



Quality of Service for Voice

This document describes quality of service (QoS) for voice and has the following sections:

- [QoS for Voice Overview, page 1](#)
- [QoS for Voice Configuration Prerequisites, page 10](#)
- [QoS for Voice Configuration Task List, page 10](#)
- [QoS for Voice Configuration Examples, page 13](#)

For a complete description of the voice commands used in this chapter, refer to the *Cisco IOS Voice Command Reference*, Release 12.3. To locate documentation for other commands that appear in this document, use the command reference master index or search online.

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

QoS for Voice Overview

Networks today are carrying more data than ever in the form of bandwidth-intensive, real-time voice, video, and data, which stretch network capability and resources. Cisco IOS software provides QoS solutions that help to solve problems caused by increasing traffic demands on a network.

QoS refers to the ability of a network, whether the network is a complex network, small corporate network, Internet service provider (ISP), or enterprise network, to provide better service to selected network traffic over various technologies, including Frame Relay, ATM, Ethernet and 802.1, and SONET, as well as IP routing networks that may use any or all of these underlying technologies.

The primary goals of QoS are to provide better and more predictable network service by providing dedicated bandwidth, controlled jitter and latency, and improved loss characteristics. QoS achieves these goals by providing tools for managing network congestion, shaping network traffic, using expensive wide-area links more efficiently, and setting traffic policies across the network.



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

Copyright © 2003 Cisco Systems, Inc. All rights reserved.

QoS provides these benefits:

- Control over bandwidth, equipment, and wide-area facilities. As an example, you can limit the bandwidth consumed over a backbone link by file transfer protocol (FTP) or queueing of an important database access.
- More efficient use of network resources—Network analysis management and accounting tools, enable you to know what your network is being used for and ensure that you are servicing the most important traffic to your business.
- Tailored services—QoS enables ISPs to offer carefully tailored grades of service differentiation to their customers.
- Coexistence of mission-critical applications—Cisco QoS technologies make certain that bandwidth and minimum delays required by time-sensitive multimedia and voice applications are available; and that other applications using the link get their fair service without interfering with mission-critical traffic.
- Foundation for a fully integrated network—Cisco QoS technologies fully integrates a multimedia network, for example, by implementing weighted fair queueing (WFQ) to increase service predictability and IP Precedence signaling for traffic differentiation. Also available is ReSerVation Protocol (RSVP), which allows you to take advantage of dynamically signaled QoS.

The basic QoS architecture has three components necessary to deliver QoS across a network comprising heterogeneous technologies (IP, ATM, LAN switches, and so on) as follows:

- QoS within a single network element (for example, queueing, scheduling, and traffic shaping tools)
- QoS signaling techniques for coordinating QoS from end-to-end between network elements
- QoS policy, management, and accounting functions to control and administer end-to-end traffic across a network

The next section describes the tools that Cisco IOS software provides in each section of the architecture, which, when combined, can create end-to-end QoS or simply solve specific problems at various points in the network.

For more information regarding the concepts and complexities of QoS, refer to the *Cisco IOS Quality of Service Solutions Configuration Guide* and *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.3. For more information about the configuration of playout delay (jitter), see the *Voice Port Configuration* document; and, for information about dial peers, see the document *Dial Peer Configuration on Voice Gateway Routers*, Cisco IOS Voice Configuration Library, Release 12.3.

For information about VoIP QoS support for Cisco Express Forwarding, and for Policy Based Routing, see the document *VoIP Interoperability with Cisco Express Forwarding and Policy Based Routing*, Cisco IOS Voice Configuration Library, Release 12.3.

QoS for Voice Tools

Cisco offers many tools for implementing QoS for voice. In general, each network has individual problems that you can solve using one or more of Cisco QoS tools. Voice over IP (VoIP) comes with its own set of problems (packet loss, jitter, and handling delay) and QoS can help solve some of these problems. Some of the problems QoS *cannot* solve are propagation delay, codec delay, sampling delay, and digitalization delay.

The International Telecommunication Union Telecommunication Standardization Sector (ITU-T) G.114 recommendation suggests no more than 150 milliseconds (ms) of end-to-end delay to maintain good voice quality.

This section contains a high-level overview of the following:

- [Edge Functions, page 3](#)
- [Packet Classification, page 5](#)
- [RSVP, page 5](#)
- [IP RTP Priority, page 7](#)

Edge Functions

As VoIP networks are designed, edge functions usually correspond to wide-area networks (WANs) that have less than a T1 or E1 line of bandwidth from the central site. The following concepts are discussed:

- [Bandwidth Limitations, page 3](#)
- [Real-Time Transport Protocol, page 4](#)
- [Queueing, page 4](#)

Bandwidth Limitations

The first issue of major concern when designing a VoIP network is bandwidth constraints. Depending upon which codec you use and how many voice samples you want per packet, the amount of bandwidth per call can increase drastically. For a list of bandwidth consumed by codec, see [Table 1](#).

Table 1 Codec Type and Sample Size Effects on Bandwidth

Codec	Bandwidth Consumed	Bandwidth Consumed with cRTP (2-Byte Header)	Sample Latency
G.729 with one 10-ms sample per frame	40 kbps	9.6 kbps	10 ms
G.729 with four 10-ms samples per frame	16 kbps	8.4 kbps	40 ms
G.729 with two 10-ms samples per frame	24 kbps	11.2 kbps	20 ms
G.711 with one 10-ms sample per frame	112 kbps	81.6 kbps	10 ms
G.711 with two 10-ms samples per frame	96 kbps	80.8 kbps	20 ms

In the table, 24 kbps of bandwidth is consumed when an 8-kbps codec is used. The amount of consumed bandwidth is affected by the codec used. For example, if the G.729 codec is used for two 10-ms samples, the amount of bandwidth consumed is 20 bytes per frame, which works out to 8 kbps. The packet headers that include IP, RTP, and User Datagram Protocol (UDP) add 40 bytes to each frame. The header is *twice* the amount of the payload.

If the G.729 codec is used with two 10-ms samples, without RTP header compression, 24 kbps are consumed in each direction per call. Although this might not be a large amount for T1 (1.544-mbps), E1 (2.048-mbps), or higher circuits, it is a large amount (42 percent) for a 56-kbps circuit.

Also, the bandwidth does not include layer 2 headers (PPP, Frame Relay, and so on). It includes headers from layer 3 (network layer) and above only. Therefore, the same G.729 call can consume different amounts of bandwidth based upon which data link layer is used (Ethernet, Frame Relay, PPP, and so on).

Real-Time Transport Protocol

To reduce the large percentage of bandwidth consumed by a G.729 voice call, you can use compressed Real-Time Transport Protocol (cRTP). cRTP enables you to compress the 40-byte IP/RTP/UDP header to 2 to 4 bytes most of the time.

With cRTP, the amount of traffic per VoIP call is reduced from 24 kbps to 11.2 kbps. This is a major improvement for low-bandwidth links. A 56-kbps link, for example, can now carry four G.729 VoIP calls at 11.2 kbps each. Without cRTP, only two G.729 VoIP calls at 24 kbps can be used.

To avoid the unnecessary consumption of available bandwidth, cRTP is used on a link-by-link basis. This compression scheme reduces the IP/RTP/UDP header to 2 bytes when UDP checksums are not used, or 4 bytes when UDP checksums are used.

cRTP uses some of the same techniques as TCP header compression. In TCP header compression, the first factor-of-two reduction in data rate occurs because half of the bytes in the IP and TCP headers remain constant over the life of the connection.

The big gain, however, comes from the fact that the difference from packet to packet is often constant, even though several fields change in every packet. Therefore, the algorithm can simply add 1 to every value received. By maintaining both the uncompressed header and the first-order differences in the session state shared between the compressor and the decompressor, cRTP must communicate only an indication that the second-order difference is zero. In that case, the decompressor can reconstruct the original header without any loss of information, simply by adding the first-order differences to the saved, uncompressed header as each compressed packet is received.

Just as TCP/IP header compression maintains shared state for multiple simultaneous TCP connections, this IP/RTP/UDP compression must maintain state for multiple session contexts. A *session context* is defined by the combination of the IP source and destination addresses, the UDP source and destination ports, and the RTP synchronization source (SSRC) field. A compressor implementation might use a hash function on these fields to index a table of stored session contexts.

The compressed packet carries a small integer, called the *session context identifier*, or CID, to indicate in which session context that packet should be interpreted. The decompressor can use the CID to index its table of stored session contexts.

cRTP can compress the 40 bytes of header down to 2 to 4 bytes most of the time. As such, about 98 percent of the time the compressed packet will be sent. Periodically, however, an entire uncompressed header must be sent to verify that both sides have the correct state. Sometimes, changes occur in a field that is usually constant, such as the payload type field. In such cases, the IP/RTP/UDP header cannot be compressed, so an uncompressed header must be sent.

You should use cRTP on any WAN interface where voice bandwidth is a concern and a high proportion of RTP traffic exists.

Queueing

Queueing is like the concept of first in first out (FIFO), which means that the first in line is the first to get out of the line. FIFO queueing was the first type of queueing to be employed in routers, and it is still useful, depending upon the network topology. In networks today, with a variety of applications, protocols, and users, a way to classify different traffic is required.

Cisco has several queueing tools that enable a network administrator to specify what type of traffic is special or important and to queue the traffic based upon that information. The most popular technique is WFQ.

There are the several queueing types that are listed below. For more information, see the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.3 and *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.3:

- Weighted fair queueing
- Custom queueing
- Priority queueing
- Class-based (CB) WFQ
- Priority queueing (PQ) with CB-WFQ

Packet Classification

To achieve your intended packet delivery, you must know how to properly weight WFQ. There are different weighting techniques and ways to use them in various networks to achieve the degree of QoS you require.

IP Precedence

IP precedence is a value defined by the three bits in the type of service (ToS) field in an IP header. IP Precedence enables a router to group traffic flows based upon the eight precedence settings and to queue traffic based upon that information as well as on source address, destination address, and port numbers.

Policy Routing

Policy routing is a routing scheme that forwards packets to specific interfaces based on user-configured policies. Such policies might specify that traffic sent from a particular network should be forwarded out one interface, while all other traffic should be forwarded out another interface.

With policy-based routing, you can configure a defined policy for traffic flows and not have to rely completely on routing protocols to determine traffic forwarding and routing. Policy routing also enables you to set the IP precedence field so that the network can utilize different classes of service.

You can base policies on IP addresses, port numbers, protocols, or the size of packets. You can use one of these descriptors to create a simple policy, or you can use all of them to create a complicated policy.

All packets received on an interface with policy-based routing enabled are passed through enhanced packet filters known as *route maps*. The route maps dictate where the packets are forwarded.

RSVP

RSVP enables endpoints to signal the network with the kind of QoS needed for a particular application. Most networks are designed to assume what QoS applications require. Network administrators can use RSVP as *dynamic access lists*. Using RSVP means that network administrators do not need to be concerned with port numbers of IP packet flows because RSVP signals that information during its original request.

RSVP is an out-of-band, end-to-end signaling protocol that requests a certain amount of bandwidth and latency with each network hop that supports RSVP. If a network node (router) does not support RSVP, RSVP moves onto the next hop. A network node has the option to approve or deny the reservation based upon the load of the interface to which the service is requested.

VoIP Call Admission Control

Cisco VoIP call admission control (CAC) applications use RSVP to limit the accepted voice load on the IP network and guarantee the QoS levels of calls. The VoIP CAC using RSVP synchronizes RSVP signaling with Cisco H.323 Version 2 and above signaling to ensure that the bandwidth reservation is established in both directions before a call moves to the alerting phase (ringing). This ensures that the called party phone rings only after the resources for the call have been reserved. Using RSVP-based admission control, VoIP applications can reserve network bandwidth and react appropriately if bandwidth reservation fails.



Note

Prior to Cisco IOS Release 12.1(5)T, VoIP gateways used H.323 Version 1 (Slow Connect) procedures when initiating calls requiring bandwidth reservation. In later releases, gateways use H.323 Version 2 (Fast Connect) for all calls, including those requiring RSVP. Fast Connect is enabled by default.

To enable backward compatibility, commands are available to force the originating gateway to initiate calls using Slow Connect procedures if the terminating gateway is running Cisco IOS Release 12.1(1)T or later. You can configure Slow Connect globally for all VoIP calls by using the **h323 call start** voice-service configuration command, or configure Slow Connect per individual VoIP dial peer by using the **call start** voice-class configuration command.

A timer can be set by using the **call rsvp-sync serv-timer** command to limit the number of seconds that the terminating gateway waits for bandwidth reservation setup before proceeding with the call setup or releasing the call, depending on the configured QoS level in the dial peers.

Synchronized RSVP is attempted for a VoIP call as long as the requested (desired) QoS for the associated dial peer is set to controlled-load or guaranteed-delay. If the requested QoS level is set to the default of best-effort, bandwidth reservation is not attempted. If RSVP reservation is attempted but fails, the acceptable QoS for the dial peer determines the outcome of the call. When the acceptable QoS is configured for best effort, the call setup proceeds, but without any bandwidth reservation in place. When the acceptable QoS on either gateway is configured for other than best effort, and the RSVP reservation fails, the call is released. The requested QoS and acceptable QoS are configured through Cisco IOS software by using the **req-qos** and **acc-qos** dial-peer configuration commands, respectively.

Table 2 summarizes the results of nine call setup scenarios using Fast Connect, based on the QoS levels configured in the VoIP dial peers at the originating and terminating gateways. The table does not include cases where the requested QoS is best-effort and the acceptable QoS is other than best-effort and is valid only for calls using Fast Connect procedures.

Table 2 Call Results Based on Configured QoS Levels

Call Scenarios	Originating Gateway		Terminating Gateway		Results
	Requested QoS	Acceptable QoS	Requested QoS	Acceptable QoS	
1	controlled-load or guaranteed-delay	controlled-load or guaranteed-delay	controlled-load or guaranteed-delay	controlled-load or guaranteed-delay	Call proceeds only if both RSVP reservations succeed.
2	controlled-load or guaranteed-delay	controlled-load or guaranteed-delay	controlled-load or guaranteed-delay	best-effort	Call proceeds only if both RSVP reservations succeed.
3	controlled-load or guaranteed-delay	controlled-load or guaranteed-delay	best-effort	best-effort	Call is released.

Table 2 Call Results Based on Configured QoS Levels (continued)

Call Scenarios	Originating Gateway		Terminating Gateway		Results
	Requested QoS	Acceptable QoS	Requested QoS	Acceptable QoS	
4	controlled-load or guaranteed-delay	best-effort	controlled-load or guaranteed-delay	controlled-load or guaranteed-delay	Call proceeds only if both RSVP reservations succeed.
5	controlled-load or guaranteed-delay	best-effort	controlled-load or guaranteed-delay	best-effort	Call proceeds regardless of RSVP results. If RSVP reservation fails, call receives best-effort service.
6	controlled-load or guaranteed-delay	best-effort	best-effort	best-effort	Call proceeds with best-effort service.
7	best-effort	best-effort	controlled-load or guaranteed-delay	controlled-load or guaranteed-delay	Call is released.
8	best-effort	best-effort	controlled-load or guaranteed-delay	best-effort	Call proceeds with best-effort service.
9	best-effort	best-effort	best-effort	best-effort	Call proceeds with best-effort service.

The following are the benefits of using CAC with RSVP:

- VoIP gateways default to H.323 Version 2 (Fast Connect) for all calls.
- Called-party phone rings only after bandwidth reservation is confirmed.
- QoS for voice calls is guaranteed across the IP network.

The following are restrictions on VoIP CAC using RSVP:

- To support RSVP-based QoS with H.323 Version 2 (Fast Connect), the originating and terminating gateways must be running Cisco IOS Release 12.1(5)T, or later.
- To support RSVP-based QoS with H.323 Version 1 (Slow Connect), Cisco H.323 Version 2 gateways must be running Cisco IOS Release 12.1(1)T or later.
- RSVP with multicast is not supported.

IP RTP Priority

When WFQ is enabled and IP RTP priority is configured, a strict priority queue is created. You can use IP RTP priority to enable use of the strict priority queueing scheme for delay-sensitive data. You can identify voice traffic by its UDP port numbers and classify it into a priority queue. The result is voice traffic that has strict priority service in preference to all other traffic. This is the most highly recommended classification scheme for VoIP networks on lower-bandwidth links (768 kbps and below).

Traffic Policing for Voice Networks

The preceding sections cover ways you can queue different flows of traffic and then prioritize those flows, an important part of QoS. Sometimes, however, it is necessary to actually regulate or limit the amount of traffic an application is allowed to send across various interfaces or networks.

Cisco IOS software has a few tools that enable network administrators to define how much bandwidth an application or even a user can use. These features have two different tools: *rate-limiting* and *shaping*.

The main difference between these two traffic-regulation tools is that rate-limiting tools drop traffic based upon policing, and shaping tools generally buffer the excess traffic while waiting for the next open interval to transmit the data.

The similarities are in that both the rate-limiting and shaping tools identify when traffic exceeds the thresholds set by the network administrator. Often, these two tools are used together. Traffic shaping is used at the edge of the network to make sure the network is utilizing the bandwidth for business needs. Rate-limiting tools often used in service provider networks to ensure that a subscriber does not exceed the amount of bandwidth set by contract with the service provider.

You can rate-limit traffic by precedence, Media Access Control (MAC) address, IP addresses, or other parameters. Network administrators also can configure access lists to create even more granular rate-limiting policies.

Traffic Shaping for Voice Networks

Cisco IOS QoS software includes two types of traffic-shaping tools: Generic Traffic Shaping (GTS) and Frame Relay traffic shaping (FRTS). The two traffic-shaping methods are similar in implementation, although their command-line interfaces differ somewhat and they use different types of queues to contain and shape traffic that is deferred.

If a packet is deferred, GTS uses a WFQ to hold the delayed traffic. FRTS uses either a custom queue (CQ) or a priority queuing (PQ) to hold the delayed traffic, depending on what you configured. FRTS also supports WFQ to hold delayed traffic.

Traffic shaping enables you to control the traffic going out of an interface to match its flow to the speed of the remote, target interface and to ensure that the traffic conforms to policies contracted for it. Thus, you can shape traffic adhering to a particular profile to meet downstream requirements, thereby eliminating bottlenecks in topologies with data-rate mismatches.

Use traffic shaping primarily for the following purposes:

- Control usage of available bandwidth
- Establish traffic policies
- Regulate traffic flow to avoid congestion

You can also use traffic shaping to do the following:

- Configure an interface if you have a network with different access rates. Suppose one end of the link in a Frame Relay network runs at 256 kbps and the other end runs at 128 kbps. Sending packets at 256 kbps could cause the applications using the link to fail.
- Configure an interface to offer a subrate service. In this case, traffic shaping enables you to use the router to partition your T1 or T3 links into smaller channels.

Traffic shaping prevents packet loss. It is especially important to use traffic shaping in Frame Relay networks because the switch cannot determine which packets take precedence and, therefore, which packets should be dropped when congestion occurs. It is critical for VoIP that you control latency. By limiting the amount of traffic and traffic loss in the network, you can smooth out traffic patterns and give priority to real-time traffic.

High-Speed Transport

High-speed transport is defined as any interface higher than T1 speed. The QoS mechanisms required to configure a high-speed transport are as follows:

- Packet Over SONET/SDH (POS)—Prioritizes traffic on this high-speed interface up to OC-48.
- Modified deficit round robin (MDRR)—Extends Deficit Round Robin (DRR) to provide priority for real-time traffic such as VoIP. Within MDRR, IP packets are mapped to different CoS queues based on precedence bits. All the queues are serviced in round-robin fashion except for one: the priority queue used to handle voice traffic.
- IP and ATM—Maps IP prioritization onto ATM by configuring precedence values to an IP packet to different ATM PVCs. The IP prioritization enables the network administrator to have different PVCs, allocating more important traffic over a variable bit rate (VBR) ATM circuit and less important traffic over an unspecified bit rate (UBR) ATM circuit; or IP prioritization onto ATM using queueing techniques such as WFQ to prioritize different flows by PVC.

Refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.3, and *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.3, for detailed information.

Congestion Avoidance

Congestion avoidance works by dropping packets from different flows, causing applications to slow the amount of traffic being sent.

WRED

Random Early Detection (RED) is a congestion avoidance mechanism, and Weighted RED (WRED) is the Cisco IOS software implementation of dropping traffic to avoid global synchronization. WRED combines the capabilities of the RED algorithm with IP precedence. This combination provides for preferential traffic handling for higher-priority packets. It can selectively discard lower-priority traffic when the interface starts to get congested and provide differentiated performance characteristics for different classes of service. To fully comprehend how WRED works, you must understand TCP packet-loss behavior.

TCP

A stream of data sent on a TCP connection is delivered reliably and in order to the destination. Transmission is made reliable through the use of sequence numbers and acknowledgments. Segments (segments sequentially numbered) carry an acknowledgment number, which is the sequence number of the next expected data octet of transmissions in the reverse direction. When the TCP transmits a segment,

it puts a copy on a retransmission queue and starts a timer; when the acknowledgment for that data is received, the segment is deleted from the queue. If the acknowledgment is not received before the timer runs out, the segment is retransmitted.

To govern the flow of data into a TCP, flow control mechanisms are used. The data-receiving TCP reports a window to the sending TCP. This window specifies the number of octets, starting with the acknowledgment number that the data-receiving TCP is currently prepared to receive.

QoS for Voice Configuration Prerequisites

The following are tasks that must be performed prior to configuring QoS for voice:

- Establish a working IP network. For information about configuring IP, see the *Cisco IOS IP Routing Configuration Guide*, Release 12.3.
- Configure your VoIP gateway for H.323. To support RSVP-based QoS with H.323 Version 2 (Fast Connect), the originating and terminating gateways must be running Cisco IOS Release 12.1(5)T, or later. For information about configuring the gateway, refer to the *Cisco IOS H.323 Configuration Guide*, Cisco IOS Voice Configuration Library, Release 12.3.
- Enable RSVP on the appropriate interfaces on your gateways by using the **ip rsvp bandwidth** interface configuration command. You must also enable fair queueing on these interfaces by using the **fair-queue** interface configuration command. For information about enabling RSVP and fair queueing, refer to the *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.3.
- Set the QoS levels in your dial peers by using the **req-qos** and **acc-qos** dial-peer configuration commands. For information about configuring QoS levels, see the document *Dial Peer Configuration on Voice Gateway Routers*, Cisco IOS Voice Configuration Library, Release 12.3.



Note

An inbound plain old telephone service (POTS) dial peer is not required if the originating and terminating gateways have outbound VoIP dial peers configured to reach the calling number at the far end and if the VoIP dial peers use the same QoS parameters. Configure an inbound POTS dial peer if the corresponding outbound VoIP dial peers at the originating and terminating gateways do not have matching QoS configurations, or if calls can be established in only one direction (for example, or if calls can be made from gateway A to gateway B, but not from gateway B to gateway A).

For information on how to configure playout delay, echo cancellation, and voice levels, see the document *Voice Port Configuration*, Cisco IOS Voice Configuration Library, Release 12.3.

QoS for Voice Configuration Task List

Refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.3, and *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.3, for tasks that enable QoS for your network. To configure the H.323 gateway, refer to the H.323 documents in the Cisco IOS Voice Configuration Library, Release 12.3.

The following sections describe optional configuration tasks for the VoIP Call Admission Control Using RSVP feature. The tasks in the first section are for configuring synchronization:

- [Configuring Synchronization and the Reservation Timer, page 11](#) (Optional)

Use the following tasks only if you require backward compatibility with H.323, Version 2 (Slow Connect) gateways running a release earlier than Cisco IOS Release 12.1(5)T:

- [Configuring Slow Connect for VoIP Globally](#), page 11 (Optional)
- [Configuring Slow Connect for a Specific Dial Peer](#), page 12 (Optional)

Configuring Synchronization and the Reservation Timer

Synchronization between RSVP and the H.323 voice signaling protocol is enabled by default; no configuration tasks are required to enable this feature. To enable the feature if the **no call rsvp sync** command was used to disable it, use the following commands in global configuration mode:

	Command	Purpose
Step 1	Router(config)# call rsvp sync	Enables synchronization between RSVP and the H.323 voice signaling protocol.
Step 2	Router(config)# call rsvp-sync resv-timer <i>seconds</i>	Sets the timer for reservation requests. The default is 10 seconds.

Configuring Slow Connect for VoIP Globally

To make an H.323 gateway backward-compatible with a destination gateway, use the following commands beginning in global configuration mode. This procedure is optional and selects Slow Connect globally for all VoIP services.

	Command	Purpose
Step 1	Router(config)# voice service voip	Enters voice-service configuration mode for VoIP services.
Step 2	Router(conf-voi-serv)# h323 call start slow	Forces the H.323 gateway to use Slow Connect procedures. Note To restore the default of Fast Connect, use the h323 call start fast command.



Note

The previous procedure selects Slow Connect globally for all VoIP calls. To change the type of connect procedures for calls associated with a specific dial peer, use the following procedure:

Configuring Slow Connect for a Specific Dial Peer


Note

This procedure is optional and selects Slow Connect for a specific VoIP dial peer.

To make an H.323 gateway backward-compatible with a destination gateway, use the following commands beginning in global configuration mode:

	Command	Purpose
Step 1	Router(config)# voice class h323 tag	Enters voice-class configuration mode and creates a voice class for H.323 attributes.
Step 2	Router(config-class)# call start slow or Router(config-class)# call start system	Forces the H.323 gateway to use Slow Connect procedures. The default is slow . The keyword system causes the H.323 gateway to use the connect procedure that is configured in the voice-service configuration (see Configuring Slow Connect for VoIP Globally). Note If you require Fast Connect for a specific dial peer, use the call start fast command to restore the default when configuring the Slow Connect for VoIP globally.
Step 3	Router(config-class)# exit	Exits voice-class configuration mode and returns to global configuration mode.
Step 4	Router(config)# dial-peer voice number voip	Enters dial-peer configuration mode for the VoIP dial peer.
Step 5	Router(config-dial-peer)# voice-class h323 tag	Assigns the voice class attributes to the dial peer, including the H.323 connect procedure that was selected in Step 2.

Verifying the RSVP CAC Configuration

To verify that RSVP-based call admission control is configured correctly, enter the **show running-config** privileged EXEC command to display the command settings for the router, as shown in the “QoS for Voice Configuration Examples” section on page 13.

Monitoring and Maintaining RSVP Call Admission Control

To display the configuration parameters for RSVP synchronization and statistics for calls that initiate RSVP, use the following commands in privileged EXEC mode:

	Command	Purpose
Step 1	Router# show call rsvp-sync conf	Displays the RSVP synchronization configuration.
Step 2	Router# show call rsvp-sync stats	Displays statistics for calls that attempted RSVP reservation.

QoS for Voice Configuration Examples

Refer to the *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.3 and *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.3 for more information.

The following examples display the screen output using the **show running-config** command:

- [RSVP Synchronization Examples, page 13](#)
- [H.323 Slow Connect by Voice Service Example, page 14](#)
- [H.323 Slow Connect by Dial Peer Example, page 14](#)

RSVP Synchronization Examples

In the example shown in [Figure 1](#), calls can be made in either direction between gateway A and gateway B, which are connected to POTS phones, with phone numbers 711 and 712, respectively. The requested QoS indicates that RSVP setup must be complete before the destination phone rings. The acceptable QoS indicates that the call is released if the RSVP setup fails or is not complete within the allotted time.

Figure 1 RSVP Synchronization Example



Gateway A	Gateway B
<pre> call rsvp-sync call rsvp-sync resv-timer 15 ! interface Ethernet0/0 ip address 10.10.107.107 10.255.255.255 fair-queue 64 256 31 ip rsvp bandwidth 1000 1000 ! voice-port 3/0/0 ! dial-peer voice 712 voip destination-pattern 712 session target ipv4:10.10.107.108 req-qos controlled-load acc-qos controlled-load ! dial-peer voice 711 pots destination-pattern 711 port 3/0/0 </pre>	<pre> call rsvp-sync call rsvp-sync resv-timer 15 ! interface Ethernet0/0 ip address 10.10.107.108 10.255.255.255 fair-queue 64 256 31 ip rsvp bandwidth 1000 1000 ! voice-port 2/0/0 ! dial-peer voice 711 voip destination-pattern 711 session target ipv4:10.10.107.107 req-qos controlled-load acc-qos controlled-load ! dial-peer voice 712 pots destination-pattern 712 port 2/0/0 </pre>

H.323 Slow Connect by Voice Service Example

The following example shows that Slow Connect is configured globally for all VoIP calls because the **h323 call start slow** command is used in the voice service configuration:

```
dial-peer voice 712 voip
 destination-pattern 712
 session target ipv4:10.10.107.108
 req-qos controlled-load
 acc-qos controlled-load
!
voice service voip
 h323 call start slow
```

The following example shows the same basic configuration but demonstrates that when the **call start system** command is used in the voice class configuration, the gateway defaults to the connect procedure that is configured in the voice service; otherwise the dial peer configuration takes precedence (see the section [“H.323 Slow Connect by Dial Peer Example”](#) section on page 14).

```
dial-peer voice 712 voip
 voice-class h323 2
 destination-pattern 712
 session target ipv4:10.10.107.108
 req-qos controlled-load
 acc-qos controlled-load
!
voice class h323 2
 call start system
!
voice service voip
 h323 call start slow
!
```

H.323 Slow Connect by Dial Peer Example

The following example shows that calls from VoIP dial peer 712 use Slow Connect procedures because the **call start slow** command is configured in the voice class assigned to the dial peer:

```
dial-peer voice 712 voip
 voice-class h323 2
 destination-pattern 712
 session target ipv4:10.10.107.108
 req-qos controlled-load
 acc-qos controlled-load
!
voice class h323 2
 call start slow
!
voice service voip
 h323 call start fast
!
```



Note

The **h323 call start fast** voice-service command is ignored because the voice class configuration takes precedence, unless the **call start system** voice-class command is used (see the section [““H.323 Slow Connect by Voice Service Example”](#) section on page 14”).