CHAPTER 2

VoIP Configuration

This chapter explains how to configure VoIP on your router and contains the following sections:

- Prerequisite Tasks
- Configuration Tasks
- Configure IP Networks for Real-Time Voice Traffic
- Configure Number Expansion
- Configure Dial Peers
- Configure Voice Ports
- Additional VoIP Dial Peer Configurations
- Configure Frame Relay for VoIP
- Configure Microsoft NetMeeting for VoIP

Prerequisite Tasks

Before you can configure your router 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" chapters in the Network Protocols Configuration Guide, Part 1 for Cisco IOS Release 12.0T.
- Install the voice interface cards (VICs) in your router. For more information about installing a VIC in your router, refer to the <Emphasis>Cisco WAN Interface Cards Hardware Installation Guide.
- Complete your company's dial plan.
- Establish a working telephony network based on your company's 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, we recommend the following:
  - Use canonical numbers wherever possible. Avoid situations where numbering systems are significantly different on different routers or access servers in your network.
  - Make routing and dialing transparent to the user—for example, avoid secondary dial tones from secondary switches, where possible.
  - Contact your PBX vendor for instructions about 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 router, you need to perform the following steps:

Step 1 Configure your IP network to support real-time voice traffic. Refer to the following section for information about selecting and configuring the appropriate QoS tool or tools to optimize voice traffic on your network.

Step 2 (Optional) If you plan to run VoIP 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. Refer to the "Configure Frame Relay for VoIP" section on page 2-24 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 a portion (an extension number) of the full E.164 telephone number. Refer to the "Configure Number Expansion" section on page 2-8 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. Refer to the "Configure Dial Peers" section on page 2-9 and the "Additional VoIP Dial Peer Configurations" section on page 2-21 for additional information about configuring dial peers and dial-peer characteristics.

Step 5 Configure your router to support voice ports. Refer to the "Configure Voice Ports" section on page 2-14 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 backbone, such as 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 take into consideration the entire scope of your network and then select the appropriate QoS tool or tools.

The important thing to remember is that QoS must be configured throughout your network—not just on your router running VoIP—to improve voice network performance. 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; 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
- Configure Multilink PPP with Interleaving
- Configure RTP Header Compression
- Configure Custom Queuing
- Configure Weighted Fair Queuing

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 for reliability and 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. It is up to the interface queuing mechanism (such as weighted fair queuing or WRED) to implement the reservation.

RSVP works well on PPP, HDLC, and similar serial line interfaces. It does not work well on multi-access 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 needs to be set.

By default, RSVP is disabled so that it is backwards compatible with systems that do not implement RSVP. To enable RSVP for IP on an interface, use the following interface configuration command:

`Router(config-if)#` **ip rsvp bandwidth** [*interface-kbps*] [*single-flow-kbps*]

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, it will still be refused because the physical interface lacks supporting bandwidth.

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

```
bps=packet_size+ip/udp/rtp header size * 50 per second
```

For G.729, 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" chapter of the *Network Protocols Configuration Guide, Part 1* for Cisco IOS Release 12.0T.

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):

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

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

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

Configure Multilink PPP with Interleaving

Multiclass multilink 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 2 Mbps

Note Do not use multilink PPP on links greater than 2 Mbps.

Multilink PPP support for interleaving can be configured on virtual templates, dialer interfaces, and ISDN BRI or PRI interfaces. To configure interleaving, you need to complete 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:

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

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" chapter in the *Dial Solutions Configuration Guide* for Cisco IOS Release 12.0T.

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:

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

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

Configure RTP Header Compression

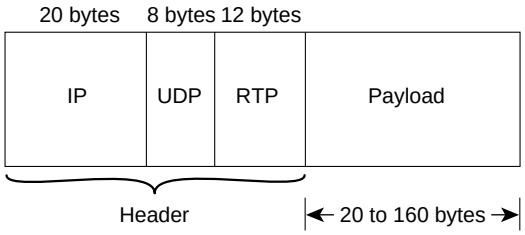
Real-Time Transport Protocol (RTP) is used for carrying audio traffic in packets over an IP network. RTP header compression compresses the IP/UDP/RTP header in an RTP data packet from 40 bytes to approximately 2 to 4 bytes (most of the time), as shown in Figure 2-1.

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.

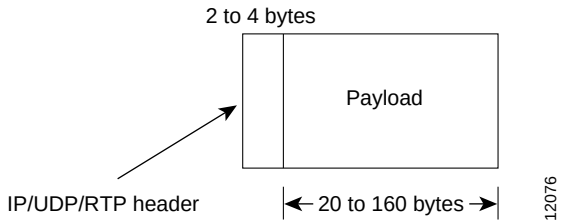
Typically, an RTP packet has a payload of approximately 20 to 160 bytes for audio applications that use compressed payloads. RTP header compression is especially beneficial when the RTP payload size is small (for example, compressed audio payloads between 20 and 50 bytes).

Figure 2-1 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 2 Mbps
- Need to save bandwidth

Note Do not use RTP header compression on links greater than 2 Mbps.

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

- Enable RTP Header Compression on a Serial Interface
- Change the Number of Header Compression Connections

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:

```
Router(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:

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

RTP Header Compression Configuration Example

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

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

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

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 number is derived from the following formula:

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

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” chapter in the *Configuration Fundamentals Configuration Guide* for Cisco IOS Release 12.0T.

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; 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” chapter in the *Configuration Fundamentals Configuration Guide* for Cisco IOS Release 12.0T.

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. VoIP can be configured 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. This can be done easily by creating a number expansion table.

Create a Number Expansion Table

In Figure 2-2, a small company decides to use VoIP to integrate its telephony network with its existing IP network. The destination pattern (or expanded telephone number) associated with Cisco 1750 Router 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 Cisco 1750 Router 2 (right of the IP cloud) is (729) 555-xxxx.

Figure 2-2 Sample VoIP Network

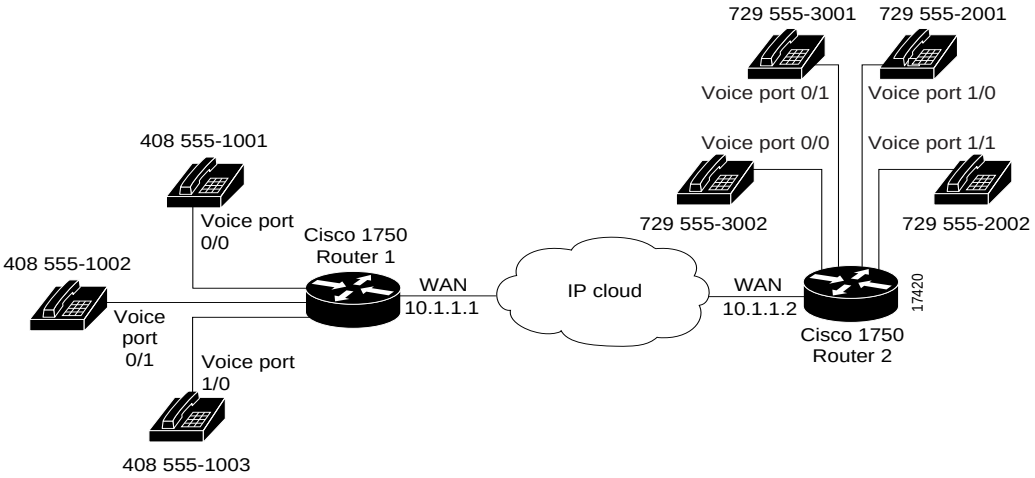


Table 2-1 shows the number expansion table for this scenario.

Table 2-1 Sample Number Expansion Table

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

Table 2-1 Sample Number Expansion Table

Extension	Destination Pattern	Num-Exp Command Entry	Description
3...	17295553...	num-exp 3... 17295553...	To expand a four-digit extension beginning with the numeral 3 by prefixing 1408555 to it

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 Cisco 1750 Router 1 and Cisco 1750 Router 2. In this configuration, Cisco 1750 Router 1 can call any number string that begins with the digits *17295552* or *17295553* to connect to Cisco 1750 Router 2. Similarly, Cisco 1750 Router 2 can call any number string that begins with the digits *14085551* to connect to Cisco 1750 Router 1.

Configure Number Expansion

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

```
Router(config)# num-exp extension-number extension-string
```

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. A call leg is a discrete segment of a call connection that lies between two points in the connection, as shown in Figure 2-3 and Figure 2-4. For instance, between a telephone and a router, a router and a network, a router and a PBX, or a router and the PSTN. Each call leg corresponds to a dial peer. An end-to-end call is comprised of four call legs, two from the perspective of the source router as shown in Figure 2-3, and two from the perspective of the destination router as shown in Figure 2-4. Dial peers are used to apply specific attributes to call legs and to identify call origin and destination. Attributes applied to a call leg include QoS, CODEC, voice activity detection (VAD), and fax rate.

Figure 2-3 Dial Peer Call Legs from the Perspective of the Source Router

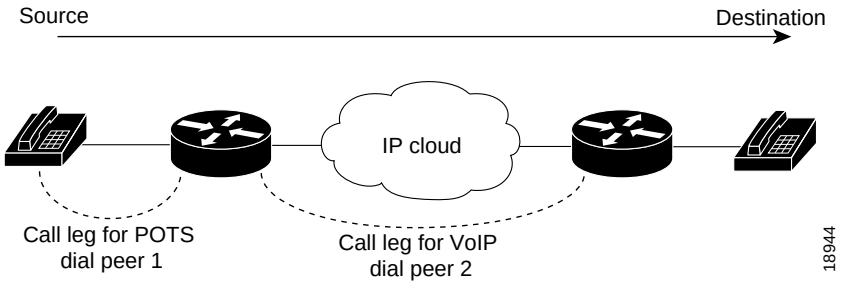
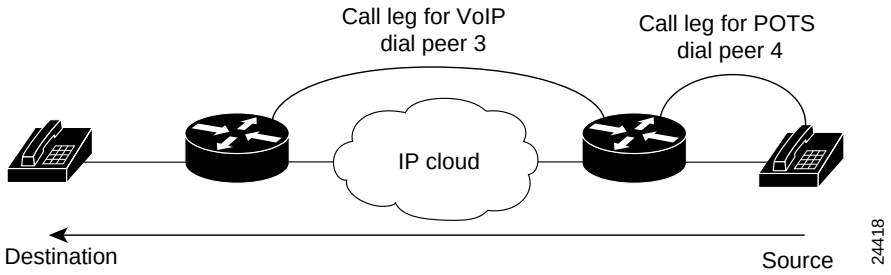


Figure 2-4 Dial Peer Call Legs from the Perspective of the Destination Router



There are basically two different kinds of dial peers with each voice implementation:

- POTS—(also known as “plain old telephone service” or “basic telephone service”) dial peer associates a physical voice port with a local telephone device, and the key commands you need to configure are the **port** and **destination-pattern** 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—dial peer associates a telephone number with an IP address, and 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

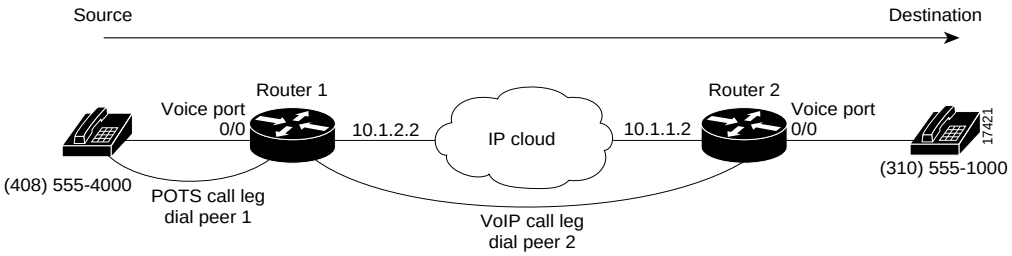
Dial peers are used for both inbound and outbound call legs. It is important to remember that these terms are defined from the *router* perspective. An inbound call leg means that an incoming call comes *to* the router. An outbound call leg means that an outgoing call is placed *from* the router.

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

POTS dial peer associate 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. Both POTS and VoIP dial peers are needed to establish VoIP connections.

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 2-5, for outgoing calls (from the perspective of the POTS dial peer 1), 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 2-5 Outgoing Calls from the Perspective of POTS Dial Peer 1



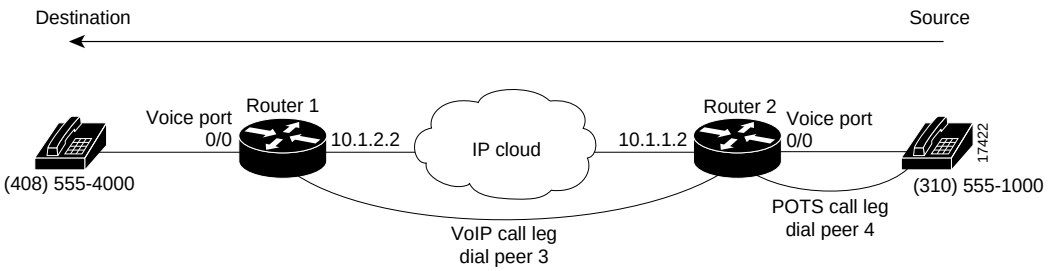
To configure call connectivity between the source and the destination as illustrated in Figure 2-5, enter the following commands on router 10.1.2.2:

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

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

Figure 2-6 shows how to complete the end-to-end call between dial peer 1 and dial peer 4.

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



To complete the end-to-end call between dial peer 1 and dial peer 4 as illustrated in Figure 2-6, enter the following commands on router 10.1.1.2:

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

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

Create a Dial-Peer Configuration Table

There is specific data relative to each dial peer that needs to be identified before you can configure dial peers in VoIP. One way to do this is to create a dial peer configuration table.

Using the example in Figure 2-2, 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, all of which are basic telephones connected to the PBX. Figure 2-2 on page 2-8 shows a diagram of this small voice network, and Table 2-1 shows the dial peer configuration table for the example in the figure.

Table 2-2 Dial-Peer Configuration Table for Sample VoIP Network

		Commands				
Router	**Dial Peer Tag**	**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 following global configuration command:

```
Router(config)# dial-peer voice number pots
```

The *number* value of the **dial-peer voice pots** command is a tag that uniquely identifies the dial peer. (This number has local significance only.)

To configure the identified POTS dial peer, use the following dial peer configuration command:

```
Router(config-dial-peer)# destination-pattern string
```

The *string* value of the **destination-pattern command** is the destination telephone number associated with this POTS dial peer.

Outbound Dialing on POTS Dial Peers

When a router receives a voice call, it selects an outbound dial peer by comparing the called number (the full E.164 telephone number) in the call information 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 (depending on the attached equipment) 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 prefix *9*, to 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.

For additional POTS dial-peer configuration options, refer to the "VoIP Commands" chapter.

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. As with POTS dial peers, under most circumstances the default values for the remaining dial peer configuration commands are adequate to establish connections.

To enter the dial peer configuration mode (and select VoIP as the method of voice-related encapsulation), use the following global configuration command:

```
Router(config)# dial-peer voice number voip
```

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

:

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

For additional VoIP dial peer configuration options, refer to the "VoIP Commands" chapter. For examples of how to configure dial peers, refer to the "VoIP Configuration Examples" chapter.

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" chapter in the Network Protocols Configuration Guide, Part 1 for Cisco IOS Release 12.0T.
- Use the **show dial-peer voice** command to verify that the operational status of the dial peer is up.
- Use the **show dialplan number** command on the local and remote routers to verify that the data is configured correctly on both.
- 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.

Caution If you are not familiar with Cisco IOS debug commands, you should read the "Using Debug Commands" section in the "VoIP Debug Commands" chapter before attempting any debugging.

- Use the **debug vpm spi** command to verify the output string the router dials is correct.
- 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

Your router provides only analog voice ports for its implementation of VoIP. The type of signaling associated with these 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, PBXs, or similar device, and 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 PBX that does not support E&M signaling. This interface is used for off-premise extension applications.

- E&M—The E&M interface uses a 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 following commands beginning in privileged EXEC mode:

	Command	Required / Optional	Task
Step 1	**configure terminal**	Required	Enter the global configuration mode.
Step 2	**voice-port** *slot-number/port*	Required	Identify the voice port you want to configure and enter the voice port configuration mode.
Step 3	**dial-type** {**dtmf** | **pulse**}	Required	(For FXO ports only) Select the appropriate dial type for out-dialing.
Step 4	**signal** {**loop-start** | **ground-start**}	Required	Select the appropriate signal type for this interface.
Step 5	**cptone** *country*	Required	Select the appropriate voice call progress tone for this interface. The default for this command is **us**. For a list of supported countries, refer to Chapter 4, "VoIP Commands."
Step 6	**ring frequency** {**25** | **50**}	Required	(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.
Step 7	**ring number** *number*	Required	(For FXO ports only) Specify the maximum number of rings before answering a call.
Step 8	**connection plar** *string*	Optional	Specify the private line auto ringdown (PLAR) connection if this voice port is used for a PLAR connection. The *string* value specifies the destination telephone number.
Step 9	**music-threshold** *number*	Optional	Specify the threshold (in dB) for on-hold music. Valid entries are from –70 to –30 db.
Step 10	**description** *string*	Optional	Attach descriptive text about this voice-port connection.
Step 11	**comfort-noise**	Optional	If voice activity detection (VAD) is activated, specify that background noise is generated.

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 you have a dial tone. 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 your 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 <Emphasis>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 following commands beginning in privileged EXEC mode:

	Command	Task	Valid Entries	Default Values
Step 1	**configure terminal**	Enter the global configuration mode.		
Step 2	**voice-port** *slot-number/port*	Identify the voice port you want to configure, and enter the voice port configuration mode.		
Step 3	**input gain** *value*	Specify (in dB) the amount of gain to be inserted at the receiver side of the interface.	–6 to 14 dB	0 dB
Step 4	**output attenuation** *value*	Specify (in dB) the amount of attenuation at the transmit side of the interface.	0 to 14 dB	0 dB

	Command	Task	Valid Entries	Default Values
Step 5	**echo-cancel enable**	Enable echo-cancellation of voice that is sent out of the interface and received back on the same interface.		
Step 6	**echo-cancel coverage** *value*	Adjust the size (in milliseconds) of the echo-cancel.	8, 16, 24, and 32 ms	16 ms
Step 7	**non-linear**	Enable nonlinear processing, which shuts off any signal if no near-end speech is detected. (Nonlinear processing is used with echo-cancellation.)		
Step 8	**timeouts initial** *seconds*	Specify the number of seconds the system will wait for the caller to input the first digit of the dialed digits.	0 to 120 sec	10 sec
Step 9	**timeouts interdigit** *seconds*	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.	0 to 120 sec	10 sec
Step 10	**timing digit** *milliseconds*	If the voice-port dial type is DTMF, configure the DTMF digit signal duration.	50 to 100 ms	100 ms
Step 11	**timing inter-digit** *milliseconds*	If the voice-port dial type is DTMF, configure the DTMF inter-digit signal duration.	50 to 500 ms	100 ms
Step 12	**timing pulse-digit** *milliseconds*	(FXO ports only) If the voice-port dial type is pulse, configure the pulse digit signal duration.	10 to 20 ms	20 ms
Step 13	**timing pulse-inter-digit** *milliseconds*	(FXO ports only) If the voice-port dial type is pulse, configure the pulse inter-digit signal duration.	100 to 1000 ms	500 ms

Note After you change any voice-port command, we recommend 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 following commands beginning in privileged EXEC mode:

	Command	Required / Optional	Task
Step 1	**configure terminal**	Required	Enter the global configuration mode.
Step 2	**voice-port** *slot-number/port*	Required	Identify the voice port you want to configure, and enter the voice port configuration mode.
Step 3	**dial-type** {**dtmf** | **pulse**}	Required	Select the appropriate dial type for out-dialing.
Step 4	**signal** {**wink-start** | **immediate** | **delay-dial**}	Required	Select the appropriate signal type for this interface.
Step 5	**cptone** {**australia** | **brazil** | **china** | **finland** | **france** | **germany** | **japan** | **northamerica** | **unitedkingdom**}	Required	Select the appropriate voice call progress tone for this interface.
Step 6	**operation** {**2-wire** | **4-wire**}	Required	Select the appropriate cabling scheme for this voice port.
Step 7	**type** {**1** | **2** | **3** | **5**}	Required	Select the appropriate E&M interface type. Type 1 is for the following lead configuration: E—output, relay to ground M—input, referenced to ground Type 2 is for the following lead configuration: 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: 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: E—output, relay to ground M—input, referenced to –48V.

	Command	Required / Optional	Task
Step 8	**impedance** {**600c** | **600r** | **900c** | **complex1** | **complex2**}	Required	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.
Step 9	**connection plar** *string*	Optional	Specify the private line auto ringdown (PLAR) connection if this voice port is used for a PLAR connection. The *string* value specifies the destination telephone number.
Step 10	**music-threshold** *number*	Optional	Specify the threshold (in dB) for on-hold music. Valid entries are from –70 to –30 dB. The default is –38 dB.
Step 11	**description** *string*	Optional	Attach descriptive text about this voice-port connection.
Step 12	**comfort-noise**	Optional	Specify that background noise is generated.

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 you have a dial tone. 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 your 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.
- 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 <Emphasis>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 following commands beginning in privileged EXEC mode:

	Command	Task	Valid Entries	Default Values
Step 1	**configure terminal**	Enter the global configuration mode.		
Step 2	**voice-port** *slot-number/port*	Identify the voice port you want to configure, and enter the voice port configuration mode.		
Step 3	**input gain** *value*	Specify (in dB) the amount of gain to be inserted at the receiver side of the interface.	–6 to 14 dB	0 dB
Step 4	**output attenuation** *value*	Specify (in dB) the amount of attenuation at the transmit side of the interface.	0 to 14 dB	0 dB
Step 5	**echo-cancel enable**	Enable echo-cancellation of voice that is sent out of the interface and received back on the same interface.		
Step 6	**echo-cancel coverage** *value*	Adjust the size (in milliseconds) of the echo-cancel.	8, 16, 24, and 32 ms	16 ms
Step 7	**non-linear**	Enable nonlinear processing, which shuts off any signal if no near-end speech is detected. (Nonlinear processing is used with echo-cancellation.)		
Step 8	**timeouts initial** *seconds*	Specify the number of seconds the system will wait for the caller to input the first digit of the dialed digits.	0 to 120 sec	10 sec
Step 9	**timeouts interdigit** *seconds*	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.	0 to 120 sec	10 sec

	Command	Task	Valid Entries	Default Values
Step 10		**Specify timing parameters for each of these commands.**		
	timing clear-wait *milliseconds*		200 to 2000 ms	
	timing delay-duration *milliseconds*		100 to 5000 ms 20 to 2000 ms	
	timing delay-start *milliseconds*		0 to 5000 ms	
	timing dial-pulse min-delay *milliseconds*		50 to 100 ms	
	timing digit *milliseconds*		50 to 500 ms	
	timing inter-digit *milliseconds*		10 to 20 pps	
	timing pulse *pulses-per-second*		100 to 1000 ms	
	timing pulse-inter-digit *milliseconds*		100 to 400 ms 100 to 5000 ms	
	timing wink-duration *milliseconds*			
	timing wink-wait *milliseconds*			

Note After you change any voice-port command, we recommend 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
- Configure RSVP for Dial Peers
- Configure CODEC and VAD for Dial Peers

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:

Step	Command	Task
1.	**dial-peer voice** *number* **voip**	Enter the dial peer configuration mode to configure a VoIP dial peer.
2.	**ip precedence** *number*	Select a precedence level for the voice traffic associated with that dial peer.

	Command	Task
Step 1	**dial-peer voice** *number* **voip**	Enter the dial peer configuration mode to configure a VoIP dial peer.
Step 2	**ip precedence** *number*	Select a precedence level for the voice traffic associated with that dial peer.

In IP precedence, the numbers 1 through 5 identify classes for IP flows; the numbers 6 through 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:

```
Router(config)# dial-peer voice 103 voip
Router(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 that voice packets will travel across. 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.

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

```
Router(config)# Dial-peer voice 108 voip
Router(config-dial-peer)# req-qos controlled-load
Router(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 We recommend that you select **controlled-load** for the requested QoS. The controlled-load service uses admission (or capacity) control to ensure that preferential service is received even when the bandwidth is overloaded.

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

	Command	Task
Step 1	**dial-peer voice** *number* **voip**	Enter the dial peer configuration mode to configure a VoIP dial peer.

	Command	Task
Step 2	**acc-qos** [**best-effort** | **controlled-load** | **guaranteed-delay**]	Generate an SNMP event if the QoS for a dial peer drops below a specified level.

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

CODEC typically is used to transform analog signals into a digital bit stream and digital signals back into analog signals—in this case, it 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, initially beginning in global configuration mode:

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

The default for the **codec** command is **g729r8**; normally, the default configuration for this command is the most desirable. 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 this value results in better voice quality, but it also requires higher bandwidth requirements for voice.

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

```
Router(config)# dial-peer voice 108 voip
Router(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. Whenever new images (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:

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

The default for the **vad** command is enabled; normally, the default configuration for this command is the most desirable. If you are operating on a high bandwidth network and voice quality is of the highest importance, you should disable VAD. Using this value results in better voice quality, but it also requires higher bandwidth requirements for voice.

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

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

Configure Frame Relay for VoIP

You need to take certain factors into consideration when configuring VoIP so that it runs smoothly over Frame Relay. A public Frame Relay cloud provides no guarantees for QoS. For real-time traffic to be transmitted in a timely manner, the data rate must not exceed the committed information rate (CIR), or there is the possibility that packets are 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 being transmitted over the same permanent virtual circuit (PVC), we recommend 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 maximum transmission unit (MTU) size—Voice packets are generally small. By lowering 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 affects data throughput speed.

- CIR equal to line rate—Make sure that the data rate does not exceed the CIR. This is accomplished through generic traffic shaping.

  - Use RSVP or IP precedence to prioritize voice traffic.
  - Use compressed RTP to minimize voice packet header size.
- Traffic shaping—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 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 of 125 milliseconds.

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

- Provision the Frame Relay 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 Serial1 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" chapter in the *Wide-Area Networking Configuration Guide* for Cisco IOS Release 12.0T.

Configure Microsoft NetMeeting for VoIP

VoIP can be used with Microsoft NetMeeting (Version 2.x) when your router is used as the voice gateway. Use the latest version of DirectX drivers from Microsoft on your PC to improve the voice quality of NetMeeting.

Configure VoIP to Support Microsoft NetMeeting

To configure VoIP to support NetMeeting, create a VoIP dial peer that has the following information:

- Session Target—IP address or domain name system (DNS) name of the PC running NetMeeting
- CODEC—g711ulaw or g711alaw

Configure Microsoft NetMeeting for VoIP

To configure NetMeeting to work with VoIP, complete the following steps:

Step 1 From the Tools menu in the NetMeeting application, select **Options**. NetMeeting will display the Options dialog box.

Step 2 Click the **Audio** tab.

Step 3 Select the "Calling a telephone using NetMeeting" check box.

Step 4 Enter the IP address of your router in the **IP address** field.

Step 5 Under **General**, click **Advanced**.

Step 6 Select the "Manually configured compression settings" check box.

Step 7 Select the CODEC value **CCITT ulaw 8000Hz**.

Step 8 Click the **Up** button until this CODEC value is at the top of the list.

Step 9 Click **OK** to exit.

Initiate a Call Using Microsoft NetMeeting

To initiate a call using Microsoft NetMeeting, perform the following steps:

Step 1 Click the **Call** icon from the NetMeeting application. Microsoft NetMeeting opens the call dialog box.

Step 2 From the Call dialog box, select **call using H.323 gateway**.

Step 3 Enter the telephone number in the **Address** field. (Enter 1 and the area code followed by the seven-digit telephone number in the following format 1Nxx-Nxx-xxxx, with N = digits 2 through 9 and x = digits 0 through 9.)

Step 4 Click **Call** to initiate a call to your router from Microsoft NetMeeting.