

Configuring RSVP

This chapter describes how to configure Resource Reservation Protocol (RSVP), which is an IP service. For a complete description of the RSVP commands in this chapter, refer to the “RSVP Commands” chapter of the *Network Protocols Command Reference, Part 1*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

RSVP allows end systems to request Quality of Service (QOS) guarantees from the network. The need for network resource reservations differs for data traffic versus for real-time traffic, as follows:

- Data traffic seldom needs reserved bandwidth since internetworks provide datagram services for data traffic. This asynchronous packet switching may not need guarantees of service quality. Routers can operate in a first-in, first out (FIFO) manner for data traffic packets. End-to-end controls between data traffic senders and receivers help ensure adequate transmission of bursts of information.
- Real-time traffic (that is, voice or video information) experiences problems when operating over datagram services. Since real-time traffic sends an almost constant flow of information, the network “pipes” must be consistent. Some guarantee must be provided that service between real-time hosts will not vary. Routers operating on a FIFO basis risk unrecoverable disruption of the real-time information that is being transmitted.

Data applications (with little need for resource guarantees) frequently demand relatively lower bandwidth than real-time traffic. The almost constant high bit-rate demands of a video conference application, and the bursty low bit-rate demands of an interactive data application, share available network resources.

RSVP prevents the demands of real-time traffic from impairing the bandwidth resources necessary for bursty data traffic. To do this, the routers sort and prioritize packets much like a statistical time division multiplexor would sort and prioritize several signal sources that shares a single channel.

RSVP mechanisms enable real-time traffic to reserve resources necessary for consistent latency. A video conferencing application can use settings in the router to propagate a request for a path with the required bandwidth and delay for video conferencing destinations. RSVP will check and repeat reservations at regular intervals. By this process, RSVP can adjust and alter the path between RSVP end systems to recover from router changes.

Real-time traffic (unlike data traffic) requires a guaranteed network consistency. Without consistent QOS, real-time traffic faces the following problems:

- Jitter—A slight time or phase movement in a transmission signal can introduce loss of synchronization or other errors.
- Insufficient bandwidth—Voice calls use a digital signal level 0 (DS0 at 64 kbps); video conferencing uses T1/E1 (1.544 Mbs or 2.048 Mpbs); and higher-fidelity video uses much more.

- Delay variations—If the wait time between when signal elements are sent and when they arrive varies, the real-time traffic will no longer be synchronized and may fail.
- Information loss—When signal elements drop or arrive too late lost audio causes distortions with noise or crackle sounds. The lost video causes image blurring, distortions, or blackouts.

RSVP works in conjunction with weighted fair queuing (WFQ) or random early detection (RED). This conjunction of reservation setting with packet queuing uses two key concepts: end-to-end flows with RSVP and router-to-router conversations with WFQ.

- RSVP Flow—This is a stream that operates “multidestination simplex,” since data travels across it in only one direction (from the origin to the targets). Flows travel from a set of senders to a set of receivers. The flows can be merged or left unmerged, and the method of merging them varies according to the attributes of application using the flow.
- WFQ Conversation—This is the traffic for a single transport layer session or network layer flow that crosses a given interface. This conversation is called from the source and destination address, protocol type, port number, or other attributes in the relevant communications layer.

RSVP allows for hosts to send packets to a subset of all hosts (*multicasting*). RSVP assumes that resource reservation applies primarily to multicast applications (such as video conferencing). Although the primary target for RSVP is multimedia traffic, a clear interest exists for the reservation of bandwidth for unicast traffic (such as NFS and virtual private network management). A *unicast* transmission involves a host sending packets to a single host.

RSVP Reservation Types

Two types of multicast flows are a flow that originates from exactly one sender (called a *distinct reservation*), and a flow that originates from one or more senders (called a *shared reservation*). RSVP describes these reservations as having certain algorithmic attributes.

Distinct Reservation

An example of a distinct reservation is a video application, in which each sender emits a distinct data stream that requires admission and management in a queue. Such a flow, therefore, requires a separate reservation per sender on each transmission facility it crosses (such as Ethernet, an HDLC line, a Frame Relay DLCI, or an ATM virtual channel). RSVP refers to this distinct reservation as explicit, and installs it using a Fixed Filter style of reservation.

Use of RSVP for unicast applications is generally a degenerate case of a distinct flow.

Shared Reservation

An example of a shared reservation is an audio application, in which each sender also emits a distinct data stream that requires admission and management in a queue. However, because of the nature of the application, a limited number of senders are transmitting data at any given time. Such a flow, therefore, does not require a separate reservation per sender. Instead, a single reservation that can be applied to any sender within a set, as needed.

RSVP installs a shared reservation using a Wild Card or Shared Explicit style of reservation, with the difference between the two being determined by the scope of application (which is either wild or explicit).

- The Wild Card Filter reserves bandwidth and delay characteristics for any sender, and is limited by the list of source addresses carried in the reservation message.
- The Shared Explicit reservation style identifies the flows for specific network resources.

Planning for RSVP Configuration

You must plan carefully to successfully configure and use RSVP on your network. At a minimum, RSVP must reflect your assessment of bandwidth needs on router interfaces. Consider the following questions as you plan for RSVP configuration:

- How much bandwidth should RSVP allow per end-user application flow? You must understand the “feeds and speeds” of your applications. By default, the amount reservable by a single flow can be the entire reservable bandwidth. You can, however, limit individual reservations to smaller amounts using the single flow bandwidth parameter. This value may not exceed the interface reservable amount, and no one flow may reserve more than the amount specified.
- How much bandwidth is available for RSVP? By default, 75 percent of the bandwidth available on an interface is reservable. If you are using a tunnel interface, RSVP can make a reservation for the tunnel whose bandwidth is the sum of the bandwidths reserved within the tunnel.
- How much bandwidth must be excluded from RSVP so that it can fairly provide the timely service required by low-volume data conversations? End-to-end controls for data traffic assumes that all sessions will behave so as to avoid congestion dynamically. Real-time demands do not follow this behavior. Determine the bandwidth to set aside so bursty data traffic will not be deprived as a side effect of the RSVP QoS configuration.

Plan for RSVP before entering the details needed as RSVP configuration parameters.

RSVP Implementation Considerations

You should be aware of RSVP implementation considerations as you design your reservation system. RSVP does not model all data links likely to be present on the internetwork. RSVP models an interface as having a queuing system that completely determines the mix of traffic on the interface; bandwidth or delay characteristics are only deterministic to the extent that this model holds. Unfortunately, data links are often imperfectly modeled this way. Use the following guidelines:

- Serial line interfaces—PPP, HDLC, LAPB, HSSI, and similar serial line interfaces are well modeled by RSVP. The device can, therefore, make guarantees on these interfaces. With NBMA interfaces, these are also the most in need of reservations.
- Multiaccess LANs—These data links are not modeled well by RSVP interfaces, because the LAN itself represents a queuing system that is not under the control of the device making the guarantees. The device guarantees what load it will offer, but cannot guarantee what competing loads or timings of loads that neighboring LAN systems will offer. The network administrator can use admission controls to control how much traffic is placed on the LAN. The network administrator, however, should focus on the use of admission in network design in order to use RSVP effectively.
- Public X.25 networks—It is not clear that rate or delay reservations can be usefully made on public X.25 networks.

You must use a specialized configuration on Frame Relay and ATM networks, as discussed in the next sections.

Considerations for a Frame Relay Internetwork

The following RSVP implementation considerations apply as you design your reservation system for a Frame Relay internetwork:

- Reservations are made for an interface or subinterface. If subinterfaces contain more than one DLC, the bandwidth required and the bandwidth reserved may differ. Therefore, RSVP subinterfaces of frame relay circuits must contain exactly one DLC to operate correctly.
- In addition, Frame Relay DLCs have rates (CIR) and burst controls (Bc and Be) that may not be reflected in the configuration, and may differ markedly from the interface speed (either adding up to exceed it or being significantly smaller). Therefore, the **ip rsvp bandwidth** interface configuration command must be entered for both the interface and the subinterface. Both bandwidths are used as admission criteria.

For example, suppose that a Frame Relay interface runs at a T1 rate (1.544 Mbps) and supports several DLCs to remote offices served by 128 and 56 kbps lines. One must configure the amount of the total interface (75 percent of which being 1.158 Mbps) and the amount of each receiving interface (75 percent of which would be 96 and 42 kbps, respectively) that may be reserved. Admission succeeds if and only if enough bandwidth is available on the DLC (the subinterface) and on the aggregate interface.

Considerations for an ATM Internetwork

The following RSVP implementation considerations apply as you design your reservation system for an ATM internetwork:

- When ATM is configured, it most likely uses a usable bit rate (UBR) or an available bit rate (ABR) virtual channel (VC) connecting individual routers. With these classes of service, the ATM network makes a “best effort” to meet the traffic’s bit-rate requirements, and assumes that the end-stations are responsible for information that does not get through the network.
- This ATM service has the capability of opening separate channels for reserved traffic having the necessary characteristics. RSVP should open these VCs and adjust the cache to make effective use of the VC for this purpose.

RSVP Task List

After you have planned your RSVP configuration, enter the Cisco IOS commands that implement your configuration plan. The following sections discuss how to configure RSVP. You must enable RSVP on an interface in order to use it; the other tasks are optional.

- Enable RSVP
- Enter Senders in the RSVP Database
- Enter Receivers in the RSVP Database
- Enter Multicast Addresses
- Control Which RSVP Neighbor Can Offer a Reservation
- Monitor RSVP

Enable RSVP

By default, RSVP is disabled so that it is backward compatible with systems that do not implement RSVP. To enable RSVP on an interface, perform the following task in global configuration mode:

Task	Command
Enable RSVP for IP on an interface.	ip rsvp bandwidth <i>[interface-kbps] [single-flow-kbps]</i>

This command starts RSVP and sets the bandwidth and single-flow limits. The default maximum bandwidth is up to 75 percent of the bandwidth available on the interface. By default, the amount reservable by a flow can be up to the entire reservable bandwidth.

On subinterfaces, this applies the more restrictive of the available bandwidths of the physical interface and the subinterface. For example, a Frame Relay interface might have a T1 connector nominally capable of 1.536 Mbps, and 64 subinterfaces on 128 kbps circuits (64K CIR), with 1200 and 100 kbps, respectively.

Reservations on individual circuits that do not exceed 100 kbps normally succeed. If, however, reservations have been made on other circuits adding up to 1.2 Mbps, and a reservation is made on a subinterface which itself has enough remaining bandwidth, it will still be refused because the physical interface lacks supporting bandwidth.

Enter Senders in the RSVP Database

You can configure the router to behave as though it is periodically receiving an RSVP PATH message from the sender or previous hop routes containing the indicated attributes. To enter senders in the RSVP database, perform the following task in global configuration mode:

Task	Command
Enter the senders in the RSVP database.	ip rsvp sender <i>session-ip-address sender-ip-address [tcp udp ip-protocol] session-dport sender-sport previous-hop-ip-address previous-hop-interface</i>

Enter Receivers in the RSVP Database

You can configure the router to behave as though it is continuously receiving an RSVP RESV message from the originator containing the indicated attributes. To enter receivers in the RSVP database, perform the following task in global configuration mode:

Task	Command
Enter the receivers in the RSVP database.	ip rsvp reservation <i>session-ip-address sender-ip-address [tcp udp ip-protocol] session-dport sender-sport next-hop-ip-address next-hop-interface {ff se wf} {rate load} [bandwidth] [burst-size]</i>

Enter Multicast Addresses

If RSVP neighbors are discovered to be using UDP encapsulation, the router will automatically generate UDP-encapsulated messages for consumption by the neighbors.

To enter multicast addresses, perform the following task in global configuration mode:

Task	Command
Enter any multicast addresses necessary if you use UDP.	ip rsvp udp-multicast <i>[multicast-address]</i>

However, in some cases, a host will not originate such a message until it has first heard from the router, which it can only do via UDP. You must instruct the router to generate UDP-encapsulated RSVP multicasts whenever it generates an IP-encapsulated multicast.

Control Which RSVP Neighbor Can Offer a Reservation

By default, any RSVP neighbor may offer a reservation. To control which RSVP neighbors can offer a reservation, perform the following task in global configuration mode:

Task	Command
Limit which routers may offer reservations.	ip rsvp neighbors <i>access-list-number</i>

When this command is configured, only neighbors conforming to the access list are accepted. The access list is applied to the IP header.

Monitor RSVP

After you configure the RSVP reservations that reflect your network resource policy, you can verify the resulting RSVP operations. To do so, perform the following tasks in EXEC mode:

Task	Command
Display RSVP-related interface information.	show ip rsvp interface <i>[type number]</i>
Display RSVP-related filters and bandwidth information.	show ip rsvp installed <i>[type number]</i>
Display current RSVP neighbors.	show ip rsvp neighbor <i>[type number]</i>
Display RSVP sender information.	show ip rsvp sender <i>[type number]</i>
Display RSVP request information.	show ip rsvp request <i>[type number]</i>
Display RSVP receiver information.	show ip rsvp reservation <i>[type number]</i>