



Configuring VoIP

The Catalyst 4224 Access Gateway Switch (Catalyst 4224) provides Voice-over-IP (VoIP) gateway applications for a *micro branch* office. This section provides comprehensive information on how to configure VoIP on your Catalyst 4224.

This section contains the following topics:

- [Prerequisite Tasks, page 6-1](#)
- [Configuration Tasks, page 6-2](#)
- [Configure IP Networks for Real-Time Voice Traffic, page 6-3](#)
- [Configure Number Expansion, page 6-12](#)
- [Configure Dial Peers, page 6-15](#)
- [Configure Voice Ports, page 6-22](#)
- [Additional VoIP Dial-Peer Configurations, page 6-32](#)
- [Configure Frame Relay for VoIP, page 6-36](#)

Prerequisite Tasks

Before you can configure your Catalyst 4224 to use VoIP, you need to perform the following tasks:

- Establish a working IP network. For more information about configuring IP, refer to the “IP Overview,” “Configuring IP Addressing,” and “Configuring IP Services” sections in the *Network Protocols Configuration Guide, Part 1* for Cisco IOS Release 12.0 T.
- Install the voice interface cards (VICs) in your Catalyst 4224. For more information about installing a VIC in your Catalyst 4224, refer to the *Cisco WAN Interface Cards Hardware Installation Guide*.
- Complete your company dial plan.
- Establish a working telephony network based on your company dial plan.
- Integrate your dial plan and telephony network into your existing IP network topology. Merging your IP and telephony networks depends on your particular IP and telephony network topology. In general, Cisco recommends the following:
 - Use canonical numbers wherever possible. Avoid situations in which numbering systems are significantly different on different Catalyst 4224s or access servers in your network.
 - Make routing and dialing transparent to the user; for example, try to avoid secondary dial tones from secondary switches.
 - Contact your private branch exchange (PBX) vendor for instructions on how to reconfigure the appropriate PBX interfaces.

After you have analyzed your dial plan and decided how to integrate it into your existing IP network, you are ready to configure your network devices to support VoIP.

Configuration Tasks

To configure VoIP on your Catalyst 4224, perform the following steps:

-
- Step 1** Configure your IP network to support real-time voice traffic. See the [“Configure IP Networks for Real-Time Voice Traffic” section on page 6-3](#) for information about selecting and configuring the appropriate quality of service (QoS) tool or tools to optimize voice traffic on your network.
 - Step 2** (Optional) If you plan to run Voice over Frame Relay, you need to consider certain factors so that VoIP runs smoothly. For example, a public Frame Relay cloud provides no guarantees for QoS. See the [“Configure Frame Relay for VoIP” section on page 6-36](#) for information about deploying VoIP over Frame Relay.
 - Step 3** Use the **num-exp** command to configure number expansion if your telephone network is configured so that you can reach a destination by dialing only an extension number of the full E.164 telephone number. See the [“Configure Number Expansion” section on page 6-12](#) for information about number expansion.
 - Step 4** Use the **dial-peer voice** command to define dial peers and switch to the dial-peer configuration mode. See the [“Configure Dial Peers” section on page 6-15](#) and the [“Additional VoIP Dial-Peer Configurations” section on page 6-32](#) for additional information about configuring dial peers and dial-peer characteristics.
 - Step 5** Configure your Catalyst 4224 to support voice ports. See the [“Configure Voice Ports” section on page 6-22](#) for information about configuring voice ports.
-

Configure IP Networks for Real-Time Voice Traffic

You need to have a well engineered end-to-end network when running delay-sensitive applications such as VoIP. Fine-tuning your network to adequately support VoIP involves a series of protocols and features to improve QoS. It is beyond the scope of this document to explain the specific details relating to wide-scale QoS deployment.

Cisco IOS software provides many tools for enabling QoS on your network backbone. These tools include Random Early Detection (RED), Weighted Random Early Detection (WRED), Fancy Queuing (meaning custom, priority, or

weighted fair queuing), and IP precedence. To configure your IP network for real-time voice traffic, you need to consider the entire scope of your network and then select the appropriate QoS tool or tools.

To improve voice network performance, QoS must be configured throughout your network, not just on your Catalyst 4224 running VoIP. Not all QoS techniques are appropriate for all network routers. Edge routers and backbone routers in your network do not necessarily perform the same operations, and the QoS tasks they perform might differ as well. To configure your IP network for real-time voice traffic, you need to consider the functions of both edge and backbone routers in your network and then select the appropriate QoS tool or tools.

In general, edge routers perform the following QoS functions:

- Packet classification
- Admission control
- Bandwidth management
- Queuing

In general, backbone routers perform the following QoS functions:

- High-speed switching and transport
- Congestion management
- Queue management

Scalable QoS solutions require cooperative edge and backbone functions.

Although not mandatory, some QoS tools can be valuable in fine-tuning your network to support real-time voice traffic. To configure your IP network for QoS, perform one or more of the following tasks:

- [Configure RSVP for Voice, page 6-4](#)
- [Configure Multilink Point-to-Point Protocol with Interleaving, page 6-6](#)
- [Configure Real-Time Transport Protocol Header Compression, page 6-9](#)
- [Configure Custom Queuing, page 6-11](#)
- [Configure Weighted Fair Queuing, page 6-12](#)

Each of these tasks is discussed in the following sections.

Configure RSVP for Voice

Resource Reservation Protocol (RSVP) enables routers to reserve enough bandwidth on an interface to provide reliable, high-quality performance. RSVP allows end systems to request a particular QoS from the network. Real-time voice traffic requires network consistency. Without consistent QoS, real-time traffic can experience jitter, insufficient bandwidth, delay variations, or information loss. RSVP works in conjunction with current queuing mechanisms. The interface queuing mechanism (such as weighted fair queuing or WRED) must implement the reservation.

RSVP works well on PPP, HDLC, and similar serial line interfaces. It does not work well on multiaccess LANs. RSVP can be equated to a dynamic access list for packet flows.

You should configure RSVP to ensure QoS if the following conditions describe your network:

- Small-scale voice network implementation
- Links slower than 2 Mbps
- Links with high utilization
- Need for the best possible voice quality

Enable RSVP

To minimally configure RSVP for voice traffic, you must enable RSVP on each interface where priority is required.

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, use the following command:

```
ip rsvp bandwidth [interface-kbps] [single-flow-kbps]
```

interface-kbps represents the maximum amount of bandwidth, in kbps, that may be allocated by RSVP flows and *single-flow-kbps* represents the maximum amount of bandwidth, in kbps, that may be allocated to a single flow. The range for both arguments is from 1 to 10,000,000.

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, RSVP applies to the more restrictive of the available bandwidths of the physical interface and the subinterface.

Reservations on individual circuits that do not exceed the single flow limit normally succeed. However, if reservations have been made on other circuits adding up to the line speed, and a reservation is made on a subinterface that itself has enough remaining bandwidth, the reservation will be refused. The reason the reservation will be refused is because the physical interface lacks supporting bandwidth.

A Cisco 1750 running VoIP and configured for RSVP requests allocations by using the following formula:

$$\text{bps} = \text{packet_size} + \text{ip/udp/rtp header size} \times 50 \text{ per second}$$

For the codec standard G.729, wherein voice is coded into 8-kbps streams, the allocation works out to be 24,000 bps. For G.711, the allocation is 80,000 bps.

For more information about configuring RSVP, refer to the “Configuring RSVP” section of the *Network Protocols Configuration Guide, Part 1* for Cisco IOS Release 12.0 T.

RSVP Configuration Example

The following example enables RSVP and sets the maximum bandwidth to 100 kbps and the maximum bandwidth per single request to 32 kbps. The example presumes that both VoIP dial peers have been configured.

```
c4224(config)# interface serial 0/0
c4224(config-if)# ip rsvp bandwidth 100 32
c4224(config-if)# fair-queue
c4224(config-if)# end
```

After enabling RSVP, you must also use the **req-qos dial-peer** configuration command to request an RSVP session on each VoIP dial peer. Otherwise, no bandwidth is reserved for voice traffic.

```
c4224(config)# dial-peer voice 211 voip
c4224(config-dial-peer)# req-qos controlled-load
c4224(config)# dial-peer voice 212 voip
c4224(config-dial-peer)# req-qos controlled-load
```

Configure Multilink Point-to-Point Protocol with Interleaving

Multiclass multilink Point-to-Point Protocol (PPP) interleaving allows large packets to be multilink-encapsulated and fragmented into smaller packets to satisfy the delay requirements of real-time voice traffic. Small real-time packets, which are not multilink-encapsulated, are transmitted between fragments of the large packets.

The interleaving feature also provides a special transmit queue for the smaller, delay-sensitive packets, enabling them to be transmitted earlier than other flows. Interleaving provides the delay bounds for delay-sensitive voice packets on a slow link that is used for other best-effort traffic.

In general, multilink PPP with interleaving is used in conjunction with weighted fair queuing and RSVP or IP precedence to ensure voice packet delivery. Use multilink PPP with interleaving and weighted fair queuing to define how data is managed; use RSVP or IP precedence to give priority to voice packets.

You should configure multilink PPP if the following conditions describe your network:

- Point-to-point connection using PPP encapsulation
- Links slower than two Mbps



Note

Do not use multilink PPP on links faster than two Mbps.

You can configure multilink PPP support for interleaving on virtual templates, dialer interfaces, and ISDN Basic Rate Interface (BRI) or Primary Rate Interface (PRI) interfaces. To configure interleaving, perform the following tasks:

- Configure the dialer interface or virtual template, as defined in the relevant chapters of the *Dial Solutions Configuration Guide* for Cisco IOS Release 12.0T.
- Configure multilink PPP and interleaving on the interface or template.

To configure multilink PPP and interleaving on a configured and operational interface or virtual interface template, use the following interface configuration commands:

	Task	Command
Step 1	Enable Multilink PPP.	<code>ppp multilink</code>
Step 2	Enable real-time packet interleaving.	<code>ppp multilink interleave</code>
Step 3	Optionally, configure a maximum fragment delay of up to 20 milliseconds.	<code>ppp multilink fragment-delay milliseconds</code>
Step 4	Reserve a special queue for real-time packet flows to specified destination User Datagram Protocol (UDP) ports, allowing real-time traffic to have higher priority than other flows. This applies only if you have not configured RSVP.	<code>ip rtp reserve lowest-UDP-port range-of-ports [maximum-bandwidth]</code>



Note

You can use the **ip rtp reserve** command instead of configuring RSVP. If you configure RSVP, this command is not required.

For more information about multilink PPP, refer to the “Configuring Media-Independent PPP and Multilink PPP” section in the *Dial Solutions Configuration Guide* for Cisco IOS Release 12.0 T.

Multilink PPP Configuration Example

The following example defines a virtual interface template that enables multilink PPP with interleaving and a maximum real-time traffic delay of 20 milliseconds, and then applies that virtual template to the multilink PPP bundle:

```
c4224(config)# interface virtual-template 1
c4224(config-if)# ppp multilink
c4224(config-if)# encapsulated ppp
c4224(config-if)# ppp multilink interleave
c4224(config-if)# ppp multilink fragment-delay 20
c4224(config-if)# ip rtp reserve 16384 100 64

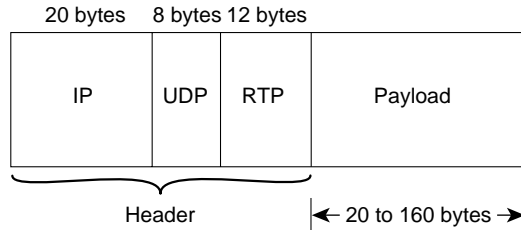
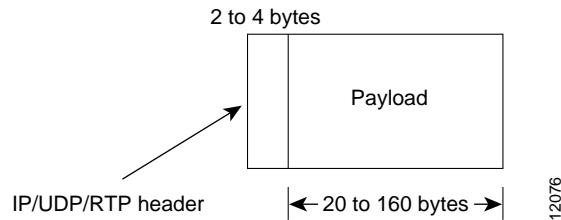
c4224(config)# multilink virtual-template 1
```

Configure Real-Time Transport Protocol Header Compression

Real-Time Transport Protocol (RTP) is used for carrying audio traffic in packets over an IP network. RTP header compression compresses the RTP/UDP/IP header in an RTP data packet from 40 bytes to approximately 2 to 4 bytes, in most cases, as shown in [Figure 6-1](#).

This compression feature is beneficial if you are running VoIP over slow links. Enabling compression on both ends of a low-bandwidth serial link can greatly reduce the network overhead if there is a lot of RTP traffic on that slow link.

Typically, an RTP packet has a payload of approximately 20 to 160 bytes for audio applications that use compressed payloads. RTP header compression is especially beneficial when the RTP payload size is small (for example, compressed audio payloads between 20 and 50 bytes).

Figure 6-1 RTP Header Compression**Before RTP header compression:****After RTP header compression:**

You should configure RTP header compression if the following conditions describe your network:

- Links slower than two Mbps
- Need to save bandwidth

**Note**

Do not use RTP header compression on links faster than two Mbps.

Perform the following tasks to configure RTP header compression for VoIP. The first task is required, but the second task is optional.

- [Enable RTP Header Compression on a Serial Interface, page 6-11](#)
- [Change the Number of Header Compression Connections, page 6-11](#)

Enable RTP Header Compression on a Serial Interface

You need to enable compression on both ends of a serial connection. To enable RTP header compression, use the following interface configuration command:

```
c4224(config-if)# ip rtp header-compression [passive]
```

If you include the **passive** keyword, the software compresses outgoing RTP packets only if incoming RTP packets on the same interface are compressed. If you use the command without the **passive** keyword, the software compresses all RTP traffic.

Change the Number of Header Compression Connections

By default, the software supports a total of 16 RTP header compression connections on an interface. To specify a different number of RTP header compression connections, use the following interface configuration command:

```
c4224(config-if)# ip rtp compression connections number
```

RTP Header Compression Configuration Example

The following example enables RTP header compression for a serial interface:

```
c4224(config)# interface serial0
c4224(config-if)# ip rtp header-compression
c4224(config-if)# encapsulation ppp
c4224(config-if)# ip rtp compression-connections 25
```

For more information about RTP header compression, see the “Configuring IP Multicast Routing” section of the *Network Protocols Configuration Guide, Part 1* for Cisco IOS Release 12.0 T.

Configure Custom Queuing

Some QoS features, such as IP RTP reserve and custom queuing, are based on the transport protocol and the associated port number. Real-time voice traffic is carried on UDP ports ranging from 16384 to 16624. This range is derived from the following formula:

16384 + (4 x number of voice ports in the c4224)

Custom queuing and other methods for identifying high-priority streams should be configured for these port ranges. For more information about custom queuing, refer to the “Managing System Performance” section in the *Configuration Fundamentals Configuration Guide* for Cisco IOS Release 12.0 T.

Configure Weighted Fair Queuing

Weighted fair queuing ensures that queues do not starve for bandwidth and that traffic gets predictable service. Low-volume traffic streams receive preferential service, while high-volume traffic streams share the remaining capacity, obtaining equal or proportional bandwidth.

In general, weighted fair queuing is used in conjunction with multilink PPP with interleaving and RSVP or IP precedence to ensure voice packet delivery. Use weighted fair queuing with multilink PPP to define how data is managed; use RSVP or IP precedence to give priority to voice packets. For more information about weighted fair queuing, refer to the “Managing System Performance” section in the *Configuration Fundamentals Configuration Guide* for Cisco IOS Release 12.0 T.

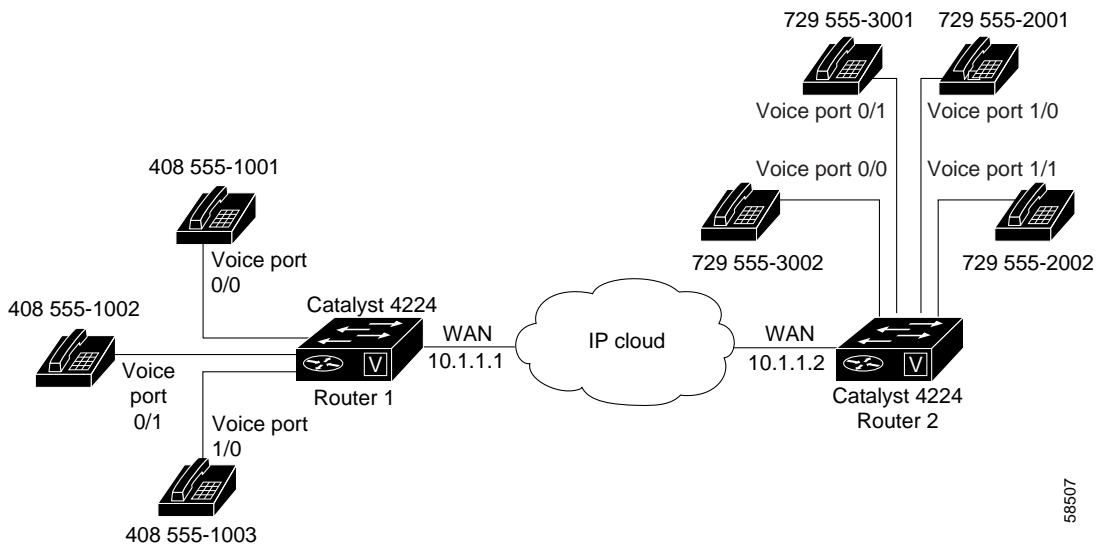
Configure Number Expansion

In most corporate environments, the telephone network is configured so that you can reach a destination by dialing only a portion (an extension number) of the full E.164 telephone number. You can configure VoIP to recognize extension numbers and expand them into their full E.164 dialed number by using two commands in tandem: **destination-pattern** and **num-exp**. Before you configure these two commands, it helps to map individual telephone extensions with their full E.164 dialed numbers. You can do this by creating a number expansion table.

Create a Number Expansion Table

The example depicted in [Figure 6-2](#) pertains to a small company that decides to use VoIP to integrate its telephony network with its existing IP network. The destination pattern (or expanded telephone number) associated with Catalyst 4224 1 (left of the IP cloud) is 408-555-xxxx, where xxxx identifies the individual dial peers by extension. The destination pattern (or expanded telephone number) associated with Catalyst 4224 2 (right of the IP cloud) is 729-555-xxxx.

Figure 6-2 Sample VoIP Network



58507

[Table 6-1](#) shows the number expansion table for this scenario.

Table 6-1 Sample Number Expansion Table

Extension	Destination Pattern	Num-Exp Command Entry	Description
1...	14085551...	num-exp 1... 14085551...	Expands a four-digit extension beginning with the numeral 1 by prefixing 1408555 to the extension.
2...	17295552...	num-exp 2... 17295552...	Expands a four-digit extension beginning with the numeral 2 by prefixing 1408555 to the extension.
3...	17295553...	num-exp 3... 17295553...	Expands a four-digit extension beginning with the numeral 3 by prefixing 1408555 to the extension.

**Note**

You can use a period (.) to represent variables, such as extension numbers, in a telephone number. A period is similar to a wildcard, which matches any entered digit.

The information included in this example needs to be configured on both Catalyst 4224 1 and Catalyst 4224 2. In this configuration, Catalyst 4224 1 can call any number string that begins with the digits *17295552* or *17295553* to connect to Catalyst 4224 2. Catalyst 4224 2 can call any number string that begins with the digits *14085551* to connect to Catalyst 4224 1.

Configure Number Expansion

To define how to expand an extension number into a particular destination pattern, use the following global configuration command:

num-exp *extension-number extension-string*

extension-number represents the digit(s) defining an extension number to be expanded, whereas *extension-string* represents the digit(s) defining an extension string to be expanded.

Use the **show num-exp** command to verify that you have mapped the telephone numbers correctly.

After you have configured dial peers and assigned destination patterns to them, use the **show dialplan number** command to see how a telephone number maps to a dial peer.

Configure Dial Peers

The key to understanding how VoIP functions is to understand dial peers. All of the voice technologies use dial peers to define the characteristics associated with a call leg. Dial peers are used to apply specific attributes to call legs and to identify call origin and destination.

As shown in [Figure 6-3](#) and [Figure 6-4](#), a *call leg* is a discrete segment of a call connection that lies between two points in the connection. Each call leg corresponds to a dial peer. An end-to-end call consists of four call legs, two from the perspective of the source Catalyst 4224 ([Figure 6-3](#)) and two from the perspective of the destination Catalyst 4224 ([Figure 6-4](#)). Attributes applied to a call leg include QoS, Coder-Decoder (codec), voice activity detection (VAD), and fax rate.

Figure 6-3 *Dial Peer Call Legs, from the Perspective of the Source Catalyst 4224*

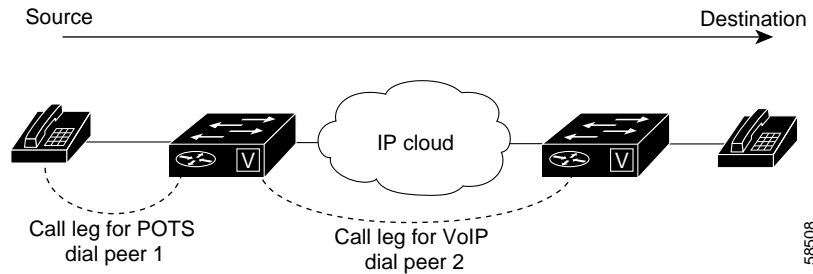
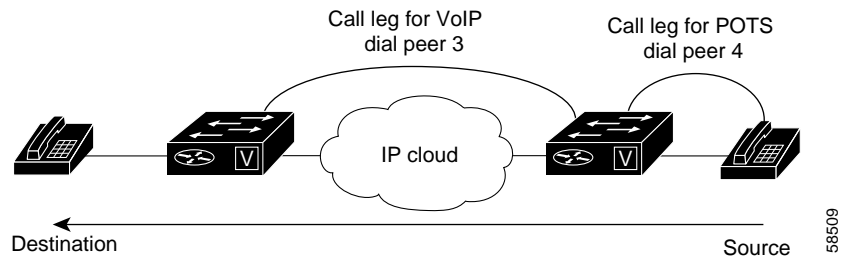


Figure 6-4 *Dial Peer Call Legs, from the Perspective of the Destination Catalyst 4224*



There are two types of dial peers with each voice implementation:

- POTS (plain old telephone service, or basic telephone service)—The dial peer associates a physical voice port with a local telephone device. The key commands you need to configure are the **destination-pattern** and **port** commands. The **destination-pattern** command defines the telephone number associated with the POTS dial peer. The **port** command associates the POTS dial peer with a specific logical dial interface, normally the voice port connecting your router to the local POTS network.
- VoIP—The dial peer associates a telephone number with an IP address. The key commands you need to configure are the **destination-pattern** and **session target** commands. The **destination-pattern** command defines the telephone number associated with the VoIP dial peer. The **session target** command

specifies a destination IP address for the VoIP dial peer. In addition, you can use VoIP dial peers to define characteristics such as IP precedence, additional QoS parameters (when RSVP is configured), codec, and VAD.

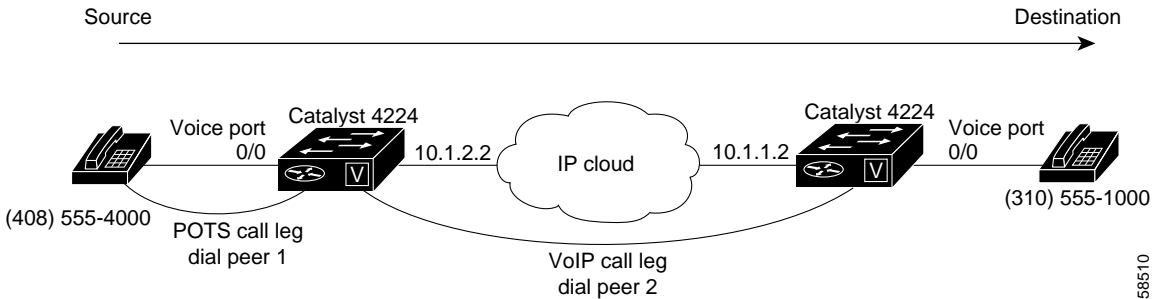
Inbound Versus Outbound Dial Peers

Dial peers are used for both inbound and outbound call legs. The terms *inbound* and *outbound* are defined from the *router* perspective. An inbound call leg means that an incoming call comes *to* the router. An outbound call leg means that an outgoing call is placed *from* the router.

For inbound call legs, a dial peer might be associated with the calling number or the voice-port number. Outbound call legs always have an associated dial peer. The destination pattern is used to identify the outbound dial peer. The call is associated with the outbound dial peer at setup time.

A POTS dial peer associates a telephone number with a particular voice port so that incoming calls for that telephone number can be received and outgoing calls can be placed. VoIP dial peers point to specific devices (by associating destination telephone numbers with a specific IP address) so that incoming calls can be received and outgoing calls can be placed. To establish VoIP connections, you need both POTS and VoIP dial peers.

Establishing communication using VoIP is similar to configuring an IP static route; you are establishing a specific voice connection between two defined endpoints. As shown in [Figure 6-5](#), the POTS dial peer establishes the source (via the originating telephone number or voice port) of the call. The VoIP dial peer establishes the destination by associating the destination telephone number with a specific IP address.

Figure 6-5 Outgoing Calls, from the Perspective of POTS Dial Peer 1

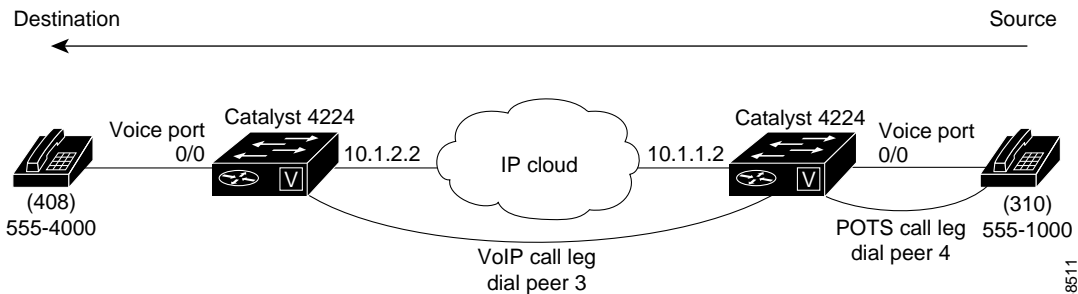
58510

To configure call connectivity between the source and the destination as illustrated in [Figure 6-5](#), enter the following commands on Catalyst 4224 10.1.2.2:

```
c4224(config)# dial-peer voice 1 pots
c4224(config-dial-peer)# destination-pattern 14085554000
c4224(config-dial-peer)# port 0/0

c4224(config)# dial-peer voice 2 voip
c4224(config-dial-peer)# destination-pattern 13105551000
c4224(config-dial-peer)# session target ipv4:10.1.1.2
```

[Figure 6-6](#) shows how to complete the end-to-end call between dial peer 1 and dial peer 4.

Figure 6-6 Outgoing Calls, from the Perspective of POTS Dial Peer 2

58511

To complete the end-to-end call between dial peer 1 and dial peer 4, as illustrated in [Figure 6-6](#), enter the following commands on Catalyst 4224 10.1.1.2:

```
c4224(config)# dial-peer voice 4 pots
c4224(config-dial-peer)# destination-pattern 13105551000
c4224(config-dial-peer)# port 0/0

c4224(config)# dial-peer voice 3 voip
c4224(config-dial-peer)# destination-pattern 14085554000
c4224(config-dial-peer)# session target ipv4:10.1.2.2
```

Create a Dial-Peer Configuration Table

Each dial peer needs to be identified by its unique data before you can configure dial peers in VoIP. Do this is by creating a dial peer configuration table.

Using the example in [Figure 6-2 on page 6-13](#), Router 1, with an IP address of 10.1.1.1, connects a small sales branch office to the main office through Router 2. There are three telephones in the sales branch office that need to be established as dial peers. Router 2, with an IP address of 10.1.1.2, is the primary gateway to the main office. There are four devices that need to be established as dial peers in the main office, and all are basic telephones connected to the PBX. [Figure 6-2 on page 6-13](#) shows a diagram of this small voice network, and [Table 6-2](#) shows the dial peer configuration table for the example in the figure.

Table 6-2 Dial Peer Example Configuration Table

Router	Dial Peer Tag	Commands				
		Destination-Pattern	Type	Session Target	codec	QoS
Cisco 1750 Router 1	10	1729555....	VoIP	IPV4 10.1.1.2	G.729	Best effort
Cisco 1750 Router 2	11	1408555....	VoIP	IPV4 10.1.1.1	G.729	Best effort

Configure POTS Dial Peers

POTS dial peers enable incoming calls to be received by a particular telephony device. To configure a POTS dial peer, you need to uniquely identify the dial peer (by assigning it a unique tag number), define its telephone number(s), and associate it with a voice port through which calls are established. Under most circumstances, the default values for the remaining dial peer configuration commands are sufficient to establish connections.

To enter the dial peer configuration mode (and select POTS as the method of voice-related encapsulation), use the **dial-peer voice number pots** global configuration command. The *number* value is a tag that uniquely identifies the dial peer. (This number has local significance only.)

To configure the identified POTS dial peer, use the **destination-pattern string** dial peer configuration command. The *string* value is the destination telephone number associated with this POTS dial peer.

Outbound Dialing on POTS Dial Peers

When a router receives a voice call, the router selects an outbound dial peer by comparing the called number with the number configured as the destination pattern for the POTS dial peer. The router then removes the left-justified numbers corresponding to the destination pattern that matches the called number. If you have configured a prefix, the prefix is put in front of the remaining numbers, creating a dial string, which the router then dials. If all numbers in the destination pattern are removed, the user receives a dial tone.

For example, suppose there is a voice call with the E.164 called number of *1-310-767-2222*. If you configure a destination-pattern of *1310767* and a prefix of *9*, the router removes *1310767* from the E.164 telephone number, leaving the extension number of *2222*. It will then create a prefix *9* at the front of the remaining numbers, so that the actual numbers dialed are *9,2222*. The comma in this example means that the router will pause for one second between dialing the *9* and the *2* to allow for a secondary dial tone.

Configure VoIP Dial Peers

VoIP dial peers enable outgoing calls to be made from a particular telephony device. To configure a VoIP dial peer, you need to identify the dial peer (by assigning it a unique tag number), define its destination telephone number, and define its destination IP address. The default values for the remaining dial peer configuration commands are usually adequate to establish connections.

To enter the dial peer configuration mode (and select VoIP as the method of voice-related encapsulation), use the **dial-peer voice *number* voip** global configuration command. The *number* value of the **dial-peer voice voip** command is a tag that uniquely identifies the dial peer.

To configure the identified VoIP dial peer, use the following dial peer configuration commands:

	Task	Command
Step 1	Define the destination telephone number associated with this VoIP dial peer.	destination-pattern <i>string</i>
Step 2	Specify a destination IP address for this dial peer.	session target { ipv4: <i>destination-address</i> dns: <i>host-name</i> }

For examples of how to configure dial peers, see [Appendix C, “VoIP Configuration Examples.”](#)

Verifying Your Configuration

You can check the validity of your dial peer configuration by performing the following tasks:

- If you have relatively few dial peers configured, you can use the **show dial-peer voice** command to verify that the data configured is correct. Use this command to display a specific dial peer or to display all configured dial peers.
- Use the **show dialplan number** command to show which dial peer is reached when a particular number is dialed.

Troubleshooting Tips

If you are having trouble connecting a call and you suspect the problem is associated with the dial-peer configuration, you can try to resolve the problem by performing the following tasks:

- Ping the associated IP address to confirm connectivity. If you cannot successfully ping your destination, refer to the “Configuring IP” section in the *Network Protocols Configuration Guide*, Part 1 for Cisco IOS Release 12.0 T.
- If you have configured number expansion, use the **show num-exp** command to check that the partial number on the local router maps to the correct full E.164 telephone number on the remote router.
- If you have configured a codec value, there can be a problem if the VoIP dial peers on either side of the connection have incompatible codec values. Make sure that both VoIP peers have been configured with the same codec value.
- Use the **debug vpm spi** command to verify that the router dials the correct output string.
- Use the **debug cch323 rtp** command to check RTP packet transport.
- Use the **debug cch323 h225** command to check the call setup.

Configure Voice Ports

Routers provide only analog voice ports for its implementation of VoIP. The type of signaling associated with analog voice ports depends on the voice interface card (VIC) installed in the device.

Each VIC is specific to a particular signaling type; therefore, VICs determine the type of signaling for the voice ports. Voice-port commands define the characteristics associated with a particular voice-port signaling type.

The voice ports support three basic voice signaling types:

- **FXS**—The foreign exchange station interface uses a standard RJ-11 modular telephone cable to connect directly to a standard telephone, fax machine, PBX or similar device. FXS supplies ring, voltage, and dial tone to the station.

- FXO—The foreign exchange office interface uses a RJ-11 modular telephone cable to connect local calls to a PSTN central office or to a PBX that does not support E&M signaling. This interface is used for off-premise extension applications.
- E&M—The E&M interface uses an RJ-48 telephone cable to connect remote calls from an IP network to PBX trunk lines (tie lines) for local distribution. It is a signaling technique for two-wire and four-wire telephone and trunk interfaces.

Configure FXS or FXO Voice Ports

Under most circumstances, the default voice port values are adequate to configure FXS and FXO ports to transport voice data over your existing IP network. However, if you need to change the default configuration for these voice ports, use the commands outlined in [Table 6-3](#), beginning in privileged EXEC mode:

Table 6-3 Commands to Configure FXS and FXO Voice Ports

	Task	Required or Optional	Command
Step 1	Enter the global configuration mode.	Required	<code>configure terminal</code>
Step 2	Identify the voice port you want to configure, and enter the voice port configuration mode.	Required	<code>voice-port slot-number/port</code>
Step 3	(For FXO ports only) Select the appropriate dial type for out-dialing.	Required	<code>dial-type {dtmf pulse}</code>
Step 4	Select the appropriate signal type for this interface.	Required	<code>signal {loop-start ground-start}</code>
Step 5	Select the appropriate voice call progress tone for this interface. The default for this command is us .	Required	<code>cptone country</code>
Step 6	(For FXS ports only) Select the ring frequency (in Hz) specific to the equipment attached to this voice port and appropriate to the country you are in.	Required	<code>ring frequency {25 50}</code>

Table 6-3 Commands to Configure FXS and FXO Voice Ports (continued)

	Task	Required or Optional	Command
Step 7	(For FXO ports only) Specify the maximum number of rings before answering a call.	Required	<code>ring number number</code>
Step 8	Specify the private line auto ringdown (PLAR) connection if this voice port is used for a PLAR connection. The <i>string</i> value specifies the destination telephone number.	Optional	<code>connection plar string</code>
Step 9	Specify the threshold (in dB) for on-hold music. Valid entries are from -70 to -30 db.	Optional	<code>music-threshold number</code>
Step 10	Attach descriptive text about this voice port connection.	Optional	<code>description string</code>
Step 11	If voice activity detection (VAD) is activated, specify that background noise is generated.	Optional	<code>comfort-noise</code>

Verifying Your Configuration

You can check the validity of your voice port configuration by performing the following tasks:

- Pick up the handset of an attached telephony device and listen for a dial tone.
- Check for dual tone multifrequency (DTMF) detection. If the dial tone stops when you dial a digit, the voice port is configured properly.
- Use the **show voice-port** command to verify that the configured data is correct.

Troubleshooting Tips

If you are having trouble connecting a call and you suspect the problem is associated with the voice port configuration, you can try to resolve the problem by performing the following tasks:

- Ping the associated IP address to confirm connectivity. If you cannot ping the destination, refer to the *Network Protocols Configuration Guide, Part 1* for Cisco IOS Release 12.0T.
- Use the **show voice-port** command to make sure that the port is enabled. If the port is offline, use the **no shutdown** command.
- Make sure the VICs are correctly installed. For more information about installing a VIC in your router, refer to the *Cisco WAN Interface Cards Hardware Installation Guide*.

Fine-Tune FXS and FXO Voice Ports

In most cases, the default values for voice-port tuning commands are sufficient. Depending on the specifics of your particular network, you might need to adjust voice parameters involving timing, input gain, and output attenuation for FXS or FXO voice ports. Collectively, these commands are referred to as voice-port tuning commands.

If you need to change the default tuning configuration for FXS and FXO voice ports, use the commands outlined in [Table 6-4](#), beginning in privileged EXEC mode:

Table 6-4 *Commands to Fine Tune FXS and FXO Voice Ports*

	Task	Command	Valid Entries	Default Value
Step 1	Enter the global configuration mode.	<code>configure terminal</code>		
Step 2	Identify the voice port you want to configure, and enter the voice port configuration mode.	<code>voice-port</code> <code>slot-number/port</code>		

Table 6-4 Commands to Fine Tune FXS and FXO Voice Ports (continued)

	Task	Command	Valid Entries	Default Value
Step 3	Specify (in dB) the amount of gain to be inserted at the receiver side of the interface.	<code>input gain value</code>	-6 to 14 dB	0 dB
Step 4	Specify (in dB) the amount of attenuation at the transmit side of the interface.	<code>output attenuation value</code>	0 to 14 dB	0 dB
Step 5	Enable echo-cancellation of voice that is sent out of the interface and received back on the same interface.	<code>echo-cancel enable</code>		
Step 6	Adjust the size (in milliseconds) of the echo-cancel.	<code>echo-cancel coverage value</code>	8, 16, 24, and 32 ms	16 ms
Step 7	Enable nonlinear processing, which shuts off any signal if no near-end speech is detected. (Nonlinear processing is used with echo-cancellation.)	<code>non-linear</code>		
Step 8	Specify the number of seconds the system will wait for the caller to input the first digit of the dialed digits.	<code>timeouts initial seconds</code>	0 to 120 sec	10 sec
Step 9	Specify the number of seconds the system will wait (after the caller has input the initial digit) for the caller to input a subsequent digit.	<code>timeouts interdigit seconds</code>	0 to 120 sec	10 sec
Step 10	If the voice-port dial type is DTMF, configure the DTMF digit signal duration.	<code>timing digit milliseconds</code>	50 to 100 ms	100 ms
Step 11	If the voice-port dial type is DTMF, configure the DTMF inter-digit signal duration.	<code>timing inter-digit milliseconds</code>	50 to 500 ms	100 ms

Table 6-4 Commands to Fine Tune FXS and FXO Voice Ports (continued)

	Task	Command	Valid Entries	Default Value
Step 12	(FXO ports only) If the voice-port dial type is pulse, configure the pulse digit signal duration.	<code>timing pulse-digit milliseconds</code>	10 to 20 ms	20 ms
Step 13	(FXO ports only) If the voice-port dial type is pulse, configure the pulse inter-digit signal duration.	<code>timing pulse-inter-digit milliseconds</code>	100 to 1000 ms	500 ms

**Note**

After you change any voice port setting, Cisco recommends that you cycle the port by using the **shutdown** and **no shutdown** commands.

Configure E&M Voice Ports

Unlike FXS and FXO voice ports, the default E&M voice-port parameters are not sufficient to enable voice and data transmission over your IP network. Because of the inherent complexities of PBX networks, E&M voice port values must match those specified by the particular PBX device to which it is connected.

To configure E&M voice ports, use the commands outlined in [Table 6-5](#), beginning in privileged EXEC mode:

Table 6-5 Commands to Configure E&M Voice Ports

	Task	Required or Optional	Command
Step 1	Enter the global configuration mode.	Required	<code>configure terminal</code>
Step 2	Identify the voice port you want to configure, and enter the voice port configuration mode.	Required	<code>voice-port slot-number/port</code>
Step 3	Select the appropriate dial type for out-dialing.	Required	<code>dial-type {dtmf pulse}</code>

Table 6-5 Commands to Configure E&M Voice Ports (continued)

	Task	Required or Optional	Command
Step 4	Select the appropriate signal type for this interface.	Required	<code>signal {wink-start immediate delay-dial}</code>
Step 5	Select the appropriate voice call progress tone for this interface.	Required	<code>cptone {australia brazil china finland france germany japan northamerica unitedkingdom}</code>
Step 6	Select the appropriate cabling scheme for this voice port.	Required	<code>operation {2-wire 4-wire}</code>
Step 7	Select the appropriate E&M interface type. <ul style="list-style-type: none"> Type 1 is for the following lead configuration: <ul style="list-style-type: none"> E—Output, relay to ground M—Input, referenced to ground Type 2 is for the following lead configuration: <ul style="list-style-type: none"> E—Output, relay to SG M—Input, referenced to ground SB—Feed for M, connected to –48V SG—Return for E, galvanically isolated from ground Type 3 is for the following lead configuration: <ul style="list-style-type: none"> E—Output, relay to ground M—Input, referenced to ground SB—Connected to –48V SG—Connected to ground Type 5 is for the following lead configuration: <ul style="list-style-type: none"> E—Output, relay to ground M—Input, referenced to –48V 	Required	<code>type {1 2 3 5}</code>

Table 6-5 Commands to Configure E&M Voice Ports (continued)

	Task	Required or Optional	Command
Step 8	Specify a terminating impedance for an E&M voice port. The impedance value selected must match the specifications from the telephony system to which this voice port is connected.	Required	<code>impedance { 600c 600r 900c complex1 complex2 }</code>
Step 9	Specify the private line auto ringdown (PLAR) connection if this voice port is used for a PLAR connection. The <i>string</i> value specifies the destination telephone number.	Optional	<code>connection plar string</code>
Step 10	Specify the threshold (in dB) for on-hold music. Valid entries are from -70 to -30 dB. The default is -38 dB.	Optional	<code>music-threshold number</code>
Step 11	Attach descriptive text about this voice port connection.	Optional	<code>description string</code>
Step 12	Specify that background noise is generated.	Optional	<code>comfort-noise</code>

Verifying Your Configuration

You can check the validity of your voice port configuration by performing the following tasks:

- Pick up the handset of an attached telephony device and listen for a dial tone.
- Check for DTMF detection. If the dial tone stops when you dial a digit, the voice port is configured properly.
- Use the **show voice-port** command to verify that the data configured is correct.

Troubleshooting Tips

If you are having trouble connecting a call and you suspect the problem is associated with the voice port configuration, you can try to resolve the problem by performing the following tasks:

- Ping the associated IP address to confirm connectivity. If you cannot ping the destination, refer to the *Network Protocols Configuration Guide, Part 1* for Cisco IOS Release 12.0 T.
- Use the **show voice-port command** to make sure that the port is enabled. If the port is offline, use the **no shutdown** command.
- If you have configured E&M interfaces, make sure that the values pertaining to your specific PBX setup, such as timing and type, are correct.
- Make sure the VICs are correctly installed. For more information, refer to the *Cisco WAN Interface Cards Hardware Installation Guide*.

Fine-Tune E&M Voice Ports

In most cases, the default values for voice port tuning commands are sufficient. Depending on the specifics of your particular network, you might need to adjust voice parameters involving timing, input gain, and output attenuation for E&M voice ports. Collectively, these commands are referred to as voice port tuning commands.

If you need to change the default tuning configuration for E&M voice ports, use the commands shown in [Table 6-6](#), beginning in privileged EXEC mode:

Table 6-6 Commands to Fine Tune E&M Voice Ports

	Task	Command	Valid Entries	Default Values
Step 1	Enter the global configuration mode.	<code>configure terminal</code>		
Step 2	Identify the voice port you want to configure, and enter the voice port configuration mode.	<code>voice-port slot-number/port</code>		

Table 6-6 Commands to Fine Tune E&M Voice Ports (continued)

	Task	Command	Valid Entries	Default Values
Step 3	Specify (in dB) the amount of gain to be inserted at the receiver side of the interface.	<code>input gain value</code>	-6 to 14 dB	0 dB
Step 4	Specify (in dB) the amount of attenuation at the transmit side of the interface.	<code>output attenuation value</code>	0 to 14 dB	0 dB
Step 5	Enable echo-cancellation of voice that is sent out of the interface and received back on the same interface.	<code>echo-cancel enable</code>		
Step 6	Adjust the size (in milliseconds) of the echo-cancel.	<code>echo-cancel coverage value</code>	8, 16, 24, and 32 ms	16 ms
Step 7	Enable nonlinear processing, which shuts off any signal if no near-end speech is detected. (Nonlinear processing is used with echo-cancellation.)	<code>non-linear</code>		
Step 8	Specify the number of seconds the system will wait for the caller to input the first digit of the dialed digits.	<code>timeouts initial seconds</code>	0 to 120 sec	10 sec

Table 6-6 Commands to Fine Tune E&M Voice Ports (continued)

	Task	Command	Valid Entries	Default Values
Step 9	Specify the number of seconds the system will wait (after the caller has input the initial digit) for the caller to input a subsequent digit.	<code>timeouts interdigit seconds</code>	0 to 120 sec	10 sec
Step 10	Specify the indicated timing parameters.	<code>timing clear-wait milliseconds</code> <code>timing delay-duration milliseconds</code> <code>timing delay-start milliseconds</code> <code>timing dial-pulse min-delay milliseconds</code> <code>timing digit milliseconds</code> <code>timing inter-digit milliseconds</code> <code>timing pulse pulses-per-second</code> <code>timing pulse-inter-digit milliseconds</code> <code>timing wink-duration milliseconds</code> <code>timing wink-wait milliseconds</code>	200 to 2000 ms 100 to 5000 ms 20 to 2000 ms 0 to 5000 ms 50 to 100 ms 50 to 500 ms 10 to 20 pps 100 to 1000 ms 100 to 400 ms 100 to 5000 ms	

**Note**

After you change any voice port setting, Cisco recommends that you cycle the port by using the **shutdown** and **no shutdown** commands.

Additional VoIP Dial-Peer Configurations

Depending on how you have configured your network interfaces, you might need to configure additional VoIP dial-peer parameters. This section describes the following topics:

- [Configure IP Precedence for Dial Peers, page 6-32](#)
- [Configure RSVP for Dial Peers, page 6-33](#)
- [Configure codec and VAD for Dial Peers, page 6-34](#)

Configure IP Precedence for Dial Peers

Use the **ip precedence** command to give voice packets a higher priority than other IP data traffic. The **ip precedence** command should also be used if RSVP is not enabled and you would like to give voice packets a priority over other IP data traffic. IP precedence scales better than RSVP but provides no admission control.

To give real-time voice traffic precedence over other IP network traffic, use the following global configuration commands:

Table 6-7 Global Configuration Commands for Dial Peers

	Task	Command
Step 1	Enter dial peer configuration mode to configure a VoIP dial peer. The <i>number</i> argument is one or more digits identifying the dial peer. Valid entries are from 1 to 2147483647.	<code>dial-peer voice <i>number</i> voip</code>
Step 2	Select a precedence level for the voice traffic associated with that dial peer. The <i>number</i> argument specifies the IP Precedence value. Valid entries are from 0 to 7. A value of 0 means that no precedence (priority) has been set.	<code>ip precedence <i>number</i></code>

In IP precedence, the numbers 1 through 5 identify classes for IP flows, while the numbers 6 and 7 are used for network and backbone routing and updates.

For example, to ensure that voice traffic associated with VoIP dial peer 103 is given a higher priority than other IP network traffic, enter the following:

```
c4224(config)# dial-peer voice 103 voip
c4224(config-dial-peer)# ip precedence 5
```

In this example, when an IP call leg is associated with VoIP dial peer 103, all packets transmitted to the IP network via this dial peer will have their precedence bits set to 5. If the networks receiving these packets have been configured to recognize precedence bits, the packets are given priority over packets with a lower configured precedence value.

Configure RSVP for Dial Peers

RSVP must be enabled at each LAN or WAN interface across which voice packets will travel. After enabling RSVP, you must use the **req-qos** dial-peer configuration command to request an RSVP session and configure the QoS for each VoIP dial peer. Otherwise, no bandwidth is reserved for voice traffic.

For example, to configure controlled-load QoS for VoIP dial peer 108, enter the following global configuration commands:

```
c4224(config)# Dial-peer voice 108 voip
c4224(config-dial-peer)# req-qos controlled-load
c4224(config-dial-peer)# session target ipv4:10.0.0.8
```

In this example, every time a connection is made through VoIP dial peer 108, an RSVP reservation request is made between the local router, all intermediate routers in the path, and the final destination router.



Note

Cisco recommends that you select **controlled-load** for the requested QoS. The controlled-load service uses admission (or capacity) control to ensure that preferential service is provided even when the bandwidth is overloaded.

To generate Simple Network Management Protocol (SNMP), use the following commands beginning in global configuration mode:

Table 6-8 Configuration Commands to Generate SNMP

	Task	Command
Step 1	Enter the dial peer configuration mode to configure a VoIP dial peer.	<code>dial-peer voice number voip</code>
Step 2	Generate an SNMP event if the QoS for a dial peer drops below a specified level.	<code>acc-qos [best-effort controlled-load guaranteed-delay]</code>



Note

RSVP reservations are only one-way. If you configure RSVP, the VoIP dial peers on either side of the connection must be configured for RSVP.

Configure codec and VAD for Dial Peers

Coder-decoder (codec) typically is used to transform analog signals into a digital bit stream and digital signals back into analog signals. The codec specifies the voice coder rate of speech for a dial peer. Voice activity detection (VAD) is used to disable the transmission of silence packets. codec and VAD values for a dial peer determine how much bandwidth the voice session uses.

Configure codec for a VoIP Dial Peer

To specify a voice coder rate for a selected VoIP dial peer, use the following commands, beginning in global configuration mode:

Table 6-9 Configuration Commands to Specify a Voice Coder Rate

	Task	Command
Step 1	Enter the dial peer configuration mode to configure a VoIP dial peer.	<code>dial-peer voice number voip</code>
Step 2	Specify the desired voice coder rate of speech.	<code>codec [g711alaw g711ulaw g729r8 g729r8 pre-ietf]</code>

The default for the **codec** command is **g729r8**, which is normally the most desirable setting. However, if you are operating on a high-bandwidth network and voice quality is of the highest importance, you should configure the **codec** command for **g711alaw** or **ulaw**. Using **g711alaw** results in better voice quality, but it also requires higher bandwidth usage for voice.

For example, to specify a codec rate of **g711alaw** for VoIP dial peer 108, enter the following:

```
c4224(config)# dial-peer voice 108 voip
c4224(config-dial-peer)# codec g711alaw
```



Note

Prior to Cisco IOS Release 12.0(5)T, **g729r8** is implemented in the pre-IETF format; thereafter, it is implemented in the standard IETF format. When new images, such as Release 12.0(5)T or later, interoperate with older versions of VoIP (when the **g729r8** codec was not compliant with the IETF standard), users can hear garbled voices and ringback on either side of the connection. To avoid this problem, configure the dial peers with the **g729r8 pre-ietf** argument.

Configure VAD for a VoIP Dial Peer

To disable the transmission of silence packets and enable VAD for a selected VoIP dial peer, use the following global configuration commands:

Table 6-10 Commands to Disable the Transmission of Silence Packets

	Task	Command
Step 1	Enter dial peer configuration mode to configure a VoIP dial peer.	<code>dial-peer voice number voip</code>
Step 2	Disable the transmission of silence packets.	<code>vad</code>

The **vad** command is enabled by default, which is normally the most desirable setting. If you are operating on a high-bandwidth network and voice quality is of the highest importance, you should disable VAD. Disabling VAD results in better voice quality, but it also requires higher bandwidth usage for voice.

For example, to enable VAD for VoIP dial peer 108, enter the following:

```
c4224(config)# Dial-peer voice 108 voip
c4224(config-dial-peer)# vad
```

Configure Frame Relay for VoIP

When you are configuring VoIP, you need to take certain factors into consideration so that it runs smoothly over Frame Relay. A public Frame Relay cloud provides no QoS guarantee. For real-time traffic to be transmitted in a timely manner, the data rate must not exceed the committed information rate (CIR), or packets might be dropped. In addition, Frame Relay traffic shaping and RSVP are mutually exclusive. This is particularly important to remember if multiple data-link connection identifiers (DLCIs) are carried on a single interface.

For Frame Relay links with slow output rates (less than or equal to 64 kbps), where data and voice are transmitted over the same permanent virtual circuit (PVC), Cisco recommends the following solutions:

- Separate DLCIs for voice and data—By providing a separate subinterface for voice and data, you can use the appropriate QoS tool per line. For example, each DLCI would use 32 kbps of a 64-kbps line.
- Apply adaptive traffic shaping to both DLCIs.
- Use RSVP or IP precedence to prioritize voice traffic.
- Use compressed RTP to minimize voice packet size.
- Use weighted fair queuing to manage voice traffic.
- Lower the maximum transmission unit (MTU) size—Voice packets are generally small. When you lower the MTU size (for example, to 300 bytes), large data packets can be broken up into smaller data packets that can more easily be interwoven with voice packets.



Note Lowering the MTU size impacts data throughput speed.

- Set CIR equal to line rate—Ensure that the data rate does not exceed the CIR through generic traffic shaping.
 - Use RSVP or IP precedence to prioritize voice traffic.
 - Use compressed RTP to minimize voice packet header size.

- Shape the traffic—Use adaptive traffic shaping to slow the output rate based on the backward explicit congestion notification (BECN). If the feedback from the switch is ignored, packets (both data and voice) might be discarded. Because the Frame Relay switch does not distinguish between voice and data packets, voice packets could be discarded, which would result in a deterioration of voice quality.
 - Use RSVP, compressed RTP, reduced MTU size, and adaptive traffic shaping based on BECN to hold the data rate to CIR.
 - Use generic traffic shaping to obtain a low interpacket wait time. For example, set committed burst (Bc) to 4000 to obtain an interpacket wait time of 125 milliseconds.

In Cisco IOS Release 12.0 T, Frame Relay traffic shaping is not compatible with RSVP. Cisco suggests one of the following workarounds:

- Provision the Frame Relay permanent virtual circuits (PVC) to have the CIR equal to the port speed.
- Use generic traffic shaping with RSVP.

Frame Relay for VoIP Configuration Example

For Frame Relay, it is customary to configure a main interface and several subinterfaces with one subinterface per PVC. The following example configures a Frame Relay main interface and a subinterface so that voice and data traffic can be successfully transported:

```
interface Serial0
  mtu 300
  no ip address
  encapsulation frame-relay
  no ip route-cache
  no ip mroute-cache
  fair-queue 64 256 1000
  frame-relay ip rtp header-compression

interface Serial11 point-to-point
  mtu 300
  ip address 40.0.0.7 255.0.0.0
  ip rsvp bandwidth 48 48
  no ip route-cache
  no ip mroute-cache
  bandwidth 64
```

```
traffic-shape rate 32000 4000 4000
frame-relay interface-dlci 16
frame-relay ip rtp header-compression
```

In this configuration example, the main interface is configured as follows:

- MTU size is 300 bytes.
- No IP address is associated with this serial interface. The IP address must be assigned for the subinterface.
- Encapsulation method is Frame Relay.
- Fair-queuing is enabled.
- IP RTP header compression is enabled.

The subinterface is configured as follows:

- MTU size is inherited from the main interface.
- IP address for the subinterface is specified.
- RSVP is enabled to use the default value, which is 75 percent of the configured bandwidth.
- Bandwidth is set to 64 kbps.
- Generic traffic shaping is enabled with 32-kbps CIR where committed burst (Bc) = 4000 bits and excess burst (Be) = 4000 bits.
- Frame Relay DLCI number is specified.
- IP RTP header compression is enabled.

**Note**

When traffic bursts over the CIR, the output rate is held at the speed configured for the CIR. For example, traffic will not go beyond 32 kbps if CIR is set to 32 kbps.

For more information about configuring Frame Relay for VoIP, refer to the “Configuring Frame Relay” section in the *Wide-Area Networking Configuration Guide* for Cisco IOS Release 12.0 T.

