QoS: RSVP Configuration Guide, Cisco IOS XE Gibraltar 16.11.x

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS

CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E for Catalyst Switching and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Feature Information

Use Cisco Feature Navigator to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- Cisco IOS Command References, All Releases

Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

CHAPTER 2

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.

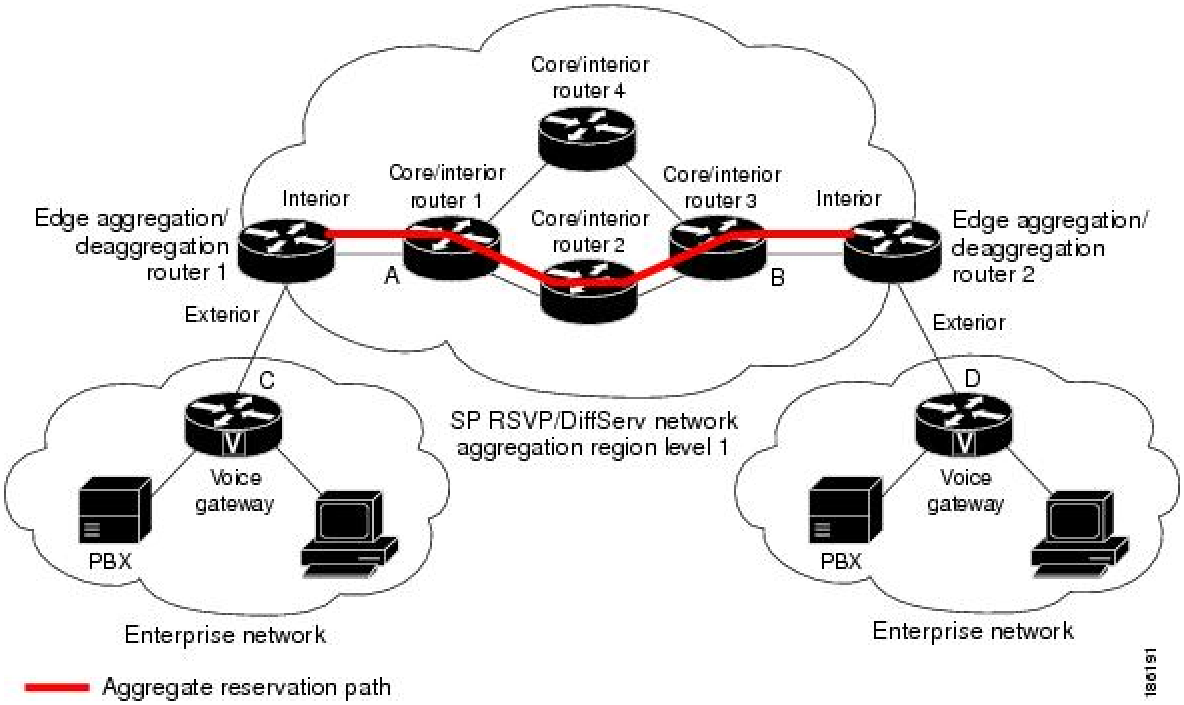
When a large number of small reservations are established, the resources required for setting and maintaining these reservations may exceed a node's capacity to the point where the node's performance is significantly degraded or it becomes unusable. The RSVP Aggregation feature addresses this scalability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

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

Perform this task to enable RSVP on all the interfaces along the path from the sender to the receiver.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip routing**
4. **ip vrf** *vrf-name*
5. **exit**
6. **interface** *type number*
7. **ip vrf forwarding** *vrf-name*
8. **ip rsvp bandwidth** [*interface-kbps*] [*single-flow-kbps*]
9. Repeat the previous step for each interface that you want to enable.
10. **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 routing** **Example:** `Device(config)# ip routing`	Enables IP routing.
Step 4	**ip vrf** *vrf-name* **Example:** `Device(config)# ip vrf vrf1`	Defines a VRF instance and enters VRF configuration mode.
Step 5	**exit** **Example:** `Device(config-vrf)# exit`	Exits VRF configuration mode and enters global configuration mode.
Step 6	**interface** *type number* **Example:** `Device(config)# interface Ethernet0/0`	Configures the interface type and enters interface configuration mode.
Step 7	**ip vrf forwarding** *vrf-name* **Example:** `Device(config-if)# ip vrf forwarding vrf1`	Associates a VRF instance with an interface or subinterface.
Step 8	**ip rsvp bandwidth** [*interface-kbps*] [*single-flow-kbps*] **Example:** `Device(config-if)# ip rsvp bandwidth 1158 100`	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 9	Repeat the previous step for each interface that you want to enable.	--

	Command or Action	Purpose

Step 10	**end**
	Example:
	`Device(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.
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.

	Command or Action	Purpose
		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.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
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

To configure class and policy maps, use the following commands, beginning in global configuration mode:

SUMMARY STEPS

1. Device(config)# **class-map** *class-map-name*
2. Device(config)# **policy-map** *policy-map-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	Device(config)# **class-map** *class-map-name*	Specifies the name of the class for which you want to create or modify class map match criteria.
Step 2	Device(config)# **policy-map** *policy-map-name*	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.

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*.

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.
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.

Before you begin

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.
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.
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:**	(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.

	Command or Action	Purpose
	`Router(config-rsvp-policy-local)# forward all`	

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:**	(Optional) Displays RSVP summary aggregation information. • The optional keywords and arguments display additional information.

	Command or Action	Purpose
	`Device# show ip rsvp aggregation ip`	
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.
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:**	(Optional) Exits privileged EXEC mode and returns to user EXEC mode.

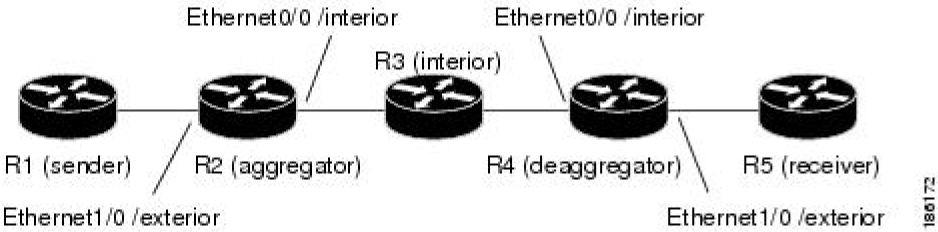
	Command or Action	Purpose
	`Device# end`	

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 Application ID Support feature.

Related Documents

Related Topic	Document Title
QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
QoS configuration tasks related to RSVP	"Configuring RSVP" module
Cisco 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
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

Standards

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

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2205	Resource ReSerVation Protocol (RSVP)
RFC 2872	Application and Sub Application Identity Policy Element for Use with RSVP
RFC 3181	Signaled Preemption Priority Policy Element
RFC 3182	Identity Representation for RSVP

Technical Assistance

Description	Link
The Cisco Support 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.

CHAPTER 3

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

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.
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

	Command or Action	Purpose
		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

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.

	Command or Action	Purpose
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.

	Command or Action	Purpose
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.
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, on page 35.

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:**	Exits global configuration mode and returns to privileged EXEC mode.

	Command or Action	Purpose
	`Router(config)# end`	

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, on page 48for 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.
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:**	Exits privileged EXEC mode and returns to user EXEC mode.

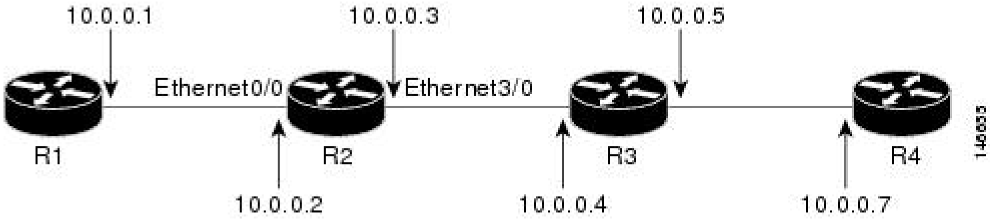
	Command or Action	Purpose
	Router# end	

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
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.

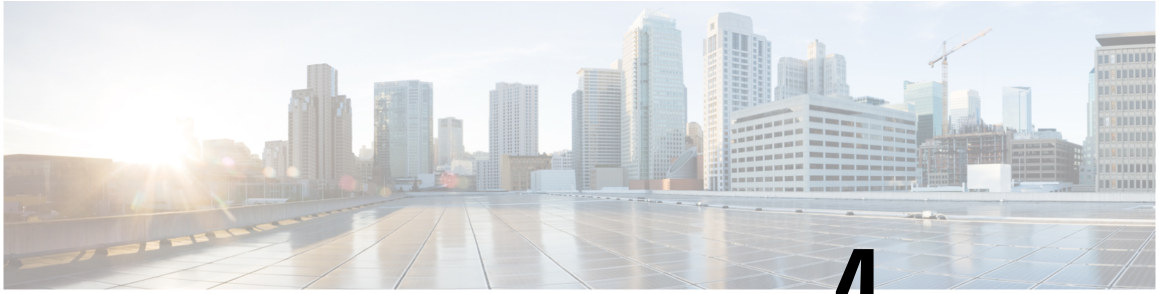
Glossary

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.

RSVP Agent --Implements a Resource Reservation Protocol (RSVP) agent on Cisco IOS voice gateways that support Unified CM.

Unified Communcations Manager (CM)--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.



CHAPTER 4

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

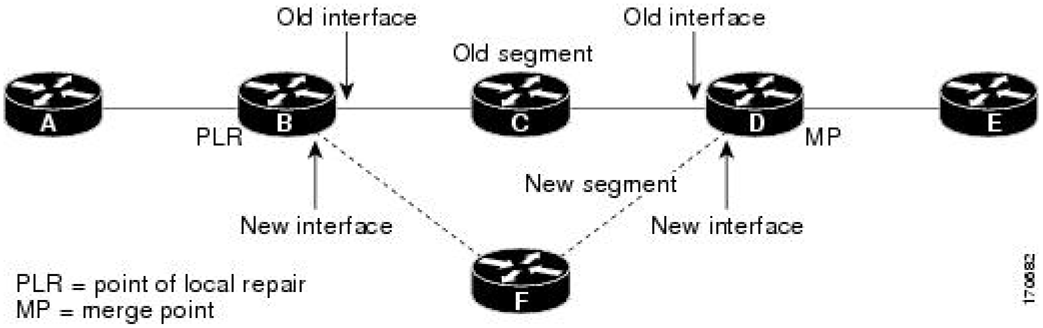
RSVP FLR provides for dynamic adaptation when routing changes occur in global or VRF routing domains. When a route changes, the next PATH and RESV message refreshes establish path and reservation states along the new route. Depending on the configured refresh interval, this reroute happens in tens of 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

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.
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:**	(Optional) Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Router(config-if)# end`	

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.
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.
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.
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 gigabitethernet 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 Control Plane DSCP Support for RSVP feature.

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
RSVP Commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Quality of service overview	"Quality of Service Overview" module

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
RFC 2206 (RSVP Management Information Base using SMIv2)	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*

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.

CHAPTER 5

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

Enabling 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`	Configures the interface type and enters interface configuration mode.
Step 4	**ip rsvp bandwidth** [*interface-kbps*][*single-flow-kbps*] **Example:** `Device(config-if)# ip rsvp bandwidth 7500`	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:
	`Device(config-if)# end`
		(Optional) Returns to privileged EXEC mode.

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

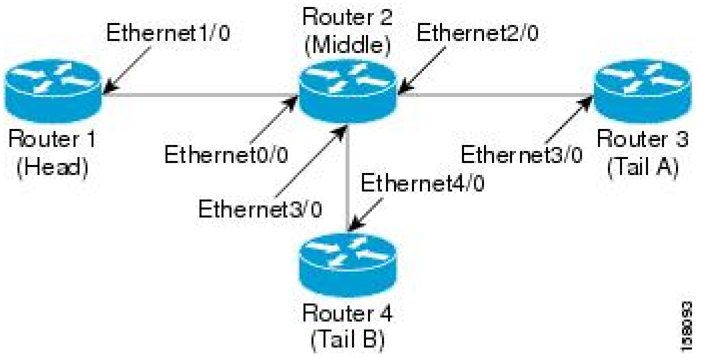
	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Optional) Enables privileged EXEC mode. - Enter your password if prompted. **Note** Omit this step if you are using the **show** commands in user EXEC mode.
Step 2	**show ip rsvp listeners** [*ip-address*| **any**] [**udp** | **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.
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.

CHAPTER 6

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.

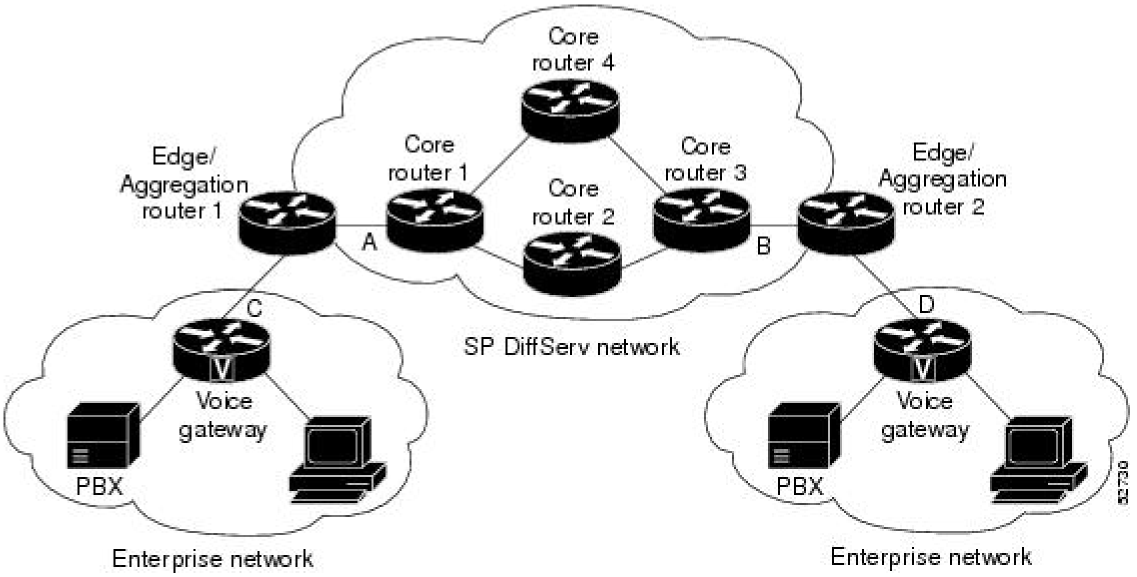
Information About RSVP Scalability Enhancements

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

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

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.

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.
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.

CHAPTER 7

Control Plane DSCP Support for RSVP

This document describes the Cisco Control Plane DSCP Support for RSVP feature.

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 Control Plane DSCP Support for RSVP

The network must support Resource Reservation Protocol (RSVP) before the Control Plane DSCP Support for RSVP feature is enabled.

Restrictions for Control Plane DSCP Support for RSVP

Control plane DSCP support for RSVP can be configured on interfaces and subinterfaces only. It affects all RSVP messages that are sent out on the interface or that are present on any logical circuit of the interface, including subinterfaces, permanent virtual circuits (PVCs), and switched virtual circuits (SVCs).

Information About Control Plane DSCP Support for RSVP

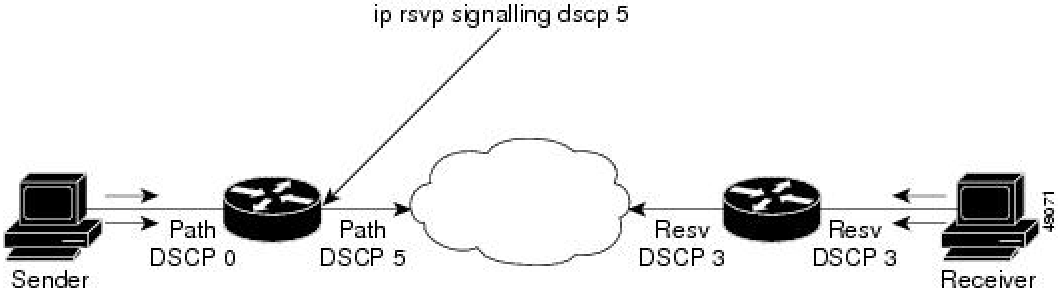
Typically, networks operate on a best-effort delivery basis, which means that all traffic has equal priority and an equal chance of being delivered in a timely manner. When congestion occurs, all traffic has an equal chance of being dropped.

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

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

The figure below shows a path message originating from a sender with a DSCP value of 0 (the default), which is changed ito 5 to give the message a higher priority, and it shows a reservation (resv) message originating from a receiver with a DSCP of 3.

Figure 7: Control Plane DSCP Support for RSVP



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

Benefits of Control Plane DSCP Support for RSVP

Faster Call Setup Time

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

Improved Message Delivery

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

Faster Recovery After Failure Conditions

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

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

How to Configure Control Plane DSCP Support for RSVP

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*]

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 gigbitEthernet 0/0/0`	Enters interface configuration mode for a specific interface.
Step 4	**ip rsvp bandwidth** [*interface-kbps*] [*single-flow-kbps*] **Example:** `Router(config-if)# ip rsvp bandwidth 23 43`	Enables RSVP on an interface.

Specifying the DSCP

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type slot* / *subslot* / *port*
4. **ip rsvp signalling dscp** *value*

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 gigbitEthernet 0/1/0`	Enters interface configuration mode for a specific interface.
Step 4	**ip rsvp signalling dscp** *value* **Example:** `Router(config-if)# ip rsvp signalling dscp 10`	Specifies the DSCP to be used on all RSVP messages that are transmitted on an interface.

Verifying Control Plane DSCP Support for RSVP Configuration

SUMMARY STEPS

1. Enter the **show running-config** command to verify the configuration.
2. Enter the **show ip rsvp interface detail**command to display RSVP-related interface information. The following is sample output from the **show ip rsvp interface detail**command. Interfaces that are not configured for DSCP do not show the DSCP value, which is 0 by default.

DETAILED STEPS

Step 1 Enter the **show running-config** command to verify the configuration.

Step 2 Enter the **show ip rsvp interface detail**command to display RSVP-related interface information. The following is sample output from the **show ip rsvp interface detail**command. Interfaces that are not configured for DSCP do not show the DSCP value, which is 0 by default.

Example:

```
Router# show
 ip rsvp interface detail
Gi0/0/0:
   RSVP: Disabled
   Interface State: N/A
   Bandwidth:
     Curr allocated: 0 bits/sec
     Max. allowed (total): 0 bits/sec
     Max. allowed (per flow): 0 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
   Signalling:
     DSCP value used in RSVP msgs: 0x17
     Number of refresh intervals to enforce blockade state: 4
   Authentication: disabled
     Key chain:   <none>
     Type:        md5
     Window size: 1
     Challenge:   disabled
   FRR Extension:
     Backup Path: Not Configured
   BFD Extension:
     State: Disabled
     Interval: Not Configured
   RSVP Hello Extension:
     State: Disabled
   RFC 3175 Aggregation: Disabled
     Role: exterior.
```

Configuration Examples for Control Plane DSCP Support for RSVP

The following example shows how to enable RSVP on an interface, specify the DSCP, and verify the control plane DSCP support for RSVP.

```
Router> enable
Router# config terminal
Router(config)# interface gigabitethernet 3/1/0
Router(config-if)# ip rsvp bandwidth 7500 7500
Router(config-if)# ip rsvp signalling dscp 48
Router(config-if)# end
```

The following example shows how to display the RSVP-related information.

```
Router# show running-config interface gigabitEthernet 0/0/0
interface gigabitEthernet 0/0/0
ip address 10.10.10.1 255.255.255.0
```

```
fair-queue 64 256 235
ip rsvp signalling dscp 48
ip rsvp bandwidth 7500 7500
```

Additional References

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

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
RSVP Commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples	*Cisco IOS Quality of Service Solutions Command Reference*
Quality of service overview	"Quality of Service Overview" module

Standards

Standard	Title
None	--

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 Control Plane DSCP Support for RSVP

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 Control Plane DSCP Support for RSVP

Feature Name	Releases	Feature Information
Control Plane DSCP Support for RSVP	Cisco IOS XE Release 2.6	The Control Plane DSCP Support for RSVP feature allows you to set the priority value in ToS byte or DiffServ field in the IP header for RSVP messages. The following commands were introduced or modified: **ip rsvp signalling dscp**, **show ip rsvp interface**.

Glossary

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 that is 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.

IP precedence --The three most significant bits of the 1-byte type of service (ToS) field. IP precedence values range between 0 for low priority and 7 for high priority.

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

marking --The process of setting a Layer 3 DSCP value in a packet.

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.

ToS --type of service. An 8-bit value in the IP header field.

type of service --See ToS.

Voice over IP --See VoIP.

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

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

WRED --weighted random early detection. A congestion avoidance mechanism that slows traffic by randomly dropping packets when there is congestion.

CHAPTER 8

MPLS TE - Tunnel-Based Admission Control

The MPLS TE--Tunnel-Based Admission Control (TBAC) feature enables classic Resource Reservation Protocol (RSVP) unicast reservations that are traveling across a Multiprotocol Label Switching traffic engineering (MPLS TE) core to be aggregated over an MPLS TE tunnel.

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 MPLS TE - Tunnel-Based Admission Control

- You must configure an MPLS TE tunnel in the network.
- You must configure RSVP on one or more interfaces on at least two neighboring routers that share a link within the network.

Restrictions for MPLS TE - Tunnel-Based Admission Control

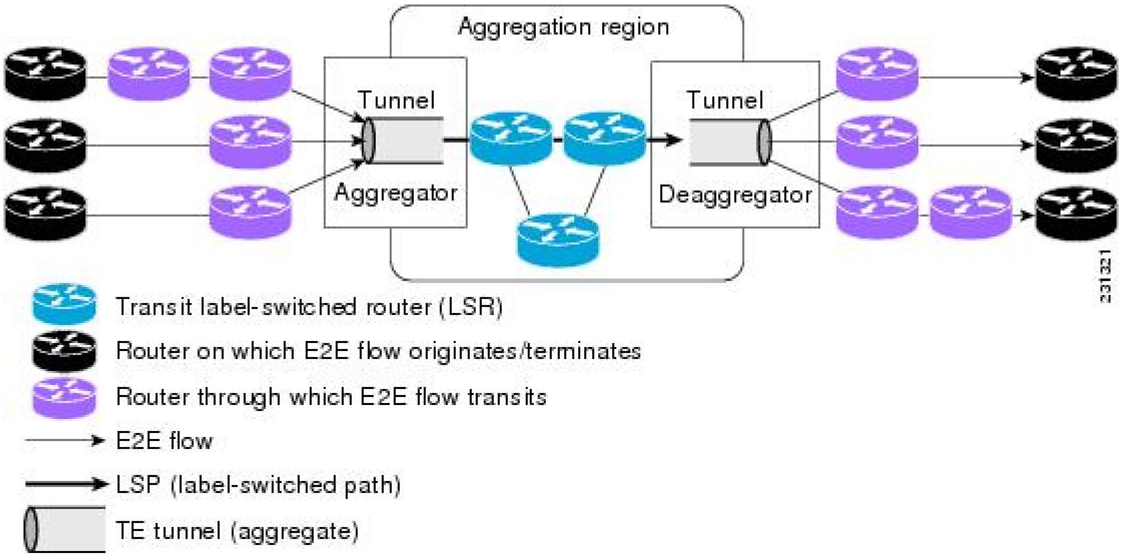
- Only IPv4 unicast RSVP flows are supported.
- Primary, one-hop tunnels are not supported. The TE tunnel cannot be a member of a class-based tunnel selection (CBTS) bundle.
- Multitopology Routing (MTR) is not supported.
- Only preestablished aggregates are supported. They can be configured statically or dynamically using command-line interface (CLI) commands.

Information About MPLS TE - Tunnel-Based Admission Control

Feature Overview of MPLS TE - Tunnel-Based Admission Control

TBAC aggregates reservations from multiple, classic RSVP sessions over different forms of tunneling technologies that include MPLS TE tunnels, which act as aggregate reservations in the core. The figure below gives an overview of TBAC.

Figure 8: TBAC Overview


Aggregation region
Tunnel
Aggregator
Tunnel
Deaggregator
231321
Transit label-switched router (LSR)
Router on which E2E flow originates/terminates
Router through which E2E flow transits
E2E flow
LSP (label-switched path)
TE tunnel (aggregate)

The figure below shows three RSVP end-to-end (E2E) flows that originate at routers on the far left, and terminate on routers at the far right. These flows are classic RSVP unicast flows, meaning that RSVP is maintaining a state for each flow. There is nothing special about these flows, except that along their path, these flows encounter an MPLS-TE core, where there is a desire to avoid creating a per-flow RSVP state.

When the E2E flows reach the edge of the MPLS-TE core, they are aggregated onto a TE tunnel. This means that when transiting through the MPLS-TE core, their state is represented by a single state; the TE tunnel is within the aggregation region, and their packets are forwarded (label-switched) by the TE tunnel. For example, if 100 E2E flows traverse the same aggregator and deaggregator, rather than creating 100 RSVP states (PATH and RESV messages) within the aggregation region, a single RSVP-TE state is created, that of the aggregate, which is the TE tunnel, to allocate and maintain the resources used by the 100 E2E flows. In particular, the bandwidth consumed by E2E flows within the core is allocated and maintained in aggregate by the TE tunnel. The bandwidth of each E2E flow is normally admitted into the TE tunnel at the headend, just as any E2E flow's bandwidth is admitted onto an outbound link in the absence of aggregation.

Benefits of MPLS TE - Tunnel-Based Admission Control

To understand the benefits of TBAC, you should be familiar with how Call Admission Control (CAC) works for RSVP and Quality of Service (QoS).

Cost Effective

Real-time traffic is very sensitive to loss and delay. CAC avoids QoS degradation for real-time traffic because CAC ensures that the accepted load always matches the current network capacity. As a result, you do not have to overprovision the network to compensate for absolute worst peak traffic or for reduced capacity in case of failure.

Improved Accuracy

CAC uses RSVP signaling, which follows the same path as the real-time flow, and routers make a CAC decision at every hop. This ensures that the CAC decision is very accurate and dynamically adjusts to the current conditions such as a reroute or an additional link. Also, RSVP provides an explicit CAC response (admitted or rejected) to the application, so that the application can react appropriately and fast; for example, sending a busy signal for a voice call, rerouting the voice call on an alternate VoIP route, or displaying a message for video on demand.

RSVP and MPLS TE Combined

TBAC allows you to combine the benefits of RSVP with those of MPLS TE. Specifically, you can use MPLS TE inside the network to ensure that the transported traffic can take advantage of Fast Reroute protection (50-millisecond restoration), Constraint Based Routing (CBR), and aggregate bandwidth reservation.

Seamless Deployment

TBAC allows you to deploy IPv4 RSVP without any impact on the MPLS part of the network because IPv4 RSVP is effectively tunneled inside MPLS TE tunnels that operate unchanged as per regular RSVP TE. No upgrade or additional protocol is needed in the MPLS core.

Enhanced Scaling Capability

TBAC aggregates multiple IPv4 RSVP reservations ingressing from the same MPLS TE headend router into a single MPLS TE tunnel and egressing from the same MPLS TE tailend router.

How to Configure MPLS TE - Tunnel-Based Admission Control

Enabling RSVP QoS

Perform this task to enable RSVP QoS globally on a device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp qos**
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 qos** **Example:** `Device(config)# ip rsvp qos`	Enables RSVP QoS globally on a device.

Step 4	**end**
	Example:
	`Device(config)# end`
		(Optional) Returns to privileged EXEC mode.

Enabling MPLS TE

Perform this task to enable MPLS TE. This task enables MPLS TE globally on a router that is running RSVP QoS.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mpls traffic-eng tunnels**
4. **end**

DETAILED STEPS

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

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**mpls traffic-eng tunnels** **Example:** `Router(config)# mpls traffic-eng tunnels`	Enables MPLS TE globally on a router.

Step 4	**end**
	Example:
	`Router(config)# end`
		(Optional) Returns to privileged EXEC mode.

Configuring an MPLS TE Tunnel Interface

Before you begin

You must configure an MPLS-TE tunnel in your network before you can proceed. For detailed information, see the "MPLS Traffic Engineering (TE)--Automatic Bandwidth Adjustment for TE Tunnels" module.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
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	**interface tunnel** *number* **Example:** `Router(config)# interface tunnel 1`	Specifies a tunnel interface and enters interface configuration mode.

Step 4	**end**
	Example:
	`Router(config-if)# end`
		(Optional) Returns to privileged EXEC mode.

Configuring RSVP Bandwidth on an MPLS TE Tunnel Interface

Perform this task to configure RSVP bandwidth on the MPLS TE tunnel interface that you are using for the aggregation.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** `Router(config)# interface tunnel 1`	Specifies a tunnel interface and enters interface configuration mode.
Step 4	**ip rsvp bandwidth** [*interface-kbps*] [*single-flow-kbps*] **Example:** `Router(config-if)# ip rsvp bandwidth 7500`	Enables RSVP bandwidth on an interface. • The optional *interface-kbps* and *single-flow-kbps* arguments specify the amount of bandwidth that can

	Command or Action	Purpose
		be allocated by RSVP flows or to a single flow, respectively. Values are from 1 to 10000000. **Note** You must enter a value for the *interface-kbps*argument on a tunnel interface.

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

Verifying the TBAC Configuration

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

SUMMARY STEPS

1. **enable**
2. **show ip rsvp**
3. **show ip rsvp reservation** [**detail**] [**filter** [**destination** {*ip-address* | *hostname*}] [**dst-port** *port-number*] [**source** {*ip-address*s | *hostname*}] [**src-port** *port-number*]]
4. **show ip rsvp sender** [**detail**] [**filter** [**destination** *ip-address* | *hostname*] [**dst-port** *port-number*] [**source** *ip-address* | *hostname*] [**src-port** *port-number*]]
5. **show mpls traffic-eng link-management bandwidth-allocation** [**summary**] [*interface-type interface-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.
Step 2	**show ip rsvp** **Example:** `Router# show ip rsvp`	Displays specific information for RSVP categories.

	Command or Action	Purpose
Step 3	**show ip rsvp reservation** [**detail**] [**filter** [**destination** {*ip-address* | *hostname*}] [**dst-port** *port-number*] [**source** {*ip-addres*s | *hostname*}] [**src-port** *port-number*]] **Example:** `Router# show ip rsvp reservation detail`	Displays RSVP-related receiver information currently in the database.
Step 4	**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.
Step 5	**show mpls traffic-eng link-management bandwidth-allocation** [**summary**] [*interface-type interface-number*] **Example:** `Router# show mpls traffic-eng link-management bandwidth-allocation`	Displays current local link information.
Step 6	**exit** **Example:** `Router# exit`	(Optional) Exits privileged EXEC mode and returns to user EXEC mode.

Configuration Examples for MPLS TE - Tunnel-Based Admission Control

Example Configuring TBAC

Note You must have an MPLS TE tunnel already configured in your network. For detailed information, see the "MPLS Traffic Engineering (TE)--Automatic Bandwidth Adjustment for TE Tunnels" module.

The following example enables RSVP and MPLS TE globally on a router and then configures a tunnel interface and bandwidth of 7500 kbps on the tunnel interface traversed by the RSVP flows:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# ip rsvp qos
Router(config)# mpls traffic-eng tunnels

Router(config)# interface tunnel 1

Router(config-if)# ip rsvp bandwidth 7500

Router(config-if)# end
```

Example Configuring RSVP Local Policy on a Tunnel Interface

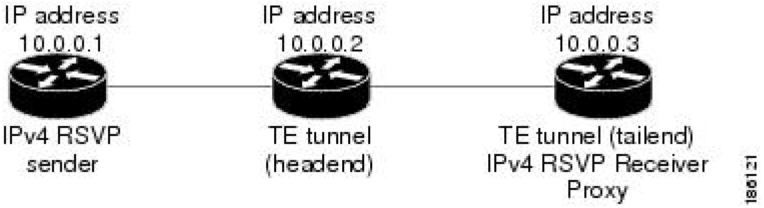
The following example configures an RSVP default local policy on a tunnel interface:

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

Router(config)# interface tunnel 1

Router(config-if)# ip rsvp policy local default

Router(config-rsvp-local-if-policy)# max bandwidth single 10

Router(config-rsvp-local-if-policy)# forward all

Router(config-rsvp-local-if-policy)# end
```

Example Verifying the TBAC Configuration

The figure below shows a network in which TBAC is configured.

Figure 9: Sample TBAC Network



The following example verifies that RSVP and MPLS TE are enabled and coexist on the headend router (10.0.0.2 in the figure above):

```
Router# show ip rsvp
RSVP: enabled (on 3 interface(s))
  RSVP QoS enabled <-------
  MPLS/TE signalling enabled <------
Signalling:
   Refresh interval (msec): 30000
   Refresh misses: 4
.
```

```
.
.
```

The following example verifies that RSVP and MPLS TE are enabled and coexist on the tailend router (10.0.0.3 in the figure above):

```
Router# show ip rsvp
RSVP: enabled (on 3 interface(s))
  RSVP QoS enabled <-------
  MPLS/TE signalling enabled <------
Signalling:
   Refresh interval (msec): 30000
   Refresh misses: 4
.
.
.
```

The following examples verify that an IPv4 flow is traveling through a TE tunnel (a label-switched path [LSP]) on the headend router (10.0.0.2 in the figure above):

```
Router# show ip rsvp sender
To              From          Pro DPort Sport Prev Hop       I/F      BPS
10.0.0.3        10.0.0.1      UDP 2     2     10.0.0.1       Et0/0    10K <-- IPv4 flow
10.0.0.3        10.0.0.2      0   1     11    none           none     100K <-- TE tunnel
```

```
Router# show ip rsvp reservation
To            From        Pro DPort Sport Next Hop     I/F    Fi Serv BPS
10.0.0.3      10.0.0.1    UDP 2     2     10.0.0.3     Tu1    SE RATE 10K <-- IPv4 flow
10.0.0.3      10.0.0.2    0   1     11    10.1.0.2     Et1/0  SE LOAD 100K <-- TE tunnel
```

The following examples verify that an IPv4 flow is traveling through a TE tunnel (LSP) on the tailend router (10.0.0.3 in the figure above):

```
Router# show ip rsvp sender
To              From          Pro DPort Sport Prev Hop       I/F      BPS
10.0.0.3        10.0.0.1      UDP 2     2     10.0.0.2       Et1/0    10K <-- IPv4 flow
10.0.0.3        10.0.0.2      0   1     11    10.1.0.1       Et1/0    100K <-- TE tunnel
```

```
Router# show ip rsvp reservation
To            From          Pro DPort Sport Next Hop   I/F    Fi Serv BPS
10.0.0.3      10.0.0.1      UDP 2     2     none       none   SE RATE 10K <-- IPv4 flow
10.0.0.3      10.0.0.2      0   1     11    none       none   SE LOAD 100K <-- TE tunnel
```

The following examples display detailed information about the IPv4 flow and the TE tunnel (LSP) on the headend router (10.0.0.2 in the figure above):

```
Router# show ip rsvp sender detail
PATH: <----------------------------------------------- IPv4 flow information begins here.
  Destination 10.0.0.3, Protocol_Id 17, Don't Police , DstPort 2
  Sender address: 10.0.0.1, port: 2
  Path refreshes:
    arriving: from PHOP 10.0.0.10 on Et0/0 every 30000 msecs. Timeout in 189 sec
  Traffic params - Rate: 10K bits/sec, Max. burst: 10K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
  Path ID handle: 02000412.
  Incoming policy: Accepted. Policy source(s): Default
  Status:
  Output on Tunnel1, out of band. Policy status: Forwarding. Handle: 0800040E <--- TE tunnel
 verified
    Policy source(s): Default
  Path FLR: Never repaired
PATH: <------------------------------------------------ TE tunnel information begins here.
  Tun Dest:   10.0.0.3  Tun ID: 1  Ext Tun ID: 10.0.0.2
  Tun Sender: 10.0.0.2  LSP ID: 11
  Path refreshes:
    sent:     to   NHOP 10.1.0.2 on GigabitEthernet1/0/0
   .
   .

.


Router# show ip rsvp reservation detail
RSVP Reservation. Destination is 10.0.0.3, Source is 10.0.0.1,<--- IPv4 flow information
begins here.
  Protocol is UDP, Destination port is 2, Source port is 2
  Next Hop: 10.0.0.3 on Tunnel1, out of band <-------------------- TE tunnel verified
  Reservation Style is Shared-Explicit, QoS Service is Guaranteed-Rate
   .
   .
   .
Reservation: <--------------------------------------- TE Tunnel information begins here.
  Tun Dest:   10.0.0.3  Tun ID: 1  Ext Tun ID: 10.0.0.2
  Tun Sender: 10.0.0.2  LSP ID: 11
  Next Hop: 10.1.0.2 on GigabitEthernet1/0/0
  Label: 0 (outgoing)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
   .
   .
   .


Router# show ip rsvp installed detail

RSVP: GigabitEthernet0/0/0 has no installed reservations

RSVP: GigabitEthernet1/0/0 has the following installed reservations
RSVP Reservation. Destination is 10.0.0.3. Source is 10.0.0.2,
  Protocol is 0  , Destination port is 1, Source port is 11
  Traffic Control ID handle: 03000405
  Created: 04:46:55 EST Fri Oct 26 2007 <------ IPv4 flow information
  Admitted flowspec:
    Reserved bandwidth: 100K bits/sec, Maximum burst: 1K bytes, Peak rate: 100K bits/sec
    Min Policed Unit: 0 bytes, Max Pkt Size: 1500 bytes
  Resource provider for this flow: None
   .
   .
   .
RSVP: Tunnel1 has the following installed reservations <------ TE tunnel verified
RSVP Reservation. Destination is 10.0.0.3. Source is 10.0.0.1,
  Protocol is UDP, Destination port is 2, Source port is 2
  Traffic Control ID handle: 01000415
  Created: 04:57:07 EST Fri Oct 26 2007 <----- IPv4 flow information
  Admitted flowspec:
    Reserved bandwidth: 10K bits/sec, Maximum burst: 10K bytes, Peak rate: 10K bits/sec
    Min Policed Unit: 0 bytes, Max Pkt Size: 0 bytes
  Resource provider for this flow: None
   .
   .
   .


Router# show ip rsvp interface detail
```

```
 Et0/0:
   RSVP: Enabled
   Interface State: Up
   Bandwidth:
     Curr allocated: 0 bits/sec
     Max. allowed (total): 3M bits/sec
     Max. allowed (per flow): 3M bits/sec
   .
   .
   .
 Et1/0:
   RSVP: Enabled
   Interface State: Up
   Bandwidth:
     Curr allocated: 0 bits/sec
     Max. allowed (total): 3M bits/sec
     Max. allowed (per flow): 3M bits/sec
   .
   .
   .
Tu1: <--------------------------------- TE tunnel information begins here.
   RSVP: Enabled
   RSVP aggregation over MPLS TE: Enabled
   Interface State: Up
   Bandwidth:
     Curr allocated: 20K bits/sec
     Max. allowed (total): 3M bits/sec
     Max. allowed (per flow): 3M bits/sec
   .
   .
   .
```

The following examples display detailed information about the IPv4 flow and the TE tunnel (LSP) on the tailend router (10.0.0.3 in the figure above):

```
Router# show ip rsvp sender detail
PATH: <----------------------------------------------- IPv4 flow information begins here.
  Destination 10.0.0.3, Protocol_Id 17, Don't Police , DstPort 2
  Sender address: 10.0.0.1, port: 2
  Path refreshes:
    arriving: from PHOP 10.0.0.2 on Et1/0 every 30000 msecs, out of band. Timeout in 188
sec
  Traffic params - Rate: 10K bits/sec, Max. burst: 10K bytes
    Min Policed Unit: 0 bytes, Max Pkt Size 2147483647 bytes
   .
   .
   .
PATH: <------------------------------------------------ TE tunnel information begins here.
  Tun Dest:   10.0.0.3  Tun ID: 1  Ext Tun ID: 10.0.0.2
  Tun Sender: 10.0.0.2  LSP ID: 11
  Path refreshes:
    arriving: from PHOP 10.1.0.1 on Et1/0 every 30000 msecs. Timeout in 202 sec
   .
   .
   .


Router# show ip rsvp reservation detail

RSVP Reservation. Destination is 10.0.0.3, Source is 10.0.0.1, <--- IPv4 flow information
begins here.
  Protocol is UDP, Destination port is 2, Source port is 2
  Next Hop: none
  Reservation Style is Shared-Explicit, QoS Service is Guaranteed-Rate
```

```
   .
   .
   .

Reservation: <--------------------------------------- TE tunnel information begins here.
  Tun Dest:   10.0.0.3  Tun ID: 1  Ext Tun ID: 10.0.0.2
  Tun Sender: 10.0.0.2  LSP ID: 11
  Next Hop: none
  Label: 1 (outgoing)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
   .
   .
   .


Router# show ip rsvp request detail

RSVP Reservation. Destination is 10.0.0.3, Source is 10.0.0.1,
  Protocol is UDP, Destination port is 2, Source port is 2
  Prev Hop: 10.0.0.2 on GigabitEthernet1/0/0, out of band <-------------- TE tunnel verified

  Reservation Style is Shared-Explicit, QoS Service is Guaranteed-Rate
  Average Bitrate is 10K bits/sec, Maximum Burst is 10K bytes
   .
   .
   .

Request: <------------------------------------ TE tunnel information begins here.
  Tun Dest:   10.0.0.3  Tun ID: 1  Ext Tun ID: 10.0.0.2
  Tun Sender: 10.0.0.2  LSP ID: 11
  Prev Hop: 10.1.0.1 on GigabitEthernet1/0/0
  Label: 0 (incoming)
  Reservation Style is Shared-Explicit, QoS Service is Controlled-Load
   .
   .
   .
```

Example Verifying the RSVP Local Policy Configuration

The following example verifies that a default local policy has been configured on tunnel interface 1:

```
Device# show run interface tunnnel 1
Building configuration...

Current configuration : 419 bytes
!
interface Tunnel1
 bandwidth 3000
 ip unnumbered Loopback0
 tunnel destination 10.0.0.3
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 1 1
 tunnel mpls traffic-eng bandwidth 100
 tunnel mpls traffic-eng path-option 1 dynamic
 tunnel mpls traffic-eng fast-reroute
 ip rsvp policy local default <---------------- Local policy information begins here.
  max bandwidth single 10
  forward all
 ip rsvp bandwidth 3000
end
```

```
The following example provides additional information about the default local policy
configured on tunnel interface 1:
Device# show ip rsvp policy local detail
Tunnel1:
  Default policy:

    Preemption Scope: Unrestricted.
    Local Override:   Disabled.
    Fast ReRoute:     Accept.
    Handle:           BC000413.

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

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

Additional References

The following sections provide references related to the RSVP--VRF Lite Admission Control 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*
VRF-related internet draft	*Support for RSVP in Layer 3 VPNs,* Internet draft, November 19, 2007 [draft-davie-tsvwg-rsvp-l3vpn-01.txt]
Cisco IOS commands	Cisco IOS Master Commands List, All Releases

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

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 MPLS TE - Tunnel-Based Admission Control

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 MPLS TE--Tunnel-Based Admission Control (TBAC)

Feature Name	Releases	Feature Information
MPLS TE Tunnel-Based Admission Control	Cisco IOS XE Release 2.6	The MPLS TE--Tunnel-Based Admission Control feature enables classic Resource Reservation Protocol (RSVP) unicast reservations that are traveling across an MPLS TE core to be aggregated over an MPLS TE tunnel. The following commands were introduced or modified: **ip rsvp qos**, **show ip rsvp**, **show ip rsvp reservation**, **show ip rsvp sender**, **show mpls traffic-eng link-management bandwidth-allocation**.

Glossary

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

QoS --quality of service. A measure of performance for a transmission system that reflects its transmission quality and service availability. Quality of service focuses on achieving appropriate network performance for networked applications; it is superior to best effort performance.

RSVP --Resource Reservation Protocol. A protocol that supports the reservation of resources across an IP network. Applications that run 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. An extension of IP routing that provides multiple routing instances. 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 provider edge (PE) device.

CHAPTER 9

PfR RSVP Control

The PfR RSVP Control feature introduces the ability to perform application-aware path selection for traffic that is controlled by Resource Reservation Protocol (RSVP). This feature allows RSVP flows to be learned by Performance Routing (PfR) and protocol Path messages to be redirected after the PfR master controller determines the best exit using PfR policies.

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.

Information About PfR RSVP Control

PfR and RSVP Control

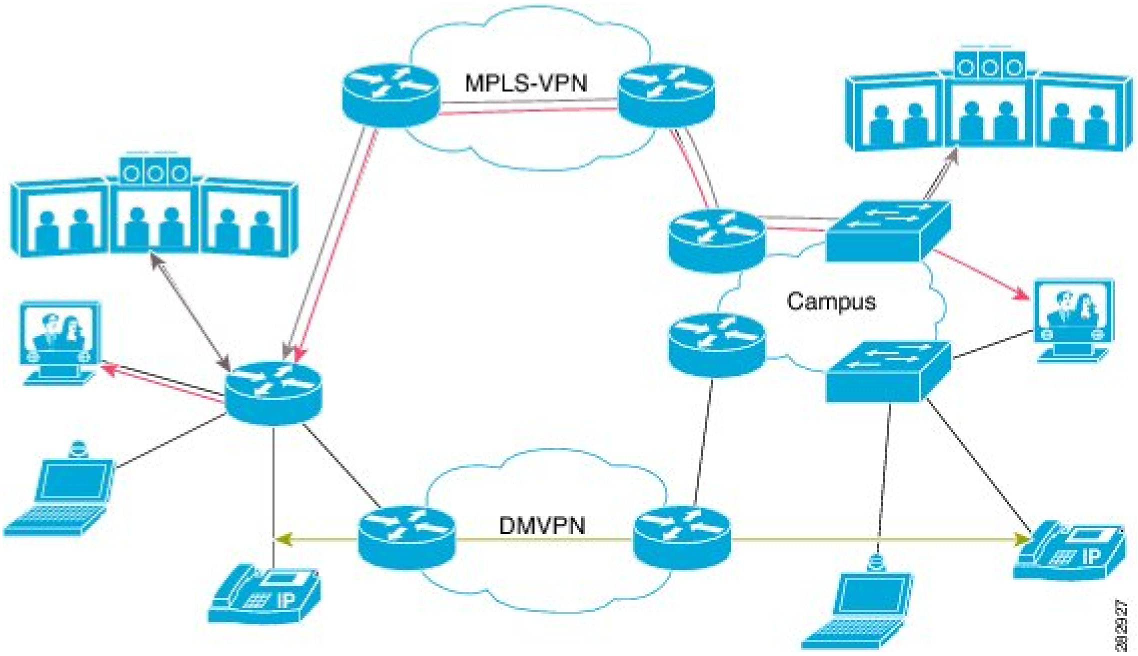
The PfR RSVP Control feature introduces the ability for Performance Routing (PfR) to learn, monitor, and optimize Resource Reservation Protocol (RSVP) flows. PfR is an integrated Cisco IOS solution that allows you to monitor IP traffic flows and then define policies and rules based on traffic class performance, link load distribution, link bandwidth monetary cost, and traffic type. PfR provides active and passive monitoring systems, dynamic failure detection, and automatic path correction. Deploying PfR enables intelligent load distribution and optimal route selection in an enterprise network that uses multiple ISP or WAN connections at the network edge.

PfR can monitor and control applications and prefixes that are configured or learned by observing traffic that is flowing on the network. The master controller (MC) is a centralized policy decision point at which policies are defined and applied to various traffic classes that traverse the border routers (BRs). The MC can be configured to learn and control traffic classes on the network. The MC makes exit selections and instructs the BRs to enforce the exit selection. While the current PfR implementation can be used to optimize voice/video traffic, the control exercised by PfR is not aware of technologies such as RSVP. The PfR RSVP integration will help RSVP leverage the application-specific control of routes that PfR can provide.

RSVP is a standards-based control protocol that allows for resources to be reserved to allow for better reliability for voice/video traffic. RSVP achieves this by signaling the traffic profile before the actual data flow to reserve resources for the data flow. Establishing end-to-end resource reservations along a media path allows RSVP to guarantee that resources are available when they are needed. RSVP consults the forwarding plane database (or CEF) in order to achieve path congruency with the media flow. The routes in the CEF database are mostly dictated by the routing protocols where the only metric for determining the best route is the cumulative cost of the links on that path.

In the diagram shown below, there are two paths for the network on the left to reach the campus network on the right. One path uses the DMVPN cloud, and the other path uses the MPLS-VPN cloud. Depending on the speed and bandwidth required, it might make sense to route video applications over the MPLS-VPN network while routing voice applications over the DMVPN network. Such kind of application-aware path selection is not possible in CEF, but PfR can determine the best path for specific application traffic based on performance criteria.

Figure 10: Application-Aware Path Selection



With the RSVP integration, PfR will learn, monitor, and optimize RSVP flows. RSVP is included as a new learn source. PfR will learn RSVP flows that traverse internal and external interfaces. Each RSVP flow is learned as a PfR traffic class and is controlled independently of the other RSVP flows. While filtering of the learned flows is supported with prefix lists and route maps, aggregating RSVP flows is not advised. The PfR master controller (MC) chooses a best exit based on the configured PfR policies and installs route maps to redirect traffic. If any of the RSVP flows enters an Out-of-Policy (OOP) condition, PfR will find and switch the RSVP flow to a new exit. RSVP will reinstall the reservation on the new path at the time of refresh (usually within a span of 30 seconds) or as a Fast Local Repair (FLR) case in less than 5 seconds.

The intent of the PfR RSVP Control feature is to identify and install route maps at the time the router receives an RSVP Path message. The route map captures the data traffic, while RSVP uses this path for the Path message.

RSVP flows are learned as PfR traffic classes defined as a single application flow that can be identified by the source address, source port, destination address, destination port and IP protocol. This microflow is optimized as an application by PfR, and a dynamic policy route is created by PfR to forward this traffic class over the selected exit.

All RSVP flows are optimized only after PfR checks that there is enough bandwidth on the exit that is being considered. This information is pushed periodically from the BRs to the MC. On the BR itself, RSVP notifies PfR every time the bandwidth pool on an interface changes.

Equivalent-Path Round-Robin Resolver

PfR introduced a new resolver with the PfR RSVP Control feature. PfR, by default, uses a random resolver to decide between equivalent paths, exits with the same cost determined by the PfR policies. When the round-robin resolver is configured using the **equivalent-path-round-robin** command, the next exit (next-hop interface) is selected and compared to the running PfR policy. The round-robin resolver is handed an array of equivalent exits from which it chooses in a round-robin fashion. Exits are pruned in the same fashion they are today by each resolver. If the exit matches the policy, the exit becomes the best exit. The round-robin resolver does not do any specific RSVP checking. To return to using the random resolver, enter the no form of the **equivalent-path-round-robin** command.

Any PfR traffiic class can use the round-robin resolver, and it provides a load-balancing scheme for multiple equivalent paths as determined by PfR policy.

RSVP Post Dial Delay Timer for Best Path Selection

In the PfR RSVP Control feature, the **rsvp post-dial-delay** command was introduced to set a value for the RSVP post dial delay timer that runs on the border routers when RSVP flow learning is enabled on a PfR master controller. The timer is updated on the border routers at the start of every PfR learn cycle, and the timer determines the delay, in milliseconds, before the routing path is returned to RSVP. When the PfR and RSVP integration is enabled, PfR tries to locate a best path for any RSVP flows that are learned before the delay timer expires. If the current path is not the best path, PfR attempts to install the new path. RSVP reacts to this policy route injection as a case of Fast Local Repair (FLR) and resignals a new reservation path.

RSVP Signaling Retries for Alternative Reservation Path

The PfR RSVP Control feature introduced a new command, **rsvp signaling-retries**, which is configured on a master controller and is used to instruct PfR to provide an alternate reservation path when an RSVP reservation returns an error condition. If an alternate path is provided by PfR, RSVP can resend the reservation signal. The default number of retries is set to 0; no signaling retries are to be permitted, and a reservation error message is sent when a reservation failure occurs.

Performance Statistics from PfR Commands

The PfR master controller learns and monitors IP traffic that flows through the border routers, and the master controller selects the best exit for a traffic flow based on configured policies and the performance information received from the border routers. To view some of the performance data collected by the master controller, you can use the following commands:

- **show pfr master active-probes**
- **show pfr master border**
- **show pfr master exits**
- **show pfr master statistics**
- **show pfr master traffic-class**
- **show pfr master traffic-class performance**

All these commands are entered at the master controller, and some of the commands have keywords and arguments to filter the output. For detailed information about these commands, see the Cisco IOS Performance Routing Command Reference.

How to Configure PfR RSVP Control

Configuring PfR RSVP Control Using a Learn List

Perform this task on the master controller to define a learn list that contains traffic classes that are automatically learned based on RSVP flows and filtered by a prefix list. In this task, the goal is to optimize all video traffic that is learned from RSVP flows.

The VIDEO traffic class is defined as any prefix that matches 10.100.0.0/16 or 10.200.0.0/16 and a PfR policy, named POLICY_RSVP_VIDEO, is created.

The learn lists are referenced in a PfR policy using a PfR map and are activated using the **policy-rules** (PfR) command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*}
4. **pfr master**
5. **policy-rules** *map-name*
6. **rsvp signaling-retries** *number*
7. **rsvp post-dial-delay** *msecs*
8. **learn**
9. **list seq** *number* **refname** *refname*
10. **traffic-class prefix-list** *prefix-list-name* [**inside**]
11. **rsvp**

12. **exit**
13. Repeat Step 9 to Step 12 to configure additional learn lists.
14. **exit**
15. Use the **exit** command as necessary to return to global configuration mode.
16. **pfr-map** *map-name sequence-number*
17. **match pfr learn list** *refname*
18. **set mode route control**
19. **set resolve equivalent-path-round-robin**
20. **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 prefix-list** *list-name* [**seq** *seq-value*] {**deny** *network/length* | **permit** *network/length*}
	Example:
	`Router(config)# ip prefix-list RSVP_VIDEO seq 10 permit 10.100.0.0/16`
		Creates an IP prefix list to filter prefixes for learning.
		• An IP prefix list is used under learn list configuration mode to filter IP addresses that are learned.
		• The example creates an IP prefix list named RSVP_VIDEO for PfR to profile the prefix, 10.100.0.0/16.

Step 4	**pfr master** **Example:** `Router(config)# pfr master`	Enters PfR master controller configuration mode to configure a Cisco router as a master controller and to configure master controller policy and timer settings.
Step 5	**policy-rules** *map-name* **Example:** `Router(config-pfr-mc)# policy-rules POLICY_RSVP_VIDEO`	Selects a PfR map and applies the configuration under PfR master controller configuration mode. • Use the *map-name* argument to specify the PfR map name to be activated. • The example applies the PfR map named POLICY_RSVP_VIDEO which includes the learn list configured in this task.

	Command or Action	Purpose
Step 6	**rsvp signaling-retries** *number* **Example:** `Router(config-pfr-mc)# rsvp signaling-retries 1`	Specifies the number of alternate paths that PfR provides for an RSVP reservation when a reservation error condition is detected. • Use the *number* argument to specify the number of alternate paths. • The example configured in this task shows how to configure PfR to set the number of alternate paths for RSVP signaling retries to 1.
Step 7	**rsvp post-dial-delay** *msecs* **Example:** `Router(config-pfr-mc)# rsvp post-dial-delay 100`	Configures the RSVP post dial delay timer to set the delay before PfR returns the routing path to RSVP. • Use the *msecs* argument to specify the delay, in milliseconds. • The example configured in this task shows how to configure PfR to set the RSVP post dial delay to 100 milliseconds.
Step 8	**learn** **Example:** `Router(config-pfr-mc)# learn`	Enters PfR Top Talker and Top Delay learning configuration mode to automatically learn traffic classes.
Step 9	**list seq** *number* **refname** *refname* **Example:** `Router(config-pfr-mc-learn)# list seq 10 refname LEARN_RSVP_VIDEO`	Creates a PfR learn list and enters learn list configuration mode. • Use the **seq** keyword and *number* argument to specify a sequence number used to determine the order in which learn list criteria are applied. • Use the **refname** keyword and *refname* argument to specify a reference name for the learn list. • The example creates a learn list named LEARN_RSVP_VIDEO.
Step 10	**traffic-class prefix-list** *prefix-list-name* [**inside**] **Example:** `Router(config-pfr-mc-learn-list)# traffic-class prefix-list RSVP_VIDEO`	Configures the master controller to automatically learn traffic based only on destination prefixes. • Use the *prefix-list-name* argument to specify a prefix list. • The example defines a traffic class using the prefix list named RSVP_VIDEO.
Step 11	**rsvp** **Example:**	Configures the master controller to learn the top prefixes based on RSVP flows.

	Command or Action	Purpose
	`Router(config-pfr-mc-learn-list)# rsvp`	• When this command is enabled, the master controller will learn the top prefixes across all border routers according to the highest outbound throughput. • The example configures a master controller to learn the top prefixes based on RSVP flows for the LEARN_RSVP_VIDEO learn list.
Step 12	**exit** **Example:** `Router(config-pfr-mc-learn-list)# exit`	Exits learn list configuration mode, and returns to PfR Top Talker and Top Delay learning configuration mode.
Step 13	Repeat Step 9 to Step 12 to configure additional learn lists.	--
Step 14	**exit** **Example:** `Router(config-pfr-mc-learn)# exit`	Exits PfR Top Talker and Top Delay learn configuration mode, and returns to PfR master controller configuration mode.
Step 15	Use the **exit** command as necessary to return to global configuration mode.	--
Step 16	**pfr-map** *map-name sequence-number* **Example:** `Router(config)# pfr-map POLICY_RSVP_VIDEO 10`	Enters PfR map configuration mode to configure a PfR map. • The example creates a PfR map named POLICY_RSVP_VIDEO.
Step 17	**match pfr learn list** *refname* **Example:** `Router(config-pfr-map)# match pfr learn list LEARN_RSVP_VIDEO`	Creates a match clause entry in a PfR map to match PfR-learned prefixes. • Only one match clause can be configured for each PfR map sequence. • The example defines a traffic class using the criteria defined in the PfR learn list named LEARN_RSVP_VIDEO. **Note** Only the syntax relevant to this task is used here.
Step 18	**set mode route control** **Example:** `Router(config-pfr-map)# set mode route control`	Creates a set clause entry to configure route control for matched traffic. • In control mode, the master controller analyzes monitored prefixes and implements changes based on policy parameters.

	Command or Action	Purpose
Step 19	**set resolve equivalent-path-round-robin** **Example:** `Router(config-pfr-map)# set resolve equivalent-path-round-robin`	Creates a set clause entry to specify the use of the equivalent-path round-robin resolver. • In this task, the equivalent-path round-robin resolver is used to choose between equivalent paths instead of the random resolver.

Step 20	**end**
	Example:
	`Router(config-pfr-map)# end`
		(Optional) Exits PfR map configuration mode and returns to privileged EXEC mode.

Displaying PfR RSVP Control Information

Although the PfR RSVP Control feature is configured on a master controller, the border routers actually collect the performance information, and there are **show** and **debug** commands available to display the RSVP information for both the master controller and border routers. The first few commands in this task are entered on a master controller and, for the rest of the commands, there is a step to move to a border router through which the application traffic is flowing. These **show** and **debug** commands can be entered in any order.

SUMMARY STEPS

1. **enable**
2. **show pfr master traffic-class** [**rsvp**] [**active** | **passive** | **status**] [**detail**]
3. **show pfr master policy** [*sequence-number* | *policy-name* | **default** | **dynamic**]
4. **debug pfr master rsvp**
5. Move to a border router through which the RSVP traffic is flowing.
6. **enable**
7. **show pfr border rsvp**
8. **show pfr border routes rsvp-cache**
9. **debug pfr border rsvp**

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 2 **show pfr master traffic-class** [**rsvp**] [**active** | **passive** | **status**] [**detail**]

This command is used to display information about PfR traffic classes that are learned as RSVP traffic classes.

Example:

```
Router# show pfr master traffic-class rsvp

OER Prefix Statistics:
 Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
 P - Percentage below threshold, Jit - Jitter (ms),
 MOS - Mean Opinion Score
 Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
 E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
 U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied

DstPrefix           Appl_ID Dscp Prot     SrcPort     DstPort SrcPrefix
           Flags             State     Time            CurrBR  CurrI/F Protocol
         PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos      EBw      IBw
         ActSDly  ActLDly   ActSUn   ActLUn  ActSJit  ActPMOS  ActSLos  ActLLos
--------------------------------------------------------------------------------
10.1.0.10/32              N    N  tcp       75-75       75-75 10.1.0.12/32
                          INPOLICY       @0         10.1.0.24 Tu24            PBR
               U        U        0        0        0        0        0        0
               1        1        0        0        N        N        N        N
```

Step 3 **show pfr master policy** [*sequence-number* | *policy-name* | **default** | **dynamic**]

This command is used to display policy information. The following example uses the **dynamic** keyword to display the policies dynamically created by provider applications. Note the RSVP configuration commands.

Example:

```
Router# show pfr master policy dynamic

Dynamic Policies:

  proxy id 10.3.3.3
  sequence no. 18446744069421203465, provider id 1001, provider priority 65535
    host priority 65535, policy priority 101, Session id 9
  backoff 90 90 90
  delay relative 50
  holddown 90
  periodic 0
  probe frequency 56
  mode route control
  mode monitor both
  mode select-exit good
  loss relative 10
  jitter threshold 20
  mos threshold 3.60 percent 30
  unreachable relative 50
  next-hop not set
  forwarding interface not set
  resolve delay priority 11 variance 20
  resolve utilization priority 12 variance 20
  proxy id 10.3.3.3
  sequence no. 18446744069421269001, provider id 1001, provider priority 65535
    host priority 65535, policy priority 102, Session id 9
  backoff 90 90 90
  delay relative 50
  holddown 90
  periodic 0
  probe frequency 56
  mode route control
  mode monitor both
  mode select-exit good
  loss relative 10
  jitter threshold 20
  mos threshold 3.60 percent 30
  unreachable relative 50
  next-hop not set
  forwarding interface not set
  resolve delay priority 11 variance 20
  resolve utilization priority 12 variance 20
  proxy id 10.3.3.4
  sequence no. 18446744069421334538, provider id 1001, provider priority 65535
    host priority 65535, policy priority 103, Session id 10
  backoff 90 90 90
  delay relative 50
  holddown 90
  periodic 0
  probe frequency 56
  mode route control
  mode monitor both
  mode select-exit good
  loss relative 10
  jitter threshold 20
  mos threshold 3.60 percent 30
  unreachable relative 50
  next-hop not set
  forwarding interface not set
  resolve delay priority 11 variance 20
  resolve utilization priority 12 variance 20
```

Step 4 **debug pfr master rsvp**

Displays debugging information about PfR RSVP events on a PfR master controller.

Example:

```
Router# debug pfr master rsvp

Jan 23 21:18:19.439 PST: PFR_MC_RSVP: recvd a RSVP flow
Jan 23 21:18:19.439 PST: PFR_MC_RSVP: Processing 1 rsvp flows
Jan 23 21:18:19.439 PST: PFR_MC_RSVP: Resolve: src: 10.1.0.12 dst: 10.1.25.19 pr
oto: 17 sport min: 1 sport max: 1 dport min: 1 dport max: 1 from BR 10.1.0.23
Jan 23 21:18:19.439 PST: PFR_MC_RSVP: Marking: 10.1.0.23, FastEthernet1/0
Jan 23 21:18:19.439 PST: %OER_MC-5-NOTICE: Uncontrol Prefix 10.1.25.19/32, Probe frequency changed
Jan 23 21:18:19.439 PST: PFR_MC_RSVP: Marked: 10.1.0.23, FastEthernet1/0 as current
Jan 23 21:18:19.467 PST: PFR_MC_RSVP: recv new pool size
Jan 23 21:18:19.467 PST: PFR_MC_RSVP: Update from 10.1.0.23, Fa1/0: pool 8999
Jan 23 21:18:20.943 PST: %OER_MC-5-NOTICE: Prefix Learning WRITING DATA
Jan 23 21:18:21.003 PST: %OER_MC-5-NOTICE: Prefix Learning STARTED
Jan 23 21:18:22.475 PST: PFR_MC_RSVP: RSVP resolver invoked
Jan 23 21:18:22.475 PST: PFR RSVP MC:  10.1.25.19/32 Appl 17 [1, 1][1, 1] 0:
        BR 10.1.0.23, Exit Fa1/0, is current exit
Jan 23 21:18:22.475 PST: PFR RSVP MC:  10.1.25.19/32 Appl 17 [1, 1][1, 1] 0:
        BR 10.1.0.23, Exit Fa1/0, is current exit
Jan 23 21:18:22.475 PST: PFR_MC_RSVP: BR:10.1.0.23 Exit:Fa1/0pool size : 8999
est : 8999 tc->tspec: 1, fit: 8999
Jan 23 21:18:22.475 PST: PFR_MC_RSVP: BR:10.1.0.24 Exit:Tu24pool size : 9000
est : 9000 tc->tspec: 1, fit: 8999
Jan 23 21:18:22.475 PST: PFR_MC_RSVP: BR:10.1.0.23 Exit:Fa1/1pool size : 9000
est : 9000 tc->tspec: 1, fit: 8999
```

Step 5 Move to a border router through which the RSVP traffic is flowing.

Step 6 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 7 **show pfr border rsvp**

The following example shows information about the current values for the RSVP post dial timeout timer and signaling retries on a PfR border router:

Example:

```
Router# show pfr border rsvp

PfR BR RSVP parameters:
       RSVP Signaling retries:         1
       Post-dial-timeout(msec):        0
```

Step 8 **show pfr border routes rsvp-cache**

This command is used to show all the RSVP paths that PfR is aware of.

Note Only syntax appropriate to this example is shown.

Example:

```
Router# show pfr border routes rsvp-cache

SrcIP       DstIP       Protocol Src_port Dst_port Nexthop       Egress I/F PfR/RIB
----------- ----------- -------- -------- -------- ------------- ---------- --------
10.1.25.19  10.1.35.5   UDP      1027     1027     10.1.248.5    Gi1/0       RIB*
10.1.0.12   10.1.24.10  UDP      48       48       10.1.248.24   Gi1/0       PfR*
10.1.0.12   10.1.42.19  UDP      23       23       10.1.248.24   Gi1/0       PfR*
10.1.0.12   10.1.18.10  UDP      12       12       172.16.43.2   Fa1/1       PfR*
```

Step 9 **debug pfr border rsvp**

Displays debugging information about PfR RSVP events on a PfR border router.

Example:

```
Router# debug pfr border rsvp

Jan 23 21:18:19.434 PST: PfR RSVP:RESOLVE called for src: 10.1.0.12 dst: 10.1.25.19
 proto: 17 sport: 1 dport: 1; tspec 1
Jan 23 21:18:19.434 PST: PfR RSVP:hash index = 618
Jan 23 21:18:19.434 PST: PfR RSVP:Searching flow: src: 10.1.0.12 dst: 10.1.25.19
 proto: 17 sport: 1 dport: 1
Jan 23 21:18:19.434 PST: PfR RSVP:Add flow: src: 10.1.0.12 dst: 10.1.25.19
 proto: 17 sport: 1 dport: 1
Jan 23 21:18:19.434 PST: PfR RSVP:hash index = 618
Jan 23 21:18:19.434 PST: PfR RSVP:Searching flow: src: 10.1.0.12 dst: 10.1.25.19
 proto: 17 sport: 1 dport: 1
Jan 23 21:18:19.434 PST: PfR RSVP:hash index = 618
Jan 23 21:18:19.434 PST: PfR RSVP:successfully added the flow to the db
Jan 23 21:18:19.434 PST: PfR RSVP:flow: src: 10.1.0.12 dst: 10.1.25.19
 proto: 17 sport: 1 dport: 1 lookup; topoid: 0
Jan 23 21:18:19.434 PST: PfR RSVP(det):ret nh: 10.185.252.1, idb: 35
Jan 23 21:18:19.434 PST: PfR RSVP:Adding new context
Jan 23 21:18:19.434 PST: PfR RSVP(det):Num contexts: 0
Jan 23 21:18:19.434 PST: PfR RSVP(det):Num contexts: 1
Jan 23 21:18:19.434 PST: PfR RSVP:flow src: 10.1.0.12 dst: 10.1.25.19
 proto: 17 sport: 1 dport: 1 now pending notify
```

```
Jan 23 21:18:19.434 PST: PfR RSVP:Resolve on flow: src: 10.1.0.12 dst: 10.1.25.19
 proto: 17 sport: 1 dport: 1
Jan 23 21:18:19.434 PST: PfR RSVP:Filtering flow: src: 10.1.0.12 dst: 10.1.25.19
 proto: 17 sport: 1 dport: 1
```

Displaying PfR Performance and Statistics Information

Enter the commands in this task to view more detailed performance or statistical information about PfR traffic classes or exits. The commands can be entered in any order within each section.

SUMMARY STEPS

1. **enable**
2. **show pfr master traffic-class** [**policy** *policy-seq-number* | *rc-protocol* | **state** {**hold**| **in** | **out** | **uncontrolled**}] [**detail**]
3. **show pfr master traffic-class performance** [**application** *application-name* [*prefix*] | **history** [**active** | **passive**] | **inside** | **learn** [**delay** | **inside** | **list** *list-name* | **rsvp** | **throughput**] | **policy** *policy-seq-number* | *rc-protocol* | **state** {**hold** | **in** | **out** | **uncontrolled**} | **static**] [**detail**]
4. **show pfr master exits**
5. **show pfr master active-probes** [**assignment** | **running**] [**forced** *policy-sequence-number* | **longest-match**]
6. **show pfr master border** [*ip-address*] [**detail** | **report** | **statistics** | **topology**]
7. **show pfr master statistics** [**active-probe** | **border** | **cc** | **exit** | **netflow** | **prefix** | **process** | **system** | **timers**]

DETAILED STEPS

Step 1 **enable**

Enables privileged EXEC mode. Enter your password if prompted.

Example:

```
Router> enable
```

Step 2 **show pfr master traffic-class** [**policy** *policy-seq-number* | *rc-protocol* | **state** {**hold**| **in** | **out** | **uncontrolled**}] [**detail**]

This command is used to display information about traffic classes that are monitored and controlled by a PfR master controller. In this example, the **state in** keywords are used to filter the output to show only traffic classes that are in an in-policy state.

Example:

```
Router# show pfr master traffic-class state in

OER Prefix Statistics:
 Pas - Passive, Act - Active, S - Short term, L - Long term, Dly - Delay (ms),
 P - Percentage below threshold, Jit - Jitter (ms),
 MOS - Mean Opinion Score
 Los - Packet Loss (packets-per-million), Un - Unreachable (flows-per-million),
 E - Egress, I - Ingress, Bw - Bandwidth (kbps), N - Not applicable
 U - unknown, * - uncontrolled, + - control more specific, @ - active probe all
 # - Prefix monitor mode is Special, & - Blackholed Prefix
 % - Force Next-Hop, ^ - Prefix is denied
```

```
DstPrefix           Appl_ID Dscp Prot     SrcPort     DstPort SrcPrefix
           Flags            State     Time           CurrBR  CurrI/F Protocol
         PasSDly  PasLDly   PasSUn   PasLUn  PasSLos  PasLLos      EBw      IBw
         ActSDly  ActLDly   ActSUn   ActLUn  ActSJit  ActPMOS  ActSLos  ActLLos
--------------------------------------------------------------------------------
10.1.0.0/24               N    N    N           N           N N
                          INPOLICY        0          10.1.1.1 Et0/0           BGP
              14       14        0        0        0        0       78        9
               N        N        N        N        N        N

10.2.0.0/24               N    N    N           N           N N
                          INPOLICY        0          10.1.1.2 Et0/0           BGP
              14       14        0        0        0        0       75        9
               N        N        N        N        N        N

10.3.0.0/24               N    N    N           N           N N
                          INPOLICY        0          10.1.1.3 Et0/0           BGP
              14       14        0        0        0        0       77        9
               N        N        N        N        N        N

10.4.0.0/24               N    N    N           N           N N
                          INPOLICY        0          10.1.1.4 Et0/0           BGP
              14       14        0        0        0        0       77        9
               N        N        N        N        N        N

10.1.8.0/24               N    N    N           N           N N
                          INPOLICY        0          10.1.1.3 Et0/0           BGP
              14       14    62500    73359        0        0        5        1
               N        N        N        N        N        N

10.1.1.0/24               N    N    N           N           N N
                          INPOLICY        0          10.1.1.2 Et0/0           BGP
              14       14     9635     9386     1605     1547       34        4
               N        N        N        N        N        N
```

Step 3 **show pfr master traffic-class performance** [**application** *application-name* [*prefix*] | **history** [**active** | **passive**] | **inside** | **learn** [**delay** | **inside** | **list** *list-name* | **rsvp** | **throughput**] | **policy** *policy-seq-number* | *rc-protocol* | **state** {**hold** | **in** | **out** | **uncontrolled**} | **static**] [**detail**]

This command displays performance information about traffic classes that are monitored and controlled by a PfR master controller.

Note Only the syntax applicable to this example is shown.

Example:

The following output shows traffic-class performance history on current exits during the last 60 minutes.

```
Router# show pfr master traffic-class performance history

Prefix: 10.70.0.0/16
efix performance history records
 Current index 1, S_avg interval(min) 5, L_avg interval(min) 60

Age       Border          Interface       OOP/RteChg Reasons
Pas: DSum  Samples  DAvg  PktLoss  Unreach   Ebytes   Ibytes     Pkts    Flows
Act: Dsum Attempts  DAvg    Comps  Unreach   Jitter LoMOSCnt   MOSCnt
00:00:33  10.1.1.4        Et0/0
Pas: 6466      517    12        2       58  3400299   336921    10499     2117
Act:    0        0     0        0        0        N        N        N
00:01:35  10.1.1.4        Et0/0
Pas:15661     1334    11        4      157  4908315   884578    20927     3765
Act:    0        0     0        0        0        N        N        N
```

```
00:02:37  10.1.1.4        Et0/0
Pas:13756     1164    11        9      126  6181747   756877    21232     4079
Act:    0        0     0        0        0        N        N        N
00:03:43  10.1.1.1        Et0/0
Pas:14350     1217    11        6      153  6839987   794944    22919     4434
Act:    0        0     0        0        0        N        N        N
00:04:39  10.1.1.3        Et0/0
Pas:13431     1129    11       10      122  6603568   730905    21491     4160
Act:    0        0     0        0        0        N        N        N
00:05:42  10.1.1.2        Et0/0
Pas:14200     1186    11        9      125  4566305   765525    18718     3461
Act:    0        0     0        0        0        N        N        N
00:06:39  10.1.1.3        Et0/0
Pas:14108     1207    11        5      150  3171450   795278    16671     2903
Act:    0        0     0        0        0        N        N        N
00:07:39  10.1.1.4        Et0/0
Pas:11554      983    11       15      133  8386375   642790    23238     4793
Act:    0        0     0        0        0        N        N        N
```

Step 4 **show pfr master exits**

Use this command to display information about the exits used for PfR traffic classes, including the IP address, nickname of the PfR managed external interface, the exit policy, interface of the border router, and exit performance data. The example below shows RSVP pool information.

Example:

```
Router# show pfr master exits

PfR Master Controller Exits:

General Info:
=============
  E - External
  I - Internal
  N/A - Not Applicable
                                                                                           Up/
   ID Name         Border          Interface   ifIdx IP Address      Mask Policy      Type Down
  --- ------------ --------------- ----------- ----- --------------- ---- ----------- ---- ----
    6 external1    10.1.0.23       Fa1/0           9 10.185.252.23     27 Util           E  UP
    5 external2    10.1.0.23       Fa1/1          10 172.16.43.23      27 Util           E  UP
    4              10.1.0.24       Tu24           33 10.20.20.24       24 Util           E  UP

Global Exit Policy:
===================
    Range Egress:      In Policy - No difference between exits - Policy 10%
   Range Ingress:      In Policy - No difference between entrances - Policy 0%
     Util Egress:      In Policy
    Util Ingress:      In Policy
            Cost:      In Policy

Exits Performance:
==================
                   Egress                                            Ingress
    ---------------------------------------------------- ------------------------------------
 ID Capacity  MaxUtil    Usage   %      RSVP POOL    OOP Capacity  MaxUtil    Usage   %  OOP
 --- -------- -------- -------- --- -------------- ----- -------- -------- -------- --- -----
  6   100000    90000       66   0           9000    N/A   100000   100000       40    0  N/A
  5   100000    90000       34   0           8452    N/A   100000   100000       26    0  N/A
  4   100000    90000      128   0           5669    N/A   100000   100000      104    0  N/A

TC and BW Distribution:
=======================
                       # of TCs                 BW (kbps)            Probe   Active
     Name/ID   Current Controlled InPolicy    Controlled       Total  Failed  Unreach
                                                                     (count) (fpm)
        ----   ----------------------------   ----------------------  ------  --------
           6        0          0        0            0           66        0          0
           5      548        548      548            0           34        0          0
           4     3202       3202     3202            0          128        0          0

Exit Related TC Stats:
======================
                                  Priority
                             highest       nth
                            ------------------
  Number of TCs with range:        0         0
   Number of TCs with util:        0         0
   Number of TCs with cost:        0         0

       Total number of TCs:     3800
```

Step 5 **show pfr master active-probes** [**assignment** | **running**] [**forced** *policy-sequence-number* | **longest-match**]

The following example shows the status of all created or in-progress probes.

Example:

```
Router# show pfr master active-probes running

PfR Master Controller running probes:

Border         Interface   Type     Target         TPort Codec    Freq Forced Pkts DSCP
                                                                       (Pol
                                                                        Seq)
-------------- ----------- -------- -------------- ----- -------- ---- ------ ---- ----
10.100.100.200 Ethernet1/0 tcp-conn 10.100.200.100 65535 g711alaw 10   20     100  ef
10.2.2.3       Ethernet1/0 tcp-conn 10.1.5.1       23    N        56   10     1    defa
10.1.1.1       Ethernet1/0 tcp-conn 10.1.5.1       23    N        30   N      1    defa
10.1.1.2       Ethernet1/0 tcp-conn 10.1.2.1       23    N        56   N      1    defa
10.2.2.3       Ethernet1/0 tcp-conn 10.1.2.1       23    N        56   N      1    defa
10.1.1.1       Ethernet1/0 tcp-conn 10.1.2.1       23    N        56   N      1    defa
```

Step 6 **show pfr master border** [*ip-address*] [**detail** | **report** | **statistics** | **topology**]

Entered on a master controller, this command displays statistics about all the border routers.

Example:

```
Router# show pfr master border statistics

PFR Master Controller Border
 MC Version: 2.3
 Keepalive : 5 second
 Keepalive : DISABLED

                                                   Last
Border           Status Up/Down UpTime   AuthFail  Receive  Version
---------------- ------ ------- -------- --------  -------- -------
10.200.200.200   ACTIVE UP      03:12:12        0  00:00:04 2.2
10.1.1.2         ACTIVE UP      03:10:53        0  00:00:10 2.2
10.1.1.1         ACTIVE UP      03:12:12        0  00:01:00 2.2

Border Connection Statistics
==============================
                          Bytes         Bytes    Msg    Msg    Sec Buf
Border                     Sent         Recvd   Sent  Recvd Bytes Used
---------------- -------------- ------------- ------ ------ ----------
10.200.200.200           345899        373749      5     10          0
10.1.1.2                 345899        373749      5     10          0
10.1.1.1                 345899        373749      5     10          0

                 Socket Invalid   Context
Border           Closed Message Not Found
---------------- ------ ------- ---------
10.200.200.200        5      10       100
10.1.1.2              5      10       100
10.1.1.1              5      10       100
```

Step 7 **show pfr master statistics** [**active-probe** | **border** | **cc** | **exit** | **netflow** | **prefix** | **process** | **system** | **timers**]

This command displays statistics from the master controller. Use the keywords to filter the display information. In the example below, the **system** keyword displays PfR system statistics.

Example:

```
Router# show pfr master statistics system

   Active Timers: 14
    Total Traffic Classes = 65, Prefixes = 65, Appls =0
   TC state:
    DEFAULT = 0, HOLDDOWN = 11, INPOLICY = 54, OOP = 0, CHOOSE = 0,
    Inside = 1, Probe all = 0, Non-op = 0, Denied = 0
    Controlled 60, Uncontrolled 5, Alloced 65, Freed 0, No memory 0
   Errors:
    Invalid state = 0, Ctrl timeout = 0, Ctrl rej = 0, No ctx = 7616,
    Martians = 0
    Total Policies = 0
    Total Active Probe Targets = 325
    Total Active Probes Running = 0
   Cumulative Route Changes:
    Total  : 3246
    Delay  : 0
    Loss   : 0
    Jitter : 0
    MOS    : 0
    Range  : 0
    Cost   : 0
    Util   : 0
   Cumulative Out-of-Policy Events:
    Total  : 0
    Delay  : 0
    Loss   : 0
    Jitter : 0
    MOS    : 0
    Range  : 0
    Cost   : 0
    Util   :
```

Configuration Examples for PfR RSVP Control

Example Defining Traffic Classes Using RSVP Flows

The following example, configured on the master controller, defines a learn list that will contain traffic classes that are automatically learned based on RSVP flows and filtered by a prefix list. In this example, the goal is to optimize all video traffic using the policy named POLICY_RSVP_VIDEO. The RSVP_VIDEO traffic class is defined as any prefix that matches 10.100.0.0/16 or 10.200.0.0/16 and is learned from RSVP flows.

This example configures prefix learning based on RSVP traffic flows.

```
ip prefix-list RSVP_VIDEO permit seq 10 10.100.0.0/16
ip prefix-list RSVP_VIDEO permit seq 20 10.200.0.0/16
pfr master
 policy-rules POLICY_RSVP_VIDEO
 rsvp signaling-retries 1
 rsvp post-dial-delay 100
 learn
 list seq 10 refname LEARN_RSVP_VIDEO
 traffic-class prefix-list RSVP_VIDEO
 rsvp
 exit
 exit
pfr-map POLICY_RSVP_VIDEO 10
 match learn list LEARN_RSVP_VIDEO
 set mode route control
 set resolve equivalent-path-round-robin
 end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Cisco PfR commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	Cisco IOS Performance Routing Command Reference
Basic PfR configuration	“Configuring Basic Performance Routing” module
NetFlow and NetFlow data export	*Configuring NetFlow and NetFlow Data Export*
PfR home page with links to PfR-related content on our DocWiki collaborative environment	PfR:Home

RFCs

RFC	Title
RFC 3954	*Cisco Systems NetFlow Services Export Version 9*

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 PfR RSVP Control

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 PfR RSVP Control

Feature Name	Releases	Feature Information
PfR RSVP Control	Cisco IOS XE Release 3.4S	The PfR RSVP Control feature provides support for optimizing RSVP flows using application-aware PfR techniques. The following commands were introduced or modified by this feature: **debug pfr border rsvp**, **debug pfr master rsvp**, **rsvp (PfR)**, **rsvp post-dial-delay**, **rsvp signaling-retries**, **resolve (PfR)**, **set resolve (PfR)**, **show pfr border rsvp**, **show pfr border routes**, **show pfr master active-probes**, **show pfr master border**, **show pfr master exits**, **show pfr master policy**, **show pfr master statistics**, **show pfr master traffic-class**, and **show pfr master traffic-class performance**.

CHAPTER 10

RSVP over UDP

The Resource Reservation Protocol (RSVP) over UDP feature provides the capability for routers to enable neighbor routers to process and send RSVP control packets over UDP. With the implementation of the RSVP over UDP feature, the RSVP protocol stack is enhanced to support processing of RSVP control messages over UDP and raw IP.

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 Over UDP

- You must enable RSVP before you enable the RSVP over UDP feature.
- The RSVP stack running on the client host must support sending and receiving the RSVP control messages with the first hop routers they are connected to.

Information About RSVP over UDP

RSVP over UDP

The RSVP over UDP feature addresses the following scenarios:

- A router intends to communicate to the first hop router over UDP but not raw IP.
- A firewall that is located in between two routers drops raw IP packets due to security concerns, but allows UDP packets.

How to Configure RSVP over UDP

Enabling RSVP

This task starts RSVP and sets the bandwidth and single-flow limits. By default, RSVP is disabled so that it is backward compatible with systems that do not implement RSVP. To enable RSVP for IP on an interface, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip rsvp bandwidth** [*interface-bandwidth* [**percent** *percent-bandwidth* | [*single-flow-bandwidth*] [**sub-pool** *bandwidth*]]]
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:**	Configures the specified interface and enters interface configuration mode.

	Command or Action	Purpose
	`Device(config)# interface fastethernet 0/1`	
Step 4	**ip rsvp bandwidth** [*interface-bandwidth* [**percent** *percent-bandwidth* | [*single-flow-bandwidth*] [**sub-pool** *bandwidth*]]] **Example:** `Device(config-if)# ip rsvp bandwidth 23 54`	Enables RSVP for IP on an interface.

Step 5	**end**
	Example:
	`Device(config-if)# end`
		Exits interface configuration mode and returns to privileged EXEC mode.

Configuring RSVP over UDP

To enable RSVP over UDP, perform the following task:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip rsvp udp neighbor** *neighbor-IP-address* **router** [**vrf** *vrf-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	**ip rsvp udp neighbor** *neighbor-IP-address* **router** [**vrf** *vrf-name*]
	Example:
	`Device(config)# ip rsvp udp neighbor 10.1.1.1`
	`router vrf vrf-1`
		Configures the RSVP over UDP feature for the neighbor router.

	Command or Action	Purpose

Step 4	**end**
	Example:
	`Device(config)# end`
		Returns to privileged EXEC mode.

Configuration examples for RSVP over UDP

Example: Enabling RSVP

The following example shows how to enable RSVP for IP on an interface:

```
enable
 configure terminal
 interface  fastethernet 0/1
  ip rsvp bandwidth 23 54
  end
```

Example: Configuring RSVP over UDP

The following example shows how to configure the RSVP over UDP feature on a neighbor router:

```
enable
 configure terminal
 ip rsvp udp neighbor 10.1.1.1 router vrf vrf-1
 end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Master Command List, All Releases
RSVP commands	*Quality of Service Solutions Command Reference*
Overview on RSVP	*Signaling Overview*

Standards and RFCs

Standard/RFC	Title
RFC 2205	*RSVP—Version 1 Function Specification*
RFC 2209	*RSVP—Version 1 Message 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 over UDP

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 9: Feature Information for RSVP over UDP

Feature Name	Releases	Feature Information
RSVP over UDP	15.2(4)M 15.4(1)S XE 3.11.0 S	The RSVP over UDP feature allows a router to enable a neighbor router to process and send RSVP control packets over UDP. The following commands were introduced or modified: **ip rsvp udp neighbor**.