuration

Perform the following task to verify the configuration. You can use these commands in any order.

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

SUMMARY STEPS

1. **enable**
2. **show ip rsvp listeners** [*ip-address*| **any**] [**udp** | **tcp** | **any** | *protocol*][*dst-port* | **any**]
3. **show ip rsvp sender** [**detail**] [**filter** [**destination** *address*] [**dst-port** *port-number*] [**source** *address*] [**src-port** *port-number*]]
4. **show ip rsvp reservation** [**detail**] [**filter** [**destination** *address*] [**dst-port** *port-number*] [**source** *address*] [**src-port** *port-number*]]
5. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	(Optional) Enables privileged EXEC mode. • Enter your password if prompted. **Note** Omit this step if you are using the **show** commands in user EXEC mode.
Step 2	**show ip rsvp listeners** [*ip-address*| **any**] [**udp**	**tcp**	**any**	*protocol*] [*dst-port*	**any**] **Example:** Router# show ip rsvp listeners	Displays RSVP listeners for a specified port or protocol.
Step 3	**show ip rsvp sender** [**detail**] [**filter** [**destination** *address*] [**dst-port** *port-number*] [**source** *address*] [**src-port** *port-number*]] **Example:** Router# show ip rsvp sender detail	Displays RSVP PATH-related sender information currently in the database.
Step 4	**show ip rsvp reservation** [**detail**] [**filter** [**destination** *address*] [**dst-port** *port-number*] [**source** *address*] [**src-port** *port-number*]] **Example:** Router# show ip rsvp reservation detail	Displays RSVP-related receiver information currently in the database.

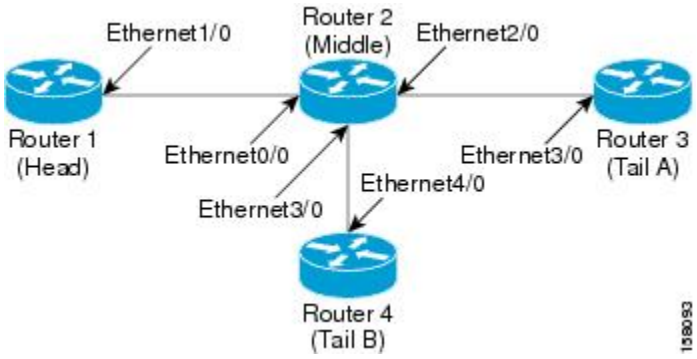
	Command or Action	Purpose
Step 5	**exit** **Example:** Router# exit	(Optional) Exits privileged EXEC mode and returns to user EXEC mode.

Configuration Examples for RSVP Interface-Based Receiver Proxy

Examples Configuring RSVP Interface-Based Receiver Proxy

The four-router network in the figure below contains the configurations for the examples shown in the following sections:

Figure 5 Sample Network with an Interface-Based Receiver Proxy Configured



Configuring a Receiver Proxy on a Middle Router on Behalf of Tailend Routers

The following example configures a receiver proxy, also called a listener, on the middle router (Router 2) on behalf of the two tailend routers (Routers 3 and 4):

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# interface gigabitEthernet 2/0/0
Router(config-if)# ip rsvp listener outbound reply
Router(config-if)# exit
Router(config)# interface gigabitethernet 3/0/0
Router(config-if)# ip rsvp listener outbound reject
Router(config-if)# end
```

Configuring PATH Messages from a Headend Router to Tailend Routers to Test the Receiver Proxy

Note If you do not have another headend router generating RSVP PATH messages available, configure one in the network for the specific purpose of testing RSVP features such as the receiver proxy. Note that these commands are not expected (or supported) in a final deployment.

The following example configures four PATH messages from the headend router (Router 1) to the tailend routers (Routers 3 and 4):

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip rsvp sender-host 10.0.0.5 10.0.0.1 TCP 2 2 100 10
Router(config)# ip rsvp sender-host 10.0.0.5 10.0.0.1 UDP 1 1 100 10
Router(config)# ip rsvp sender-host 10.0.0.7 10.0.0.1 TCP 4 4 100 10
Router(config)# ip rsvp sender-host 10.0.0.7 10.0.0.1 UDP 3 3 100 10
Router(config)# end
```

Examples Verifying RSVP Interface-Based Receiver Proxy

This section contains the following verification examples:

Verifying the PATH Messages in the Database

The following example verifies that the PATH messages you configured are in the database:

```
Router# show ip rsvp sender
To          From        Pro DPort Sport Prev Hop      I/F      BPS
10.0.0.5    10.0.0.1    TCP 2     2     none          none     100K
10.0.0.5    10.0.0.1    UDP 1     1     none          none     100K
10.0.0.7    10.0.0.1    TCP 4     4     none          none     100K
10.0.0.7    10.0.0.1    UDP 3     3     none          none     100K
```

The following example verifies that a PATH message has been terminated by a receiver proxy configured to reply.

Note A receiver proxy that is configured to reject does not cause any state to be stored in the RSVP database; therefore, this **show** command does not display these PATH messages. Only one PATH message is shown.

```
Router# show ip rsvp sender detail
PATH:
  Destination 10.0.0.5, Protocol_Id 17, Don't Police , DstPort 1
  Sender address: 10.0.0.1, port: 1
  Path refreshes:
    arriving: from PHOP 10.1.2.1 on Et0/0 every 30000 msecs
  Traffic params - Rate: 100K bits/sec, Max. burst: 10K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
  Path ID handle: 01000402.
  Incoming policy: Accepted. Policy source(s): Default
  Status: Proxy-terminated
  Output on Ethernet2/0. Policy status: NOT Forwarding. Handle: 02000401
    Policy source(s):
  Path FLR: Never repaired
```

Verifying the Running Configuration

The following example verifies the configuration for GigabitEthernet interface 2/0/0:

```
Router# show running-config interface gigbitEthernet 2/0/0
```

```
Building configuration...
Current configuration : 132 bytes
!
interface gigabitEthernet2/0/0
 ip address 172.16.0.1 255.0.0.0
 no cdp enable
 ip rsvp bandwidth 2000
 ip rsvp listener outbound reply
end
```

The following example verifies the configuration for GigabitEthernet interface 3/0/0:

```
Router# show running-config interface gigbitEthernet 3/0/0
Building configuration...
Current configuration : 133 bytes
!
interface gigabitEthernet3/0/0
 ip address 172.16.0.2 255.0.0.0
 no cdp enable
 ip rsvp bandwidth 2000
 ip rsvp listener outbound reject
end
```

Verifying the Listeners

The following example verifies the listeners (proxies) that you configured on the middle router (Router 2) on behalf of the two tailend routers (Routers 3 and 4):

```
Router# show ip rsvp listener
To            Protocol  DPort  Description          Action   OutIf
10.0.0.0        0       0      RSVP Proxy           reply    Et2/0
10.0.0.0        0       0      RSVP Proxy           reject   Et3/0
```

Verifying the Reservations

The following example displays reservations established by the middle router (Router 2) on behalf of the tailend routers (Routers 3 and 4) as seen from the headend router (Router 1):

```
Router# show ip rsvp reservation
To          From        Pro DPort Sport Next Hop      I/F      Fi Serv BPS
10.0.0.7    10.0.0.1    TCP 4     4     10.0.0.2      Gi1/0    FF RATE 100K
10.0.0.7    10.0.0.1    UDP 3     3     10.0.0.2      Gi1/0    FF RATE 100K
```

The following example verifies that a reservation is locally generated (proxied). Only one reservation is shown:

```
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: 10.2.3.3 on GigabitEthernet2/0/0
  Reservation Style is Fixed-Filter, QoS Service is Guaranteed-Rate
  Resv ID handle: 01000405.
  Created: 09:24:24 EST Fri Jun 2 2006
  Average Bitrate is 100K bits/sec, Maximum Burst is 10K bytes
  Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  Status: Proxied
  Policy: Forwarding. Policy source(s): Default
```

Verifying CAC on an Outbound Interface

The following example verifies that the proxied reservation performed CAC on the local outbound interface:

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

```
RSVP: GigabitEthernet2/0/0 has no installed reservations
RSVP: GigabitEthernet3/0/0
BPS   To          From        Protoc DPort  Sport
100K  10.0.0.7    10.0.0.1    UDP    1      1
```

Additional References

The following sections provide references related to the RSVP Interface-Based Receiver Proxy 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
Internet draft	*RSVP Proxy Approaches* , Internet draft, October 2006 [draft-lefaucheur-tsvwg-rsvp-proxy-00.txt]

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 software 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)

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for RSVP Interface-Based Receiver Proxy

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 4 Feature Information for RSVP Interface-Based Receiver Proxy

Feature Name	Releases	Feature Information
RSVP Interface-Based Receiver Proxy	Cisco IOS XE Release 2.6 Cisco IOS XE Release 3.8S	The RSVP Interface-Based Receiver Proxy feature lets you configure a proxy router by outbound interface instead of configuring a destination address for each flow going through the same interface. The following commands were introduced or modified: **ip rsvp bandwidth**, **ip rsvp listener outbound**, **show ip rsvp listeners**, **show ip rsvp reservation**, **show ip rsvp sender**. In Cisco IOS XE Release 3.8S, support was added for the Cisco ASR 903 Router.

Glossary

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

PE router --provider edge router. A router that is part of a service provider's network and is connected to a customer edge (CE) router.

proxy --A component of RSVP that manages all locally originated and terminated state.

receiver proxy --A configurable feature that allows a router to proxy RSVP RESV messages for local or remote destinations.

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

set-top box--A computer that acts as a receiver and decodes the incoming signal from a satellite dish, a cable network, or a telephone line.

RSVP Scalability Enhancements

This document describes the Cisco Resource Reservation Protocol (RSVP) scalability enhancements. It provides an overview of the feature, includes configuration tasks and examples, and lists related Cisco IOS command-line interface (CLI) commands.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for RSVP Scalability Enhancements

The network must support the following Cisco IOS XE features before the RSVP scalability enhancements are enabled:

- Resource Reservation Protocol (RSVP)
- Class-based weighted fair queueing (CBWFQ)

Restrictions for RSVP Scalability Enhancements

- Sources should not send marked packets without an installed reservation.

- Sources should not send marked packets that exceed the reserved bandwidth.
- Sources should not send marked packets to a destination other than the reserved path.

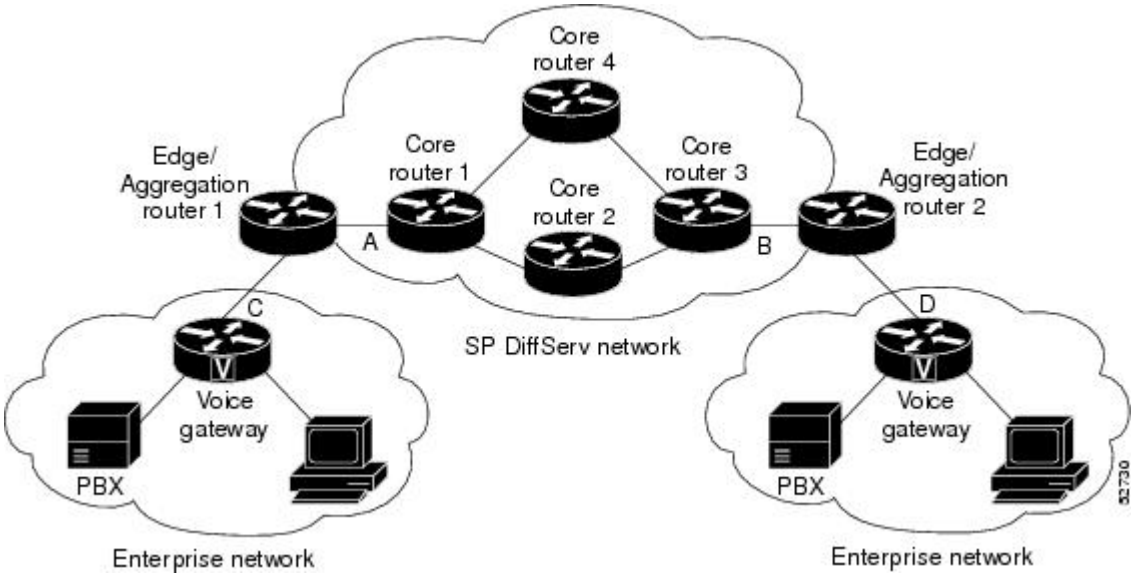
Information About RSVP Scalability Enhancements

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

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

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

Figure 6 RSVP/DiffServ Integration Topology



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

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

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

- Benefits of RSVP Scalability Enhancements, page 83

Benefits of RSVP Scalability Enhancements

Enhanced Scalability

RSVP scalability enhancements handle similar flows on a per-class basis instead of a per-flow basis. Since fewer resources are required to maintain per-class QoS guarantees, the RSVP scability enhancements provide faster processing results, thereby enhancing scalability.

Improved Router Performance

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

How to Configure RSVP Scalability Enhancements

- Configuring the Resource Provider, page 83
- Disabling Data Packet Classification, page 85
- Configuring Class Maps and Policy Maps, page 86
- Attaching a Policy Map to an Interface, page 87
- Verifying RSVP Scalability Enhancements Configuration, page 88

Configuring the Resource Provider

Note The resource provider was formerly called the QoS provider.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot / subslot / port*
4. **ip rsvp bandwidth** [*interface-kbps* [*single-flow-kbps*[**bc1** *kbps* | **sub-pool** *kbps*]/| **percent** *percent-bandwidth* [*single-flow-kbps*]]
5. **ip rsvp resource-provider none**
6. **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 slot* / *subslot* / *port* **Example:** Router(config)# interface gigabitEthernet 0/0/0	Configures the interface type and enters interface configuration mode.
Step 4	**ip rsvp bandwidth** [*interface-kbps* [*single-flow-kbps*[**bc1** *kbps* | **sub-pool** *kbps*]*]*| **percent** *percent-bandwidth* [*single-flow-kbps*]] **Example:** Router(config-if)# ip rsvp bandwidth 7500 7500	Enables RSVP on an interface. • The optional *interface-kbps* and *single-flow-kbps* arguments specify the amount of bandwidth that can be allocated by RSVP flows or to a single flow, respectively. Range is from 1 to 10000000. • The optional **sub-pool**and *kbps*keyword and argument specify subpool traffic and the amount of bandwidth that can be allocated by RSVP flows. Range is from 1 to 10000000. **Note** Repeat this command for each interface on which you want to enable RSVP. **Note** The bandwidth that you configure on the interface must match the bandwidth that you configure for the CBWFQ priority queue.
Step 5	**ip rsvp resource-provider none** **Example:** Router(config-if)# ip rsvp resource-provider none	Sets the resource provider to none. **Note** Setting the resource provider to none instructs RSVP to not associate any resources, such as WFQ queues or bandwidth, with a reservation.
Step 6	**end** **Example:** Router(config-if)# **end**	(Optional) Returns to privileged EXEC mode.

Disabling Data Packet Classification

Perform the following task to disable data packet classification. Disabling data packet classification instructs RSVP not to process every packet, but to perform admission control only.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *subslot* / *port*
4. **ip rsvp data-packet classification none**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type slot* / *subslot* / *port* **Example:** Router(config)# interface gigabitEthernet0/0/0	Configures the interface type and enters interface configuration mode.
Step 4	**ip rsvp data-packet classification none** **Example:** Router(config-if)# ip rsvp data-packet classification none	Disables data packet classification.
Step 5	**end** **Example:** Router(config-if)# **end**	(Optional) Returns to privileged EXEC mode.

Configuring Class Maps and Policy Maps

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** *class-map-name*
4. **exit**
5. **policy-map** *policy-map-name*
6. **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	**class-map** *class-map-name* **Example:** Router(config)# class-map class1	Specifies the name of the class for which you want to create or modify class-map match criteria and enters the class map configuration mode.
Step 4	**exit** **Example:** Router(config-cmap)# exit	Returns to the global configuration mode.
Step 5	**policy-map** *policy-map-name* **Example:** Router(config)# policy-map policy1	Specifies the name of the policy map to be created, added to, or modified before you can configure policies for classes whose match criteria are defined in a class map.

	Command or Action	Purpose
Step 6	**end** **Example:** Router(config-control-policymap)# **end**	(Optional) Returns to privileged EXEC mode.

Attaching a Policy Map to an Interface

Perform the following task to attach a policy map to an interface. If at the time you configure the RSVP scalability enhancements, there are existing reservations that use classic RSVP, no additional marking, classification, or scheduling is provided for these flows. You can also delete these reservations after you configure the RSVP scalability enhancements.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *subslot* / *port*
4. **service-policy** {**input** | **output**} *policy-map-name*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type slot* / *subslot* / *port* **Example:** Router(config)# interface gigabitEthernet 0/0/0	Configures the interface type and enters interface configuration mode.

	Command or Action	Purpose
Step 4	**service-policy** {**input** | **output**} *policy-map-name* **Example:** Router(config-if)# service-policy input policy1	Attaches a single policy map to one or more interfaces to specify the service policy for those interfaces.
Step 5	**end** **Example:** Router(config-if)# **end**	(Optional) Returns to privileged EXEC mode.

Verifying RSVP Scalability Enhancements Configuration

SUMMARY STEPS

1. Enter the **show ip rsvp interface detail**command to display information about interfaces, subinterfaces, resource providers, and data packet classification. The output in the following example shows that the ATM interface 6/0 has resource provider none configured and that data packet classification is turned off:
2. Enter the **show ip rsvp installed detail**command to display information about interfaces, subinterfaces, their admitted reservations, bandwidth, resource providers, and data packet classification.
3. Wait for a while, then enter the **show ip rsvp installed detail**command again. In the following output, notice there is no increment in the number of packets classified:

DETAILED STEPS

Step 1 Enter the **show ip rsvp interface detail**command to display information about interfaces, subinterfaces, resource providers, and data packet classification. The output in the following example shows that the ATM interface 6/0 has resource provider none configured and that data packet classification is turned off:

Example:

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

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

Step 2 Enter the **show ip rsvp installed detail**command to display information about interfaces, subinterfaces, their admitted reservations, bandwidth, resource providers, and data packet classification.

Example:

```
Router# show ip rsvp installed detail
RSVP: GigabitEthernet0/0/0 has no installed reservations
RSVP: ATM6/0 has the following installed reservations
RSVP Reservation. Destination is 10.20.20.212, Source is 10.10.10.211,
  Protocol is UDP, Destination port is 14, Source port is 14
  Reserved bandwidth: 50K bits/sec, Maximum burst: 1K bytes, Peak rate: 50K bits/sec
  Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
  Resource provider for this flow: None
  Conversation supports 1 reservations
  Data given reserved service: 0 packets (0 bytes)
  Data given best-effort service: 0 packets (0 bytes)
  Reserved traffic classified for 54 seconds
  Long-term average bitrate (bits/sec): 0M reserved, 0M best-effort
RSVP Reservation. Destination is 10.20.20.212, Source is 10.10.10.211,
  Protocol is UDP, Destination port is 10, Source port is 10
  Reserved bandwidth: 20K bits/sec, Maximum burst: 1K bytes, Peak rate: 20K bits/sec
  Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
  Resource provider for this flow: None
  Conversation supports 1 reservations
  Data given reserved service: 0 packets (0 bytes)
  Data given best-effort service: 0 packets (0 bytes)
  Reserved traffic classified for 80 seconds
  Long-term average bitrate (bits/sec): 0M reserved, 0M best-effort
```

Step 3 Wait for a while, then enter the **show ip rsvp installed detail**command again. In the following output, notice there is no increment in the number of packets classified:

Example:

```
Router# show ip rsvp installed detail
RSVP: Ethernet3/3 has no installed reservations
RSVP: ATM6/0 has the following installed reservations
RSVP Reservation. Destination is 10.20.20.212, Source is 10.10.10.211,
  Protocol is UDP, Destination port is 14, Source port is 14
  Reserved bandwidth: 50K bits/sec, Maximum burst: 1K bytes, Peak rate: 50K bits/sec
  Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
  Resource provider for this flow: None
  Conversation supports 1 reservations
  Data given reserved service: 0 packets (0 bytes)
  Data given best-effort service: 0 packets (0 bytes)
  Reserved traffic classified for 60 seconds
  Long-term average bitrate (bits/sec): 0 reserved, OM best-effort
RSVP Reservation. Destination is 10.20.20.212, Source is 10.10.10.211,
  Protocol is UDP, Destination port is 10, Source port is 10
  Reserved bandwidth: 20K bits/sec, Maximum burst: 1K bytes, Peak rate: 20K bits/sec
  Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
  Resource provider for this flow: None
  Conversation supports 1 reservations
  Data given reserved service: 0 packets (0 bytes)
  Data given best-effort service: 0 packets (0 bytes)
  Reserved traffic classified for 86 seconds
  Long-term average bitrate (bits/sec): OM reserved, 0M best-effort
```

Monitoring and Maintaining RSVP Scalability Enhancements

To monitor and maintain RSVP scalability enhancements, use the following commands in EXEC mode. The following commands can be entered in any order.

Command	Purpose
Router# **show ip rsvp installed**	Displays information about interfaces and their admitted reservations.
Router# **show ip rsvp installed detail**	Displays additional information about interfaces and their admitted reservations.
Router# **show ip rsvp interface**	Displays RSVP-related interface information.
Router# **show ip rsvp interface detail**	Displays additional RSVP-related interface information.
Router# **show queueing** [**custom** | **fair** | **priority** | **random-detect** [**interface** *serial-number*]]	Displays all or selected configured queueing strategies and available bandwidth for RSVP reservations.

Configuration Examples for RSVP Scalability Enhancements

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

Following is output from the **showiprsvpinterfacedetail** command before a resource provider is configured as none and data-packet classification is turned off:

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

Following is the output from the **showqueueing**command before a resource provider is configured as none and data packet classification is turned off:

```
Router# show queueing int atm6/0
```

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

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

The following example shows how to configure resource provider as none:

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

Router(config-if)# end
Router#
```

The following example shows how to turn off the data packet classification:

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

Router(config-if)# end
```

Following is the output from the **showiprsvpinterfacedetail** command after resource provider has been configured as none and data packet classification has been turned off:

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

The following output from the **showiprsvpinstalleddetail** command verifies that resource provider none is configured and data packet classification is turned off:

```
Router# show ip rsvp installed detail
RSVP: ATM6/0 has the following installed reservations
RSVP Reservation. Destination is 10.20.20.212, Source is 10.10.10.211,
  Protocol is UDP, Destination port is 14, Source port is 14
  Reserved bandwidth: 50K bits/sec, Maximum burst: 1K bytes, Peak rate: 50K bits/sec
  Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
  Resource provider for this flow: None
  Conversation supports 1 reservations
  Data given reserved service: 3192 packets (1557696 bytes)
  Data given best-effort service: 42 packets (20496 bytes)
  Reserved traffic classified for 271 seconds
  Long-term average bitrate (bits/sec): 45880 reserved, 603 best-effort
RSVP Reservation. Destination is 10.20.20.212, Source is 10.10.10.211,
  Protocol is UDP, Destination port is 10, Source port is 10
  Reserved bandwidth: 20K bits/sec, Maximum burst: 1K bytes, Peak rate: 20K bits/sec
  Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
```

```
  Resource provider for this flow: None
  Conversation supports 1 reservations
  Data given reserved service: 1348 packets (657824 bytes)
  Data given best-effort service: 0 packets (0 bytes)
  Reserved traffic classified for 296 seconds
  Long-term average bitrate (bits/sec): 17755 reserved, 0M best-effort
```

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

```
Router# show ip rsvp installed detail
RSVP: GigabitEthernet3/3 has no installed reservations
RSVP: ATM6/0 has the following installed reservations
RSVP Reservation. Destination is 10.20.20.212, Source is 10.10.10.211,
  Protocol is UDP, Destination port is 14, Source port is 14
  Reserved bandwidth: 50K bits/sec, Maximum burst: 1K bytes, Peak rate: 50K bits/sec
  Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
  Resource provider for this flow: None
  Conversation supports 1 reservations
  Data given reserved service: 3192 packets (1557696 bytes)
  Data given best-effort service: 42 packets (20496 bytes)
  Reserved traffic classified for 282 seconds
  Long-term average bitrate (bits/sec): 44051 reserved, 579 best-effort
RSVP Reservation. Destination is 145.20.20.212, Source is 145.10.10.211,
  Protocol is UDP, Destination port is 10, Source port is 10
  Reserved bandwidth: 20K bits/sec, Maximum burst: 1K bytes, Peak rate: 20K bits/sec
  Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
  Resource provider for this flow: None
  Conversation supports 1 reservations
  Data given reserved service: 1348 packets (657824 bytes)
  Data given best-effort service: 0 packets (0 bytes)
  Reserved traffic classified for 307 seconds
  Long-term average bitrate (bits/sec): 17121 reserved, 0M best-effort
```

The following output verifies that data packet classification is occurring:

```
Router# show ip rsvp installed detail
Enter configuration commands, one per line.  End with CNTL/Z.
RSVP: ATM6/0 has the following installed reservations
RSVP Reservation. Destination is 10.20.20.212, Source is 10.10.10.211,
  Protocol is UDP, Destination port is 14, Source port is 14
  Reserved bandwidth: 50K bits/sec, Maximum burst: 1K bytes, Peak rate: 50K bits/sec
  Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
  Resource provider for this flow: None
  Conversation supports 1 reservations
  Data given reserved service: 3683 packets (1797304 bytes)
  Data given best-effort service: 47 packets (22936 bytes)
  Reserved traffic classified for 340 seconds
  Long-term average bitrate (bits/sec): 42201 reserved, 538 best-effort
RSVP Reservation. Destination is 10.20.20.212, Source is 10.10.10.211,
  Protocol is UDP, Destination port is 10, Source port is 10
  Reserved bandwidth: 20K bits/sec, Maximum burst: 1K bytes, Peak rate: 20K bits/sec
  Min Policed Unit: 0 bytes, Max Pkt Size: 1514 bytes
  Resource provider for this flow: None
  Conversation supports 1 reservations
  Data given reserved service: 1556 packets (759328 bytes)
  Data given best-effort service: 0 packets (0 bytes)
  Reserved traffic classified for 364 seconds
  Long-term average bitrate (bits/sec): 16643 reserved, 0M best-effort
```

Note You can use **debugiprsvptraffic-control** and **debugiprsvpwfq** simultaneously. Use the**showdebug** command to see which debugging commands are enabled.

Additional References

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

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
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

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

RFCs

RFC	Title
RFC 2205	Resource Reservation Protocol
RFC 2206	RSVP Management Information Base using SMIv2

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for RSVP Scalability Enhancements

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 5 Feature Information for RSVP Scalability Enhancements

Feature Name	Releases	Feature Information
RSVP Scalability Enhancements	Cisco IOS XE Release 2.6 Cisco IOS XE Release 3.8S	RSVP scalability enhancements let you select a resource provider (formerly called a QoS provider) and disable data packet classification so that RSVP performs admission control only. This facilitates integration with service provider (DiffServ) networks and enables scalability across enterprise networks. The following commands were introduced or modified: **debug ip rsvp traffic-control**, **debug ip rsvp wfq**, **ip rsvp data-packet classification none**, **ip rsvp resource-provider**, **show ip rsvp installed**, **show ip rsvp interface**, **show queueing**. In Cisco IOS XE Release 3.8S, support was added for the Cisco ASR 903 Router.

Glossary

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

aggregate --A collection of packets with the same DSCP.

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

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

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

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

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

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

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

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

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

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

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

Voice over IP --See VoIP.

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

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

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

RSVP Message Authentication

The Resource Reservation Protocol (RSVP) Message Authentication feature provides a secure method to control quality of service (QoS) access to a network.

History for the RSVP Message Authentication Feature

Release	Modification
12.2(15)T	This feature was introduced.
12.0(26)S	Restrictions were added for interfaces that use Fast Reroute (FRR) node or link protection and for RSVP hellos for FRR for packet over SONET (POS) interfaces.
12.0(29)S	Support was added for per-neighbor keys.
12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This feature was integrated into Cisco IOS Release 12.2(33)SXH.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for RSVP Message Authentication

Ensure that RSVP is configured on one or more interfaces on at least two neighboring devices that share a link within the network.

Restrictions for RSVP Message Authentication

- The RSVP Message Authentication feature is only for authenticating RSVP neighbors.
- The RSVP Message Authentication feature cannot discriminate between various QoS applications or users, of which many may exist on an authenticated RSVP neighbor.
- Different send and accept lifetimes for the same key in a specific key chain are not supported; all RSVP key types are bidirectional.
- Authentication for graceful restart hello messages is supported for per-neighbor and per-access control list (ACL) keys, but not for per-interface keys.
- You cannot use the **ip rsvp authentication key** and the **ip rsvp authentication key-chain** commands on the same device interface.
- For a Multiprotocol Label Switching/Traffic Engineering (MPLS/TE) configuration, use per-neighbor keys with physical addresses and device IDs.

Information About RSVP Message Authentication

Feature Design of RSVP Message Authentication

Network administrators need the ability to establish a security domain to control the set of systems that initiate RSVP requests.

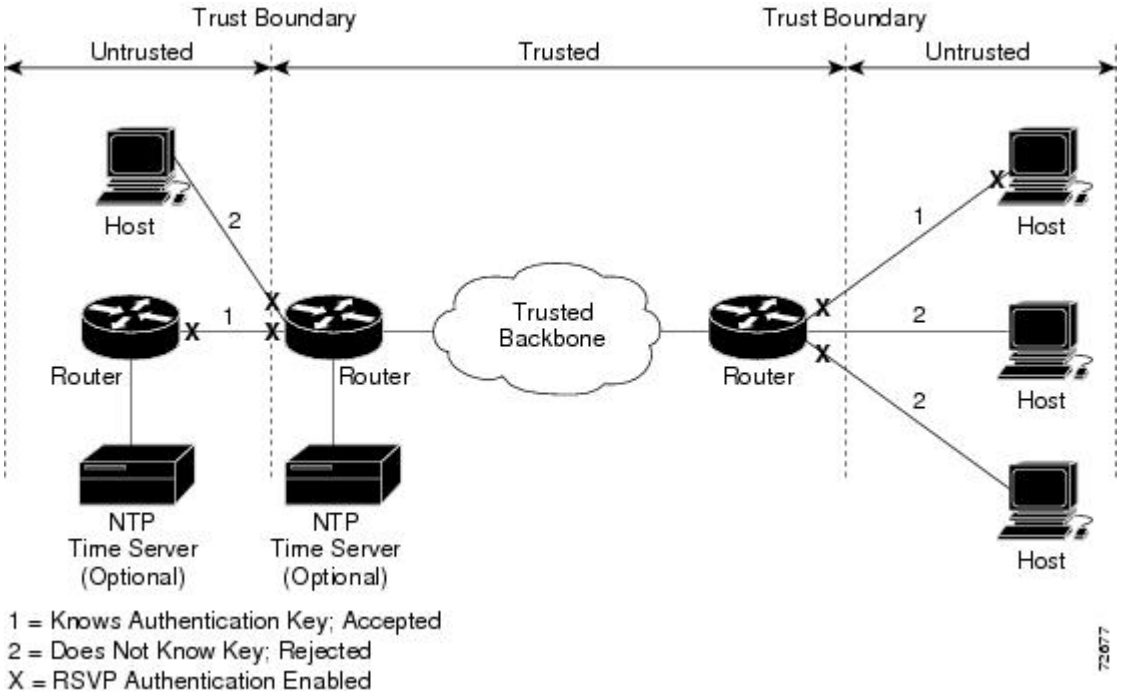
The RSVP Message Authentication feature permits neighbors in an RSVP network to use a secure hash to sign all RSVP signaling messages digitally, thus allowing the receiver of an RSVP message to verify the sender of the message without relying solely on the sender's IP address as is done by issuing the **ip rsvp neighbor** command with an ACL.

The signature is accomplished on a per-RSVP-hop basis with an RSVP integrity object in the RSVP message as defined in RFC 2747. This method provides protection against forgery or message modification. However, the receiver must know the security key used by the sender in order to validate the digital signature in the received RSVP message.

Network administrators manually configure a common key for each RSVP neighbor interface on the shared network. A sample configuration is shown in the figure below.

Figure 7

RSVP Message Authentication Configuration



Global Authentication and Parameter Inheritance

You can configure global defaults for all authentication parameters including key, type, window size, lifetime, and challenge. These defaults are inherited when you enable authentication for each neighbor or interface. However, you can also configure these parameters individually on a per-neighbor or per-interface basis in which case the inherited global defaults are ignored.

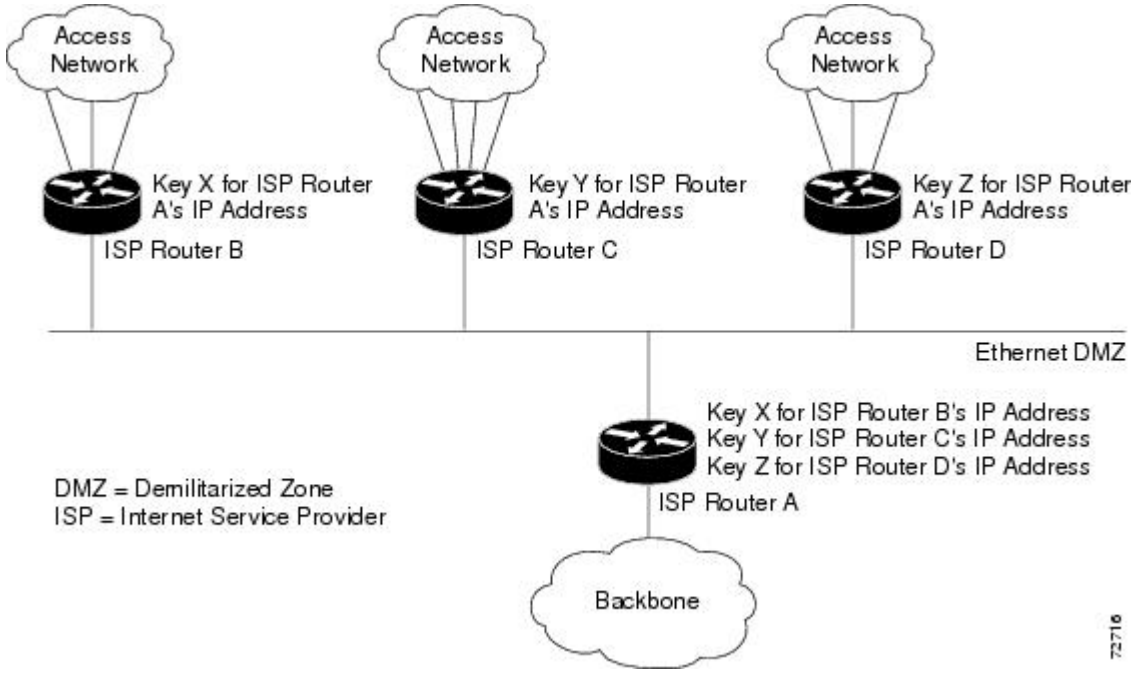
Using global authentication and parameter inheritance can simplify configuration because you can enable or disable authentication without having to change each per-neighbor or per-interface attribute. You can activate authentication for all neighbors by using two commands, one to define a global default key and one to enable authentication globally. However, using the same key for all neighbors does not provide the best network security.

Note RSVP uses the following rules when choosing which authentication parameter to use when that parameter is configured at multiple levels (per-interface, per-neighbor, or global). RSVP goes from the most specific to the least specific; that is, per-neighbor, per-interface, and then global. The rules are slightly different when searching the configuration for the right key to authenticate an RSVP message-- per-neighbor, per-ACL, per-interface, and then global.

Per-Neighbor Keys

In the figure below, to enable authentication between Internet service provider (ISP) Routers A and B, A and C, and A and D, the ISPs must share a common key. However, sharing a common key also enables authentication between ISP Routers B and C, C and D, and B and D. You may not want authentication among all the ISPs because they might be different companies with unique security domains.

Figure 8 RSVP Message Authentication in an Ethernet Configuration



On ISP Router A, you create a different key for ISP Routers B, C, and D and assign them to their respective IP addresses using RSVP commands. On the other devices, create a key to communicate with ISP Router A's IP address.

Key Chains

For each RSVP neighbor, you can configure a list of keys with specific IDs that are unique and have different lifetimes so that keys can be changed at predetermined intervals automatically without any disruption of service. Automatic key rotation enhances network security by minimizing the problems that could result if an untrusted source obtained, deduced, or guessed the current key.

Note If you use overlapping time windows for your key lifetimes, RSVP asks the Cisco software key manager component for the next live key starting at time T. The key manager walks the keys in the chain until it finds the first one with start time S and end time E such that S <= T <= E. Therefore, the key with the smallest value (E-T) may not be used next.

Benefits of RSVP Message Authentication

Improved Security

The RSVP Message Authentication feature greatly reduces the chance of an RSVP-based spoofing attack and provides a secure method to control QoS access to a network.

Multiple Environments

The RSVP Message Authentication feature can be used in traffic engineering (TE) and non-TE environments as well as with the subnetwork bandwidth manager (SBM).

Multiple Platforms and Interfaces

The RSVP Message Authentication feature can be used on any supported RSVP platform or interface.

How to Configure RSVP Message Authentication

The following configuration parameters instruct RSVP on how to generate and verify integrity objects in various RSVP messages.

Note There are two configuration procedures: full and minimal. There are also two types of authentication procedures: interface and neighbor.

Per-Interface Authentication--Full Configuration

Perform the following procedures for a full configuration for per-interface authentication:

Per-Interface Authentication--Minimal Configuration

Perform the following tasks for a minimal configuration for per-interface authentication:

Per-Neighbor Authentication--Full Configuration

Perform the following procedures for a full configuration for per-neighbor authentication:

Per-Neighbor Authentication--Minimal Configuration

Perform the following tasks for a minimal configuration for per-neighbor authentication:

- Enabling RSVP on an Interface, page 102
- Configuring an RSVP Authentication Type, page 103
- Configuring an RSVP Authentication Key, page 105
- Enabling RSVP Key Encryption, page 107
- Enabling RSVP Authentication Challenge, page 108
- Configuring RSVP Authentication Lifetime, page 111
- Configuring RSVP Authentication Window Size, page 114
- Activating RSVP Authentication, page 117

Enabling RSVP on an Interface

Perform this task to enable RSVP on an interface.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Device(config)# interface Ethernet0/0	Enters interface configuration mode. • The *type number*argument identifies the interface to be configured.
Step 4	ip rsvp bandwidth [*interface-kbps* [*single-flow-kbps*]] **Example:** Device(config-if)# ip rsvp bandwidth 7500 7500	Enables RSVP on an interface. • The optional *interface-kbps* and *single-flow-kbps* arguments specify the amount of bandwidth that can be allocated by RSVP flows or to a single flow, respectively. Values are from 1 to 10,000,000. **Note** Repeat this command for each interface that you want to enable.

	Command or Action	Purpose
Step 5	**end** **Example:** Device(config-if)# **end**	Returns to privileged EXEC mode.

Configuring an RSVP Authentication Type

Perform this task to configure an RSVP authentication type.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Do one of the following:
   - **ip rsvp authentication type** {**md5 | sha-1**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Device(config)# interface Ethernet0/0	Enters interface configuration mode. • The *type number*argument identifies the interface to be configured. **Note** Omit this step if you are configuring an authentication type for a neighbor or setting a global default.

Command or Action	Purpose
Step 4 Do one of the following: • **ip rsvp authentication type** {**md5 | sha-1** **Example:** For interface authentication: **Example:** Device(config-if)# **ip rsvp authentication type sha-1** **Example:** **Example:** For neighbor authentication: **Example:** Device(config)# **ip rsvp authentication neighbor address 10.1.1.1 type sha-1** **Example:** **Example:** Device(config)# **ip rsvp authentication neighbor access-list 1 type sha-1** **Example:** **Example:** For a global default:	Specifies the algorithm used to generate cryptographic signatures in RSVP messages on an interface or globally. • The algorithms are **md5**, the default, and **sha-1**, which is newer and more secure than **md5**. **Note** Omit the **neighbor address** *address*or the **neighbor access-list** *acl-name*or *acl-number*to set the global default.

	Command or Action	Purpose
	Example: Device(config)# **ip rsvp authentication type sha-1**	
Step 5	**end** **Example:** Device(config-if)# **end**	Returns to privileged EXEC mode.

Configuring an RSVP Authentication Key

Perform this task to configure an RSVP authentication key.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip rsvp authentication key passphrase**
5. **exit**
6. Do one of the following:
   - **ip rsvp authentication key-chain** *chain*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode. **Note** If you want to configure a key, proceed to Step 3; if you want to configure a key chain, proceed to Step 6.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** Device(config)# interface Ethernet0/0	Enters interface configuration mode. • The *type number*argument identifies the interface to be configured. **Note** Omit this step and go to Step 6 if you want to configure only a key chain.
Step 4	**ip rsvp authentication key passphrase** **Example:** Device(config-if)# **ip rsvp authentication key** 11223344 **Example:**	Specifies the data string (key) for the authentication algorithm. • The key consists of 8 to 40 characters. It can include spaces and multiple words. It can also be encrypted or appear in clear text when displayed. **Note** Omit this step if you want to configure a key chain.
Step 5	**exit** **Example:** Device(config-if)# exit	Exits to global configuration mode.

	Command or Action	Purpose
Step 6	Do one of the following: • **ip rsvp authentication key-chain** *chain* **Example:** For neighbor authentication: **Example:** Device(config)# **ip rsvp authentication neighbor address 10.1.1.1 key-chain xzy** **Example:** **Example:** Device(config)# **ip rsvp authentication neighbor access-list 1 key-chain xzy** **Example:** **Example:** For a global default: **Example:** Device(config)# **ip rsvp authentication key-chain xzy**	Specifies the data string (key chain) for the authentication algorithm. • The key chain must have at least one key, but can have up to 2,147,483647 keys. **Note** You cannot use the **ip rsvp authentication key** and the **ip rsvp authentication key-chain** commands on the same device interface. The commands supersede each other; however, no error message is generated. **Note** Omit the **neighbor address** *address*or the **neighbor access-list** *acl-name*or *acl-number*to set the global default.
Step 7	**end** **Example:** Device(config)# **end**	Returns to privileged EXEC mode.

Enabling RSVP Key Encryption

Perform this task to enable RSVP key encryption when the key is stored in the configuration. (This prevents anyone from seeing the clear text key in the configuration file.)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key config-key 1** *string*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**key config-key 1** *string* **Example:** Device(config)# key config-key 1 11223344	Enables key encryption in the configuration file. **Note** The *string* argument can contain up to eight alphanumeric characters.
Step 4	**end** **Example:** Device(config)# **end**	Returns to privileged EXEC mode.

Enabling RSVP Authentication Challenge

Perform this task to enable RSVP authentication challenge.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Do one of the following:
   - **ip rsvp authentication challenge**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Device(config)# interface Ethernet0/0	Enters interface configuration mode. • The *type number*argument identifies the interface to be configured. **Note** Omit this step if you are configuring an authentication challenge for a neighbor or setting a global default.

Command or Action	Purpose
Step 4 Do one of the following: • **ip rsvp authentication challenge** **Example:** For interface authentication: **Example:** Device(config-if)# **ip rsvp authentication challenge** **Example:** **Example:** For neighbor authentication: **Example:** Device(config)# **ip rsvp authentication neighbor address 10.1.1.1 challenge** **Example:** **Example:** Device(config)# **ip rsvp authentication neighbor access-list 1 challenge** **Example:** **Example:** For a global default:	Makes RSVP perform a challenge-response handshake on an interface or globally when RSVP learns about any new challenge-capable neighbors on a network. **Note** Omit the **neighbor address** *address*or the **neighbor access-list** *acl-name*or *acl-number*to set the global default.

	Command or Action	Purpose
	Example: Device(config)# **ip rsvp authentication challenge**	
Step 5	**end** **Example:** Device(config-if)# **end**	Returns to privileged EXEC mode.

Configuring RSVP Authentication Lifetime

Perform this task to configure the lifetimes of security associations between RSVP neighbors.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Do one of the following:
   - **ip rsvp authentication lifetime** *hh* **:** *mm* **:** *ss*
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.

Command or Action	Purpose
Step 3 **interface** *type number* **Example:** Device(config)# interface Ethernet0/0	Enters interface configuration mode. **Note** Omit this step if you are configuring an authentication lifetime for a neighbor or setting a global default. • The *type number*argument identifies the interface to be configured.

Command or Action	Purpose
Step 4 Do one of the following: • **ip rsvp authentication lifetime** *hh* **:** *mm* **:** *ss* **Example:** For interface authentication: **Example:** Device(config-if)# **ip rsvp authentication lifetime 00:05:00** **Example:** **Example:** For neighbor authentication: **Example:** Device(config)# **ip rsvp authentication neighbor address 10.1.1.1 lifetime 00:05:00** **Example:** **Example:** Device(config)# **ip rsvp authentication neighbor access-list 1 lifetime 00:05:00** **Example:** **Example:** For a global default:	Controls how long RSVP maintains security associations with RSVP neighbors on an interface or globally. • The default security association for **hh:mm:ss** is 30 minutes; the range is 1 second to 24 hours. **Note** Omit the **neighbor address** *address*or the **neighbor access-list** *acl-name*or *acl-number*to set the global default.

Command or Action	Purpose
Example: Device(config)# **ip rsvp authentication 00:05:00**	
Step 5 **end** **Example:** Device(config-if)# **end**	Returns to privileged EXEC mode.

Configuring RSVP Authentication Window Size

Perform this task to configure the RSVP authentication window size.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Do one of the following:
   - **ip rsvp authentication window-size n**
5. **end**

DETAILED STEPS

Command or Action	Purpose
Step 1 **enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2 **configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.

Command or Action	Purpose
Step 3 **interface** *type number* **Example:** Device(config)# interface Ethernet0/0	Enters interface configuration mode. • The *type number*argument identifies the interface to be configured. **Note** Omit this step if you are configuring a window size for a neighbor or setting a global default.

Command or Action	Purpose
Step 4 Do one of the following: • **ip rsvp authentication window-size n** **Example:** For interface authentication: **Example:** Device(config-if)# **ip rsvp authentication** window-size 2 **Example:** **Example:** For neighbor authentication: **Example:** Device(config)# **ip rsvp authentication neighbor address 10.1.1.1** window-size 2 **Example:** **Example:** Device(config)# **ip rsvp authentication neighbor access-list 1** window-size **Example:** **Example:** For a global default:	Specifies the maximum number of authenticated messages that can be received out of order on an interface or globally. • The default value is one message; the range is 1 to 64 messages. **Note** Omit the **neighbor address** *address*or the **neighbor access-list** *acl-name*or *acl-number*to set the global default.

	Command or Action	Purpose
	Example: Device(config)# **ip rsvp authentication** window-size 2	
Step 5	**end** **Example:** Device(config-if)# **end**	Returns to privileged EXEC mode.

Activating RSVP Authentication

Perform this task to activate RSVP authentication.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. Do one of the following:
   - **ip rsvp authentication**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.

Command or Action	Purpose
Step 3 **interface** *type number* **Example:** Device(config)# interface Ethernet0/0	Enters interface configuration mode. • The *type number*argument identifies the interface to be configured. **Note** Omit this step if you are configuring authentication for a neighbor or setting a global default.

Command or Action	Purpose
Step 4 Do one of the following: • **ip rsvp authentication** **Example:** For interface authentication: **Example:** Device(config-if)# **ip rsvp authentication** **Example:** **Example:** For neighbor authentication: **Example:** Device(config)# **ip rsvp authentication neighbor address 10.1.1.1** **Example:** **Example:** Device(config)# **ip rsvp authentication neighbor access-list 1** **Example:** **Example:** For a global default: **Example:** Device(config)# **ip rsvp authentication**	Activates RSVP cryptographic authentication on an interface or globally. **Note** Omit the **neighbor address** *address*or the **neighbor access-list** *acl-name*or *acl-number*to set the global default.

	Command or Action	Purpose
Step 5	**end** **Example:** Device(config-if)# **end**	Returns to privileged EXEC mode.

Verifying RSVP Message Authentication

Perform this task to verify that the RSVP Message Authentication feature is functioning.

SUMMARY STEPS

1. **enable**
2. **show ip rsvp interface [detail] [interface-type interface-number]**
3. **show ip rsvp authentication** [**detail**] [**from** {*ip-address* | *hostname*}] [**to** {*ip-address* | *hostname*}]
4. **show ip rsvp counters** [**authentication** | **interface** *interface-unit* | **neighbor** | **summary**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**show ip rsvp interface [detail] [interface-type interface-number]** **Example:** Device# show ip rsvp interface detail	Displays information about interfaces on which RSVP is enabled, including the current allocation budget and maximum available bandwidth. • The optional **detail** keyword displays the bandwidth, signaling, and authentication parameters.
Step 3	**show ip rsvp authentication** [**detail**] [**from** {*ip-address* | *hostname*}] [**to** {*ip-address* | *hostname*}] **Example:** Device# show ip rsvp authentication detail	Displays the security associations that RSVP has established with other RSVP neighbors. • The optional **detail** keyword displays state information that includes IP addresses, interfaces enabled, and configured cryptographic authentication parameters about security associations that RSVP has established with neighbors.

	Command or Action	Purpose
Step 4	**show ip rsvp counters** [**authentication** | **interface** *interface-unit* | **neighbor** | **summary**] **Example:** Device# show ip rsvp counters summary **Example:** **Example:** Device# show ip rsvp counters authentication	Displays all RSVP counters. **Note** The errors counter increments whenever an authentication error occurs, but can also increment for errors not related to authentication. • The optional **authentication** keyword shows a list of RSVP authentication counters. • The optional **interface** *interface-unit* keyword argument combination shows the number of RSVP messages sent and received by the specific interface. • The optional **neighbor**keyword shows the number of RSVP messages sent and received by the specific neighbor. • The optional **summary**keyword shows the cumulative number of RSVP messages sent and received by the device. It does not print per-interface counters.

Configuring a Key Chain

Perform this task to configure a key chain for neighbor authentication.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **key chain** *name-of-chain*
4. {**key** [*key-ID*] | **key-string** [*text*] | **accept-lifetime** [*start-time* {**infinite** | *end-time* | **duration** *seconds*}] | **send-lifetime** [*start-time* {**infinite** | *end-time* | **duration** *seconds*}]
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**key chain** *name-of-chain* **Example:** Device(config)# key chain neighbor_V	Enters key-chain mode.
Step 4	{**key** [*key-ID*] | **key-string** [*text*] | **accept-lifetime** [*start-time* {**infinite** | *end-time* | **duration** *seconds*}] | **send-lifetime** [*start-time* {**infinite** | *end-time* | **duration** *seconds*}] **Example:** Device(config-keychain)# key 1 **Example:** **Example:** Device(config-keychain)# key-string ABcXyz	Selects the parameters for the key chain. (These are submodes.) **Note** For details on these parameters, see the Cisco IOS IP Command Reference, Volume 2 of 4, Routing Protocols, Release 12.3T. **Note** **accept-lifetime** is ignored when a key chain is assigned to RSVP.
Step 5	**end** **Example:** Device(config-keychain)# **end**	Returns to privileged EXEC mode.

Binding a Key Chain to an RSVP Neighbor

Perform this task to bind a key chain to an RSVP neighbor for neighbor authentication.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. Do one of the following:
   - ip rsvp authentication neighbor address *address* **key-chain** *key-chain-name*
   -
   - **ip rsvp authentication neighbor access-list** *acl-name* **or** *acl-number* **key-chain** *key-chain-name*
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Device# configure terminal	Enters global configuration mode.
Step 3	Do one of the following: • ip rsvp authentication neighbor address *address* **key-chain** *key-chain-name* • • **ip rsvp authentication neighbor access-list** *acl-name* **or** *acl-number* **key-chain** *key-chain-name* **Example:** Device(config)# ip rsvp authentication neighbor access-list **1** key-chain neighbor_V	Binds a key chain to an IP address or to an ACL and enters key-chain mode. **Note** If you are using an ACL, you must create it before you bind it to a key chain. See the ip rsvp authentication command in the Glossary, page 129 section for examples.
Step 4	**end** **Example:** Device(config-keychain)# **end**	Returns to privileged EXEC mode.

Troubleshooting Tips

After you enable RSVP authentication, RSVP logs system error events whenever an authentication check fails. These events are logged instead of just being displayed when debugging is enabled because they may indicate potential security attacks. The events are generated when:

- RSVP receives a message that does not contain the correct cryptographic signature. This could be due to misconfiguration of the authentication key or algorithm on one or more RSVP neighbors, but it may also indicate an (unsuccessful) attack.
- RSVP receives a message with the correct cryptographic signature, but with a duplicate authentication sequence number. This may indicate an (unsuccessful) message replay attack.
- RSVP receives a message with the correct cryptographic signature, but with an authentication sequence number that is outside the receive window. This could be due to a reordered burst of valid RSVP messages, but it may also indicate an (unsuccessful) message replay attack.
- Failed challenges result from timeouts or bad challenge responses.

To troubleshoot the RSVP Message Authentication feature, use the following commands in privileged EXEC mode.

Command	Purpose
Device# **debug ip rsvp authentication**	Displays output related to RSVP authentication.
Device# **debug ip rsvp dump signalling**	Displays brief information about signaling (Path and Resv) messages.
Device# **debug ip rsvp errors**	Displays error events including authentication errors.

Configuration Examples for RSVP Message Authentication

Example RSVP Message Authentication Per-Interface

In the following example, the cryptographic authentication parameters, including type, key, challenge, lifetime, and window size are configured; and authentication is activated:

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# interface e0/0
Device(config-if)# ip rsvp bandwidth 7500 7500
Device(config-if)# ip rsvp authentication type sha-1
Device(config-if)# ip rsvp authentication key 11223344
Device(config-if)# ip rsvp authentication challenge
Device(config-if)# ip rsvp authentication lifetime 00:30:05
Device(config-if)# ip rsvp authentication window-size 2
Device(config-if)# ip rsvp authentication
```

In the following output from the **show ip rsvp interface detail** command, notice the cryptographic authentication parameters that you configured for the Ethernet0/0 interface:

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

In the preceding example, the authentication key appears in clear text. If you enter the **key-config-key 1** *string* command, the key appears encrypted, as in the following example:

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

In the following output, notice that the authentication key changes from encrypted to clear text after the **no key config-key 1** command is issued:

```
Device# show running-config interface e0/0
Building configuration...
Current configuration :247 bytes
!
interface Ethernet0/0
 ip address 192.168.101.2 255.255.255.0
 no ip directed-broadcast
 ip pim dense-mode
 no ip mroute-cache
 no cdp enable
 ip rsvp bandwidth 7500 7500
 ip rsvp authentication key 7>70>9:7<872>?74
 ip rsvp authentication
end
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# no key config-key 1

Device(config)# end


Device# show running-config
*Jan 30  08:02:09.559:%SYS-5-CONFIG_I:Configured from console by console
int e0/0
Building configuration...
Current configuration :239 bytes
!
interface Ethernet0/0
 ip address 192.168.101.2 255.255.255.0
 no ip directed-broadcast
 ip pim dense-mode
 no ip mroute-cache
 no cdp enable
 ip rsvp bandwidth 7500 7500
 ip rsvp authentication key 11223344
 ip rsvp authentication
end
```

Example RSVP Message Authentication Per-Neighbor

In the following example, a key chain with two keys for each neighbor is defined, then an access list and a key chain are created for neighbors V, Y, and Z and authentication is explicitly enabled for each neighbor and globally. However, only the neighbors specified will have their messages accepted; messages from other sources will be rejected. This enhances network security.

For security reasons, you should change keys on a regular basis. When the first key expires, the second key automatically takes over. At that point, you should change the first key's key-string to a new value and then set the send lifetimes to take over after the second key expires. The device will log an event when a key expires to remind you to update it.

The lifetimes of the first and second keys for each neighbor overlap. This allows for any clock synchronization problems that might cause the neighbors not to switch keys at the right time. You can avoid these overlaps by configuring the neighbors to use Network Time Protocol (NTP) to synchronize their clocks to a time server.

For an MPLS/TE configuration, physical addresses and device IDs are given.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# key chain neighbor_V
Device(config-keychain)# key 1
Device(config-keychain-key)# key-string R72*UiAXy
Device(config-keychain-key)# send-life 02:00:00 1 jun 2003 02:00:00 1 aug 2003
Device(config-keychain-key)# exit
Device(config-keychain)# key 2
Device(config-keychain-key)# key-string Pl349&DaQ
Device(config-keychain-key)# send-life 01:00:00 1 jun 2003 02:00:00 1 aug 2003
Device(config-keychain-key)# exit
Device(config-keychain)# exit
Device(config)# key chain neighbor_Y
Device(config-keychain)# key 3
Device(config-keychain-key)# key-string *ZXFwR!03
Device(config-keychain-key)# send-life 02:00:00 1 jun 2003 02:00:00 1 aug 2003
Device(config-keychain-key)# exit
Device(config-keychain)# key 4
Device(config-keychain-key)# key-string UnGR8f&lOmY
Device(config-keychain-key)# send-life 01:00:00 1 jun 2003 02:00:00 1 aug 2003
Device(config-keychain-key)# exit
Device(config-keychain)# exit
Device(config)# key chain neighbor_Z
Device(config-keychain)# key 5
Device(config-keychain-key)# key-string P+T=77&/M
Device(config-keychain-key)# send-life 02:00:00 1 jun 2003 02:00:00 1 aug 2003
Device(config-keychain-key)# exit
Device(config-keychain)# key 6
Device(config-keychain-key)# key-string payattention2me
Device(config-keychain-key)# send-life 01:00:00 1 jun 2003 02:00:00 1 aug 2003
Device(config-keychain-key)# exit
Device(config-keychain)# exit
Device(config)# end
```

Note You can use the **key-config-key 1** *string* command to encrypt key chains for an interface, a neighbor, or globally.

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# ip access-list standard neighbor_V
Device(config-std-nacl)# permit 10.0.0.1
<------- physical address
Device(config-std-nacl)# permit 10.0.0.2
<------- physical address
Device(config-std-nacl)# permit 10.0.0.3
<------- router ID
Device(config-std-nacl)# exit
Device(config)# ip access-list standard neighbor_Y
Device(config-std-nacl)# permit 10.0.0.4
<------- physical address
Device(config-std-nacl)# permit 10.0.0.5
<------- physical address
Device(config-std-nacl)# permit 10.0.0.6
<------- router ID
```

```
Device(config-std-nacl)# exit
Device(config)# ip access-list standard neighbor_Z
Device(config-std-nacl)# permit 10.0.0.7
<------- physical address
Device(config-std-nacl)# permit 10.0.0.8
<------- physical address
Device(config-std-nacl)# permit 10.0.0.9
<------- router ID
Device(config-std-nacl)# exit
Device(config)# ip rsvp authentication neighbor access-list neighbor_V key-chain neighbor_V
Device(config)# ip rsvp authentication neighbor access-list neighbor_Y key-chain neighbor_Y
Device(config)# ip rsvp authentication neighbor access-list neighbor_Z key-chain neighbor_Z
Device(config)# ip rsvp authentication
Device(config)# end
```

Additional References

The following sections provide references related to the RSVP Message Authentication feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
RSVP commands: complete command syntax, command mode, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
QoS features including signaling, classification, and congestion management	"Quality of Service Overview" module
Inter-AS features including local policy support and per-neighbor keys authentication	"MPLS Traffic Engineering--Inter-AS-TE" module

Standards

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

MIBs

MIBs	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

RFCs	Title
RFC 1321	*The MD5 Message Digest Algorithm*
RFC 2104	*HMAC: Keyed-Hashing for Messaging Authentication*
RFC 2205	*Resource Reservation Protocol*
RFC 2209	*RSVP--Version 1 Message Processing Rules*
RFC 2401	*Security Architecture for the Internet Protocol*
RFC 2747	*RSVP Cryptographic Authentication*
RFC 3097	*RSVP Crytographic Authentication--Updated Message Type Value*
RFC 3174	*US Secure Hash Algorithm 1 (SHA1)*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for RSVP Message Authentication

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 6 Feature Information for RSVP Message Authentication

Feature Name	Releases	Feature Information
RSVP Message Authentication	Cisco IOS XE Release 3.8S	In Cisco IOS XE Release 3.8S, support was added for the Cisco ASR 903 Router.

Glossary

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.

DMZ--demilitarized zone. The neutral zone between public and corporate networks.

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

key --A data string that is combined with source data according to an algorithm to produce output that is unreadable until decrypted.

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

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 based on network layer information.

RSVP --Resource Reservation Protocol. A protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive.

security association --A block of memory used to hold all the information RSVP needs to authenticate RSVP signaling messages from a specific RSVP neighbor.

spoofing --The act of a packet illegally claiming to be from an address from which it was not actually sent. Spoofing is designed to foil network security mechanisms, such as filters and access lists.

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.

trusted neighbor --A device with authorized access to information.

RSVP Support for RTP Header Compression Phase 1

The Resource Reservation Protocol (RSVP) Support for Real-Time Transport Protocol (RTP) Header Compression, Phase 1 feature provides a method for decreasing a flow's reserved bandwidth requirements so that a physical link can accommodate more voice calls.

Feature Specifications for RSVP Support for RTP Header Compression, Phase 1

Feature History	
Release	Modification
12.2(15)T	This feature was introduced.
Supported Platforms	
For platforms supported in Cisco IOS Release 12.2(15)T, consult Cisco Feature Navigator.	

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.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release.

To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for RSVP Support for RTP Header Compression Phase 1

- Ensure that Real-Time Transport Protocol (RTP) or User Data Protocol (UDP) header compression is configured in the network.
- Ensure that RSVP is configured on two or more routers within the network before you can use this feature.

Restrictions for RSVP Support for RTP Header Compression Phase 1

- Routers do not generate compression hints, as described in RFC 3006, in this release.
- Signalled compression hints are not supported.
- Admission control with compression is limited to reservations with one sender per session.

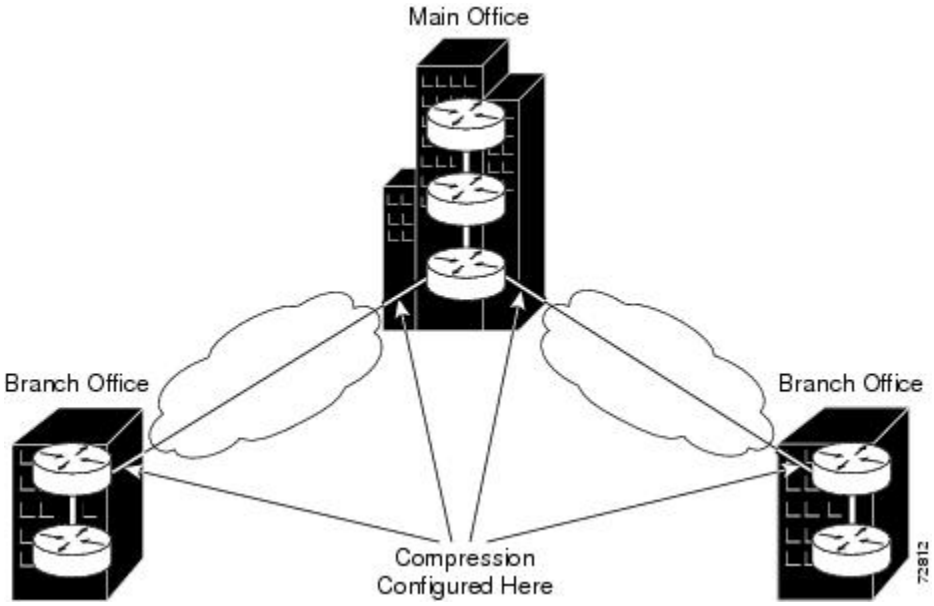
Information About RSVP Support for RTP Header Compression Phase 1

Feature Design of RSVP Support for RTP Header Compression Phase 1

Network administrators use RSVP with Voice over IP (VoIP) to provide quality of service (QoS) for voice traffic in a network. Because VoIP is a real-time application, network administrators often configure compression within the network to decrease bandwidth requirements. Typically, compression is configured on slow serial lines (see the figure below), where the savings from reduced bandwidth requirements outweigh the additional costs associated with the compression and decompression processes.

Note RTP header compression is supported by Cisco routers.

Figure 9 Configuring Compression



Originating applications know if their traffic is considered compressible, but not whether the network can actually compress the data. Additionally, compression may be enabled on some links along the call's path, but not on others. Consequently, the originating applications must advertise their traffic's uncompressed bandwidth requirements, and receiving applications must request reservation of the full amount of bandwidth. This causes routers whose RSVP implementations do not take compression into consideration to admit the same number of flows on a link running compression as on one that is not.

- Predicting Compression within Admission Control, page 133

Predicting Compression within Admission Control

Network administrators, especially those whose networks have very low speed links, may want RSVP to use their links as fully as possible. Such links typically have minimum acceptable outgoing committed information rate (minCIR) values between 19 and 30 kbps. Without accounting for compression, RSVP can admit (at most) one G.723 voice call onto the link, despite the link's capacity for two compressed calls. Under these circumstances, network administrators may be willing to sacrifice a QoS guarantee for the last call, if the flow is less compressible than predicted, in exchange for the ability to admit it.

In order to account for compression during admission control, routers use signalled Tspec information, as well as their awareness of the compression schemes running on the flow's outbound interfaces, to make local decisions as to how much bandwidth should actually be reserved for a flow. By reserving fewer resources than signalled by the receiver, RSVP can allow links to be more fully used.

Benefits of RSVP Support for RTP Header Compression Phase 1

Additional Calls Accommodated on the Same Link

The RSVP Support for RTP Header Compression, Phase 1 feature performs admission control based on compressed bandwidth so that additional voice calls can be accommodated on the same physical link.

How to Configure RSVP Support for RTP Header Compression Phase 1

Configuring RSVP Admission-Control Compression

Note RSVP predicted compression is enabled by default.

Perform this task to configure RSVP admission-control compression.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. interface [*type number*]
4. **ip rsvp admission-control compression predict** [*method* {**rtp** | **udp**} [*bytes-saved N*]]
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	interface [*type number*] **Example:** Router(config-if)# interface Serial3/0	Enters interface configuration mode. • The *type number* argument identifies the interface to be configured.
Step 4	**ip rsvp admission-control compression predict** [*method* {**rtp** | **udp**} [*bytes-saved N*]] **Example:** Router(config-if)# **ip rsvp admission-control compression predict method udp bytes-saved 16**	Configures RSVP admission-control compression prediction. • The optional method keyword allows you to select Real-Time Transport Protocol (rtp) or User Data Protocol (udp) for your compression scheme. • The optional bytes-saved N keyword allows you to configure the predicted number of bytes saved per packet when RSVP predicts that compression will occur using the specified method.
Step 5	**end** **Example:** Router(config-if)# **end**	Exits to privileged EXEC mode.

Verifying RSVP Support for RTP Header Compression Phase 1 Configuration

Perform this task to verify that the RSVP Support for RTP Header Compression, Phase 1 feature is functioning.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**show ip rsvp installed [detail]** **Example:** Router# show ip rsvp installed detail	Displays information about interfaces and their admitted reservations and the resources needed for a traffic control state block (TCSB) after taking compression into account. • The optional **detail** keyword displays the reservation's traffic parameters, downstream hop, compression, and resources used by RSVP to ensure QoS for this reservation.
Step 3	**show ip rsvp interface [interface-type interface-number] [detail]** **Example:** Router# show ip rsvp interface detail	Displays information about interfaces on which RSVP is enabled, including the current allocation budget and maximum available bandwidth and the RSVP bandwidth limit counter, taking compression into account. • The optional **detail** keyword displays RSVP parameters associated with an interface including bandwidth, admission control, and compression methods.

Examples

Sample Output for the show ip rsvp installed detail Command

In this example, the show ip rsvp installed detail command displays information, including the predicted compression method, its reserved context ID, and the observed bytes saved per packet average, for the admitted flowspec.

```
Router# show ip rsvp installed detail
RSVP: Ethernet2/1 has no installed reservations
RSVP: Serial3/0 has the following installed reservations
RSVP Reservation. Destination is 10.1.1.2. Source is 10.1.1.1,
  Protocol is UDP, Destination port is 18054, Source port is 19156
  Compression: (method rtp, context ID = 1, 37.98 bytes-saved/pkt avg)
  Admitted flowspec:
    Reserved bandwidth: 65600 bits/sec, Maximum burst: 328 bytes, Peak rate: 80K bits/sec
    Min Policed Unit: 164 bytes, Max Pkt Size: 164 bytes
  Admitted flowspec (as required if compression were not applied):
    Reserved bandwidth: 80K bits/sec, Maximum burst: 400 bytes, Peak rate: 80K bits/sec
    Min Policed Unit: 200 bytes, Max Pkt Size: 200 bytes
  Resource provider for this flow:
    WFQ on FR PVC dlci 101 on Se3/0:  PRIORITY queue 24.  Weight: 0, BW 66 kbps
  Conversation supports 1 reservations [0x1000405]
  Data given reserved service: 3963 packets (642085 bytes)
Data given best-effort service: 0 packets (0 bytes)
Reserved traffic classified for 80 seconds
  Long-term average bitrate (bits/sec): 64901 reserved, 0 best-effort
  Policy: INSTALL. Policy source(s): Default
```

Sample Output for the show ip rsvp interface detail Command

In this example, the show ip rsvp interface detail command displays the current interfaces and their configured compression parameters.

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


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

Troubleshooting Tips

The observed bytes-saved per packet value should not be less than the configured or default value. Otherwise, the flow may be experiencing degraded QoS. To avoid any QoS degradation for future flows, configure a lower bytes-saved per packet value.

Flows may achieve less compressibility than the default RSVP assumes for many reasons, including packets arriving out of order or having different differentiated services code point (DSCP) or precedence values, for example, due to policing upstream within the network.

If compression is enabled on a flow's interface, but the compression prediction was unsuccessful, the reason appears in the output instead of the reserved compression ID and the observed bytes-saved per packet.

Configuration Examples for RSVP Support for RTP Header Compression Phase 1

- Example RSVP Support for RTP Header Compression Phase 1, page 138

Example RSVP Support for RTP Header Compression Phase 1

The following sample configuration shows the compression prediction enabled for flows using UDP and disabled for flows using RTP:

```
Router# configure terminal

Router(config)# interface Serial3/0
Router(config-if)# ip rsvp admission-control compression predict method udp bytes-saved 16
Router(config-if)# no
ip rsvp admission-control compression predict method rtp
```

Use the **show run** command to display all the RSVP configured parameters:

```
Router# show run

2d18h: %SYS-5-CONFIG_I: Configured from console by console

Router# show run int se3/0
Building configuration...


Current configuration : 339 bytes
!
interface Serial3/0
 ip address 10.2.1.1 255.255.0.0
 fair-queue 64 256 8
 serial restart_delay 0
 clock rate 128000
 ip rtp header-compression
 ip rsvp bandwidth
 no ip rsvp admission-control compression predict method rtp
 ip rsvp admission-control compression predict method udp bytes-saved 16
end
```

Additional References

For additional information related to RSVP Support for RTP Header Compression, Phase 1, refer to the following references:

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Signalling	"Signalling Overview" module
RSVP	"Configuring RSVP" module
Header compression concepts and topics	"Header Compression" 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[1]	MIBs Link
• RFC 2206, RSVP Management Information Base using SMIv2	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register

RFCs

RFCs[2]	Title
RFC 2205	Resource Reservation Protocol (RSVP)
RFC 2508	Compressing IP/UDP/RTP Headers for Low-Speed Serial Links
RFC 3006	Integrated Services in the Presence of Compressible Flows

1 Not all supported MIBs are listed.

2 Not all supported RFCs are listed.

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for RSVP Support for RTP Header Compression

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 7 Feature Information for RSVP Support for RTP Header Compression

Feature Name	Releases	Feature Information
RSVP Support for RTP Header Compression	Cisco IOS XE Release 3.8S	In Cisco IOS XE Release 3.8S, support was added for the Cisco ASR 903 Router.

Glossary

admission control --The process in which a Resource Reservation Protocol (RSVP) reservation is accepted or rejected based on end-to-end available network resources.

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.

compression --The running of a data set through an algorithm that reduces the space required to store or the bandwidth required to transmit the data set.

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.

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

flowspec --In IPv6, the traffic parameters of a stream of IP packets between two applications.

G.723 --A compression technique that can be used for compressing speech or audio signal components at a very low bit rate as part of the H.324 family of standards. This codec has two bit rates associated with it: 5.3 and 6.3 kbps. The higher bit rate is based on ML-MLQ technology and provides a somewhat higher quality of sound. The lower bit rate is based on code excited linear prediction (CELP) compression and provides system designers with additional flexibility. Described in the ITU-T standard in its G-series recommendations.

minCIR --The minimum acceptable incoming or outgoing committed information rate (CIR) for a Frame Relay virtual circuit.

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

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

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 based on network layer information.

RSVP --Resource Reservation Protocol. A protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive.

RTP --Real-Time Transport Protocol. A protocol that is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP provides such services as payload type identification, sequence numbering, timestamping, and delivery monitoring to real-time applications.

TCSB --traffic control state block. A Resource Reservatiion Protocol (RSVP) state that associates reservations with their reserved resources required for admission control.

Tspec --Traffic specification. The traffic characteristics of a data stream from a sender or receiver (included in a Path message).

UDP--User Datagram Protocol. A connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.

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

RSVP Local Policy Support

Feature History

Release	Modification
12.2(13)T	This feature was introduced.

This document describes the Resource Reservation Protocol (RSVP) Local Policy Support feature in Cisco IOS Release 12.2(13)T. It identifies the supported platforms, provides configuration examples, and lists related Cisco IOS command line interface (CLI) commands.

This document includes the following sections:

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

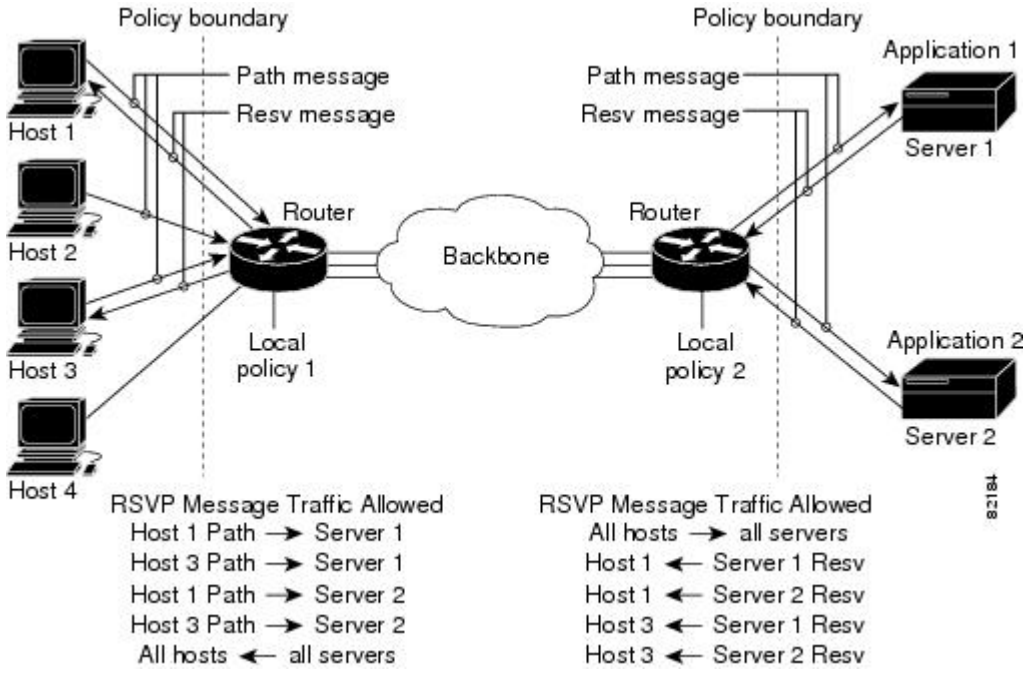
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Feature Overview

Network administrators need the ability to control the resources that RSVP reservations are allowed to use. For example, they may want to restrict RSVP reservations to certain subnets or from specific network servers.

The RSVP Local Policy Support feature allows network administrators to create default and access control list (ACL)-based policies. These policies, in turn, control how RSVP filters its signalling messages to allow or deny quality of service (QoS), as shown in the figure below, to networking applications based on the IP addresses of the requesting hosts.

Figure 10 RSVP Local Policy Configuration



- Benefits of RSVP Local Policy Support, page 144

Benefits of RSVP Local Policy Support

RSVP Reservation Control

Network administrators can restrict the source of RSVP reservations to specific endpoints.

RSVP Reservation Preemption

High priority reservations can preempt existing reservations if there is otherwise no bandwidth available for the new, high priority reservation.

Supported Platforms

For supported platforms in Cisco IOS Release 12.2(13)T, consult Cisco Feature Navigator.

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To get updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature

Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

http://www.cisco.com/register http://www.cisco.com/register

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

http://www.cisco.com/go/fn

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Prerequisites

RSVP must be configured on two or more routers or on one router and one host within the network before you can use the RSVP Local Policy Support feature.

Configuration Tasks

Creating an RSVP Local Policy

To create an RSVP local policy, use the following command beginning in global configuration mode:

Command	Purpose
Router(config)# **ip rsvp policy local {default | acl** acl [acl1...acl8]}	Creates a local policy to determine how RSVP resources are used in a network.

Specifying Command Line Interface Submodes

To specify CLI submodes, use the following command beginning in local policy mode:

Command	Purpose
Router(config-rsvp-policy-local)# {**accept** | **forward** } {**all** | **path** | **path-error** | **resv** | **resv-error** }	Defines the properties of the default or ACL-based local policy that you are creating.

See the **ip rsvp policy local** command in the Cisco IOS Quality of Service Solutions Command Reference for more detailed information on submodes.

Verifying RSVP Local Policy Configuration

To verify RSVP local policy configuration, use this procedure:

SUMMARY STEPS

1. Enter the **show ip rsvp policy**command to display policy-related information including local and default policies configured, Common Open Policy Service (COPS) servers configured, and the preemption parameter configured--enabled or disabled.
2. Enter the **show ip rsvp policy local detail** command to display information about the (selected) local policies currently configured.

DETAILED STEPS

Step 1 Enter the **show ip rsvp policy**command to display policy-related information including local and default policies configured, Common Open Policy Service (COPS) servers configured, and the preemption parameter configured--enabled or disabled.

Note There are no COPS servers configured in the following output.

Example:

```
Router# show ip rsvp policy
Local policy:
   A=Accept    F=Forward
   Path:-- Resv:-- PathErr:-- ResvErr:-- ACL:104
   Path:-- Resv:-- PathErr:-- ResvErr:-- ACL:None [Default policy]
```

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

Step 2 Enter the **show ip rsvp policy local detail** command to display information about the (selected) local policies currently configured.

Example:

```
Router# show ip rsvp policy local detail
Local policy for ACL(s): 104
   Preemption Priority: Start at 0, Hold at 0.
   Local Override: Disabled.
              Accept   Forward
   Path:       No       No
   Resv:       No       No
   PathError:  No       No
   ResvError:  No       No
Default local policy:
   Preemption Priority: Start at 0, Hold at 0.
   Local Override: Disabled.
              Accept   Forward
   Path:       No       No
   Resv:       No       No
   PathError:  No       No
   ResvError:  No       No
Generic policy settings:
   Default policy: Accept all
   Preemption:     Disabled
```

Monitoring and Maintaining RSVP Local Policy Support

To monitor and maintain the RSVP Local Policy Support feature, use the following commands in EXEC mode:

Command	Purpose
Router# **show ip rsvp policy**	Displays either the configured COPS servers or the local policies.
Router# **show ip rsvp policy local**	Displays selected local policies that have been configured.
Router# **show ip rsvp reservation detail**	Displays detailed RSVP-related receiver information currently in the database.
Router# **show ip rsvp sender detail**	Displays detailed RSVP-related sender information currently in the database.

Configuration Examples

Example RSVP Local Policy Support

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 only to reservation requests. 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.

In the following example, ACL 104 is configured for a local policy:

```
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)# end
```

In the following example, a default local policy is configured:

```
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)# end
```

Additional References

The following sections provide references related to the RSVP Local Policy Support feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Signalling Overview	"Signalling Overview" module
QoS configuration tasks related to RSVP	"Configuring RSVP" module
Conceptual information and configuration tasks for classifying network traffic.	"Classifying Network Traffic" module
Congestion Management	"Congestion Management Overview" module
Cisco United 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
None	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for RSVP Local Policy Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 8 Feature Information for RSVP Local Policy Support

Feature Name	Releases	Feature Information
RSVP Local Policy Support	Cisco IOS XE Release 3.8S	In Cisco IOS XE Release 3.8S, support was added for the Cisco ASR 903 Router.

Glossary

access control list-- See ACL.

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, though it may be used to provide a generic packet classification facility.

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

latency --The delay between the time a device receives a packet and the time that packet is forwarded out the destination port.

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

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.

port scanning --The act of systematically checking a computer's ports to find an access point.

Resource Reservation Protocol --See RSVP.

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

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 based on network layer information.

tunnel --A secure communications path between two peers, such as routers.

Voice over IP --See VoIP.

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