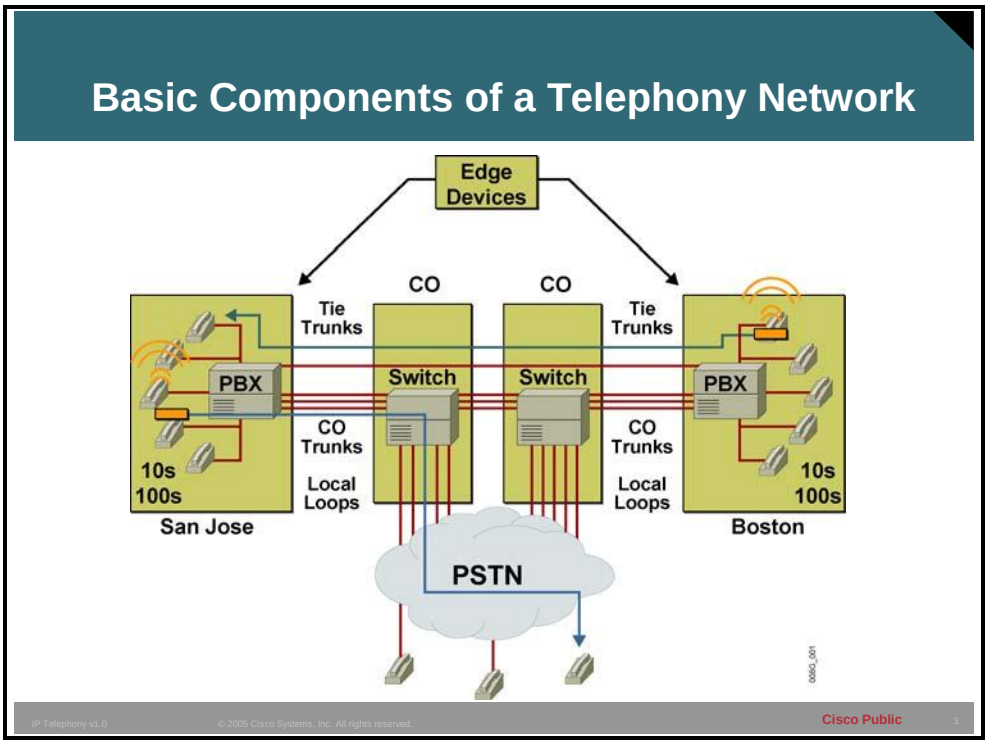
Traditional Telephony

Basic Components of a Telephony Network

This topic introduces the components of traditional telephony networks.



A number of components must be in place for an end-to-end call to succeed. These components are shown in the figure and include the following:

- Edge devices
- Local loops
- Private or central office (CO) switches
- Trunks

Edge Devices

The two types of edge devices that are used in a telephony network include:

- **Analog telephones:** Analog telephones are most common in home, small office/home office (SOHO), and small business environments. Direct connection to the PSTN is usually made by using analog telephones. Proprietary analog telephones are occasionally used in conjunction with a PBX. These telephones provide additional functions such as speakerphone, volume control, PBX message-waiting indicator, call on hold, and personalized ringing.
- **Digital telephones:** Digital telephones contain hardware to convert analog voice into a digitized stream. Larger corporate environments with PBXs generally use digital

telephones. Digital telephones are typically proprietary, meaning that they work with the PBX or key system of that vendor only.

Local Loops

A local loop is the interface to the telephone company network. Typically, it is a single pair of wires that carry a single conversation. A home or small business may have multiple local loops.

Private or CO Switches

The CO switch terminates the local loop and handles signaling, digit collection, call routing, call setup, and call teardown.

A PBX switch is a privately owned switch located at the customer site. A PBX typically interfaces with other components to provide additional services, such as voice mail.

Trunks

The primary function of a trunk is to provide the path between two switches. There are several common trunk types, including:

- **Tie trunk:** A dedicated circuit that connects PBXs directly
- **CO trunk:** A direct connection between a local CO and a PBX
- **Interoffice trunk:** A circuit that connects two local telephone company COs

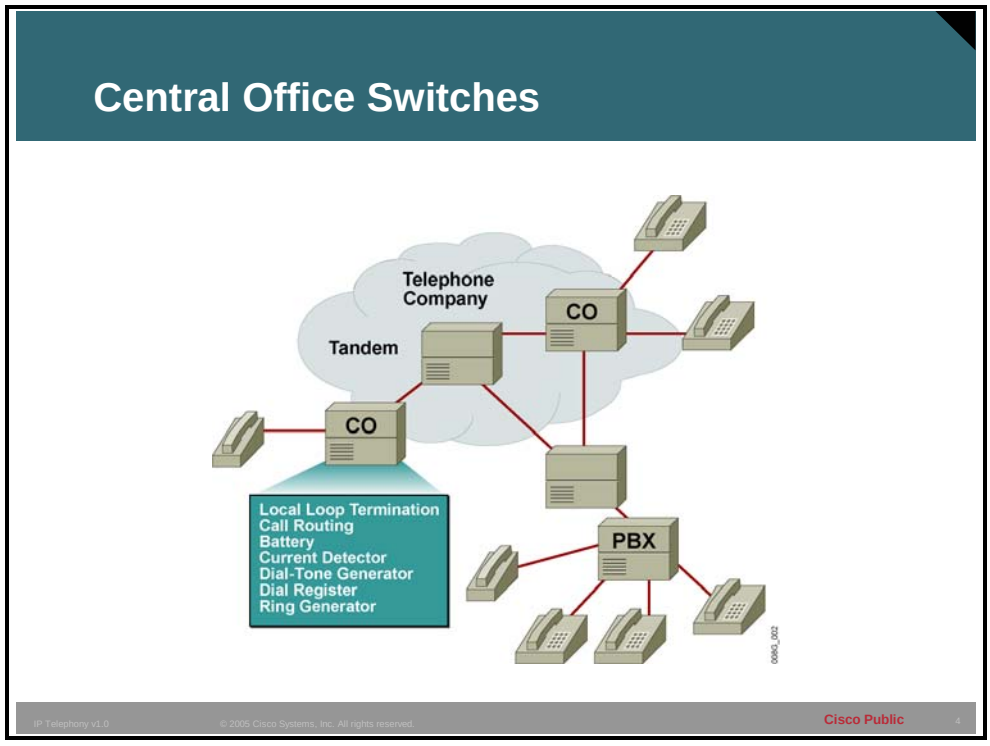
Example: Telephony Components

The telephone installed in your home is considered an edge device because it terminates the service provided by your local telephone company. PBXs or key systems installed in a business would also be considered edge devices. The local loop is the pair of wires that come to your house to provide residential telephone service. Trunks are the interconnections between telephone switches. They can be between private switches or telephone company switches.

 Copyright © 2005, Cisco Systems, Inc.

CO Switches

This topic describes how CO switches function and make switching decisions.



The figure shows a typical CO switch environment. The CO switch terminates the local loop and makes the initial call-routing decision.

The call-routing function forwards the call to one of the following:

- Another end-user telephone, if it is connected to the same CO
- Another CO switch
- A tandem switch

The CO switch makes the telephone work with the following components:

- **Battery:** The battery is the source of power to both the circuit and the telephone. It determines the status of the circuit. When the handset is lifted to let current flow, the telephone company provides the source that powers the circuit and the telephone. Because the telephone company powers the telephone from the CO, electrical power outages should not affect the basic telephone.

Note	Some telephones on the market offer additional features that require a supplementary power source that the subscriber supplies; for example, cordless telephones. Some cordless telephones may lose function during a power outage.

- **Current detector:** The current detector monitors the status of a circuit by detecting whether it is open or closed. The table here describes current flow in a typical telephone.

Current Flow in a Typical Telephone

Handset	Circuit	Current Flow
On cradle	On hook/open circuit	No
Off cradle	Off hook/closed circuit	Yes

- **Dial-tone generator:** When the digit register is ready, the dial-tone generator produces a dial tone to acknowledge the request for service.
- **Dial register:** The digit register receives the dialed digits.
- **Ring generator:** When the switch detects a call for a specific subscriber, the ring generator alerts the called party by sending a ring signal to that subscriber.

You must configure a PBX connection to a CO switch that matches the signaling of the CO switch. This configuration ensures that the switch and the PBX can detect on hook, off hook, and dialed digits coming from either direction.

CO Switching Systems

Switching systems provide three primary functions:

- Call setup, routing, and teardown
- Call supervision
- Customer ID and telephone numbers

CO switches switch calls between locally terminated telephones. If a call recipient is not locally connected, the CO switch decides where to send the call based on its call-routing table. The call then travels over a trunk to another CO or to an intermediate switch that may belong to an inter-exchange carrier (IXC). Although intermediate switches do not provide dial tone, they act as hubs to connect other switches and provide interswitch call routing.

PSTN calls are traditionally circuit-switched, which guarantees end-to-end path and resources. Therefore, as the PSTN sends a call from one switch to another, the same resource is associated with the call until the call is terminated.

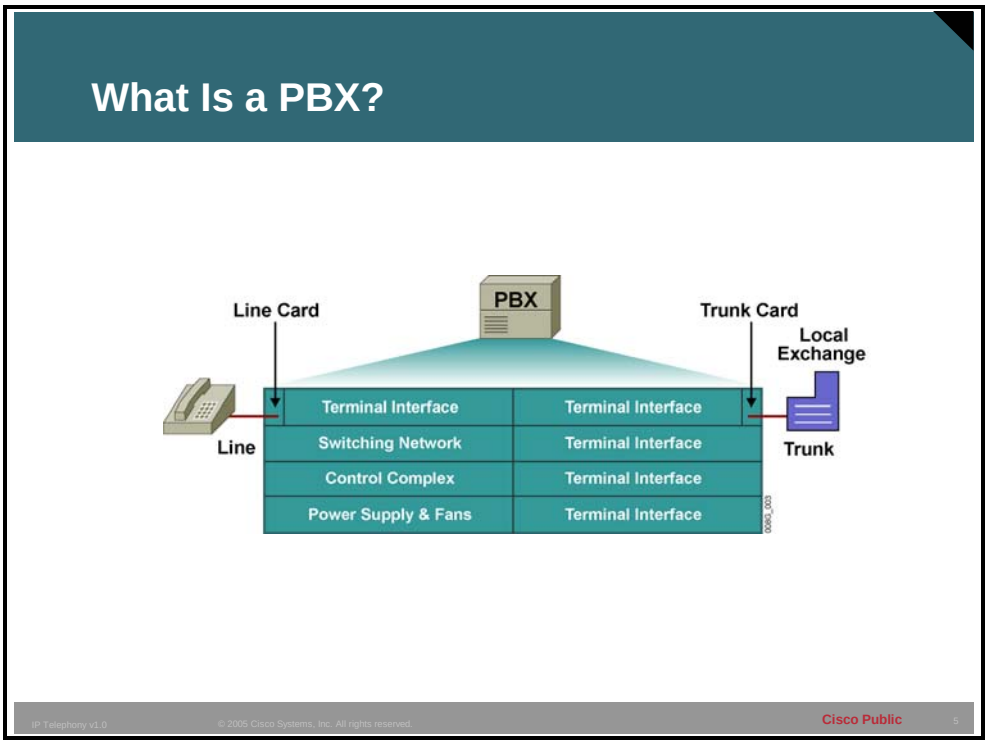
Example: CO Switches

CO switches provide local service to your residential telephone. The CO switch provides dial tone, indicating that the switch is ready to receive digits. When you dial your phone, the CO switch receives the digits, then routes your call. The call routing may involve more than one switch as the call progresses through the network.

 Copyright © 2005, Cisco Systems, Inc.

Private Switching Systems

In a corporate environment, where large numbers of staff need access to each other and the outside, individual telephone lines are not economically viable. This topic explores PBX and key telephone system functionality in environments today.



A PBX is a smaller, privately owned version of the CO switches used by telephone companies.

Most businesses have a PBX telephone system, a key telephone system, or Centrex service. Large offices with more than 50 telephones or handsets choose a PBX to connect users, both in-house and to the PSTN.

PBXs come in a variety of sizes, from 20 to 20,000 stations. The selection of a PBX is important to most companies because a PBX has a typical life span of seven to ten years.

All PBXs offer a standard, basic set of calling features. Optional software provides additional capabilities.

The figure illustrates the internal components of a PBX. It connects to telephone handsets using line cards and to the local exchange using trunk cards.

A PBX has three major components:

- **Terminal interface:** The terminal interface provides the connection between terminals and PBX features that reside in the control complex. Terminals can include telephone handsets, trunks, and lines. Common PBX features include dial tone and ringing.
- **Switching network:** The switching network provides the transmission path between two or more terminals in a conversation. For example, two telephones within an office communicate over the switching network.
- **Control complex:** The control complex provides the logic, memory, and processing for call setup, call supervision, and call disconnection.

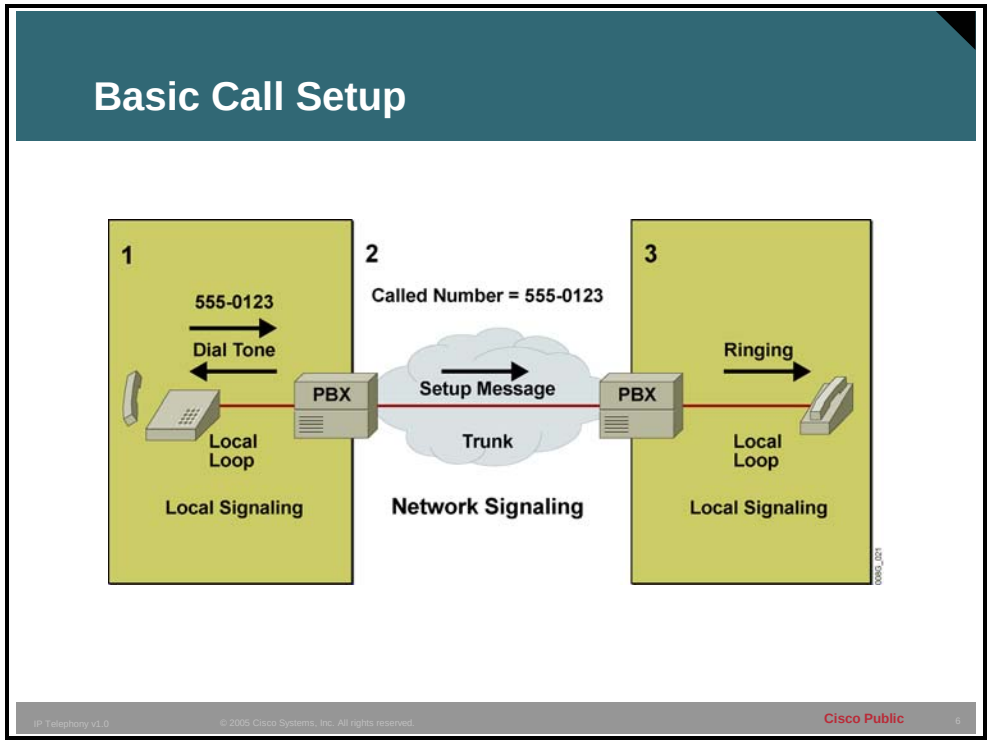
Example: PBX Installations

PBX switches are installed in large business campuses to relieve the public telephone company switches from having to switch local calls. When you call a coworker locally in your office campus, the PBX switches the call locally instead of having to rely on the public CO switch. The existence of PBX switches also limits the number of trunks needed to connect to the telephone company's CO switch. With a PBX installed, every office desktop telephone does not need its own trunk to the CO switch. Rather, the trunks are shared among all users.

 Copyright © 2005, Cisco Systems, Inc.

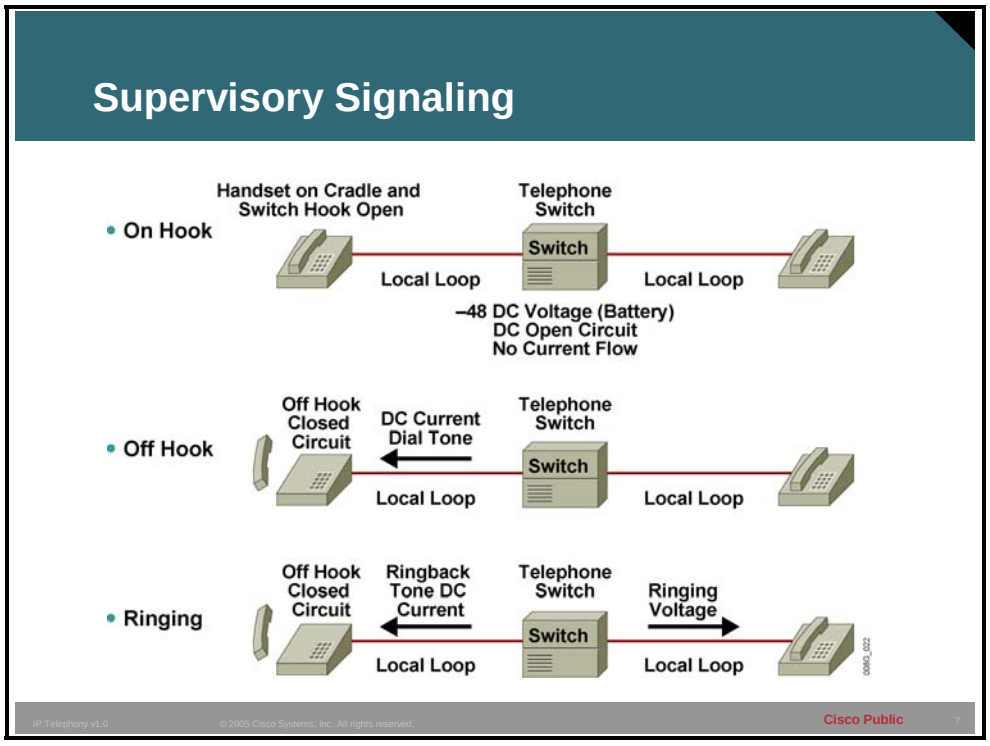
Call Signaling

Call signaling, in its most basic form, is the capacity of a user to communicate a need for service to a network. The call-signaling process requires the ability to detect a request for service and termination of service, send addressing information, and provide progress reports to the initiating party. This functionality corresponds to the three call-signaling types discussed in this topic: supervisory, address, and informational signaling.



The figure shows the three major steps in an end-to-end call. These steps include:

1. **Local signaling — originating side:** The user signals the switch by going off hook and sending dialed digits through the local loop.
2. **Network signaling:** The switch makes a routing decision and signals the next, or terminating, switch through the use of setup messages sent across a trunk.
3. **Local signaling — terminating side:** The terminating switch signals the call recipient by sending ringing voltage through the local loop to the recipient telephone.



A subscriber and telephone company notify each other of call status with audible tones and an exchange of electrical current. This exchange of information is called supervisory signaling.

There are three different types of supervisory signaling:

- **On hook:** When the handset rests on the cradle, the circuit is on hook. The switch prevents current from flowing through the telephone. Regardless of the signaling type, a circuit goes on hook when the handset is placed on the telephone cradle and the switch hook is toggled to an open state. This prevents the current from flowing through the telephone. Only the ringer is active when the telephone is in this position.
- **Off hook:** When the handset is removed from the telephone cradle, the circuit is off hook. The switch hook toggles to a closed state, causing circuit current to flow through the electrical loop. The current notifies the telephone company equipment that someone is requesting to place a telephone call. When the telephone network senses the off-hook connection by the flow of current, it provides a signal in the form of a dial tone to indicate that it is ready.
- **Ringing:** When a subscriber makes a call, the telephone sends voltage to the ringer to notify the other subscriber of an inbound call. The telephone company also sends a ringback tone to the caller alerting the caller that it is sending ringing voltage to the recipient telephone. Although the ringback tone sounds similar to ringing, it is a call-progress tone and not part of supervisory signaling.

Note	The ringing tone in the United States is 2 seconds of tone followed by 4 seconds of silence. Europe uses a double ring followed by 2 seconds of silence.

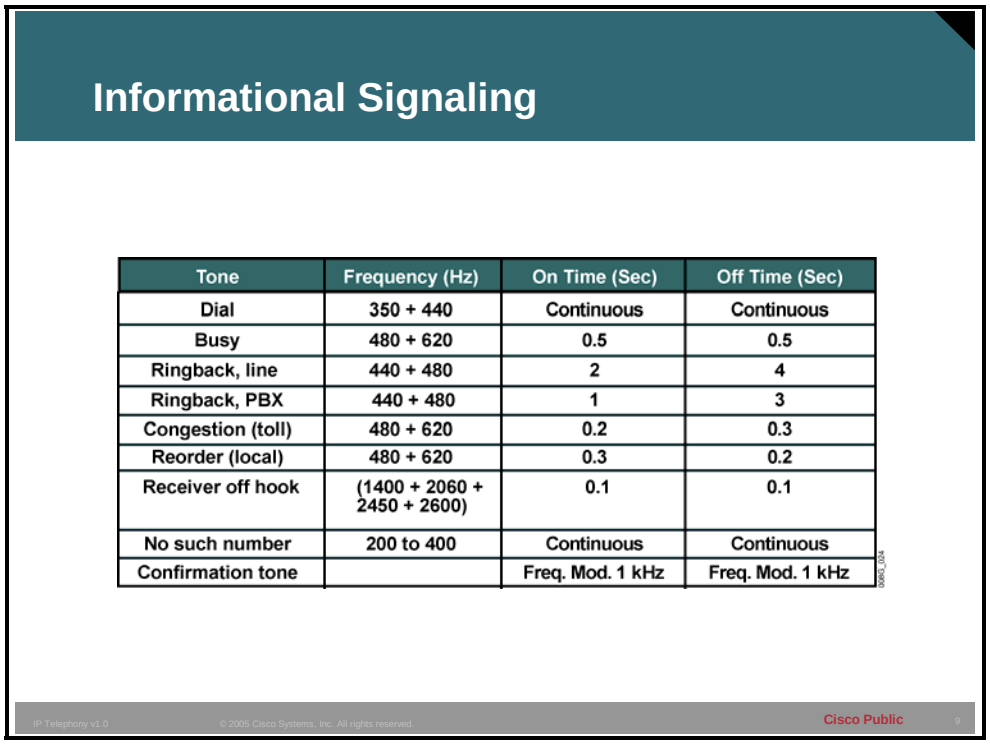
 Copyright © 2005, Cisco Systems, Inc.



There are two types of telephones: a rotary-dial telephone and a push-button (tone) telephone. These telephones use two different types of address signaling to notify the telephone company where a subscriber is calling:

- **Dual tone multifrequency:** Each button on the keypad of a touch-tone pad or push-button telephone is associated with a set of high and low frequencies. On the keypad, each row of keys is identified by a low-frequency tone and each column is associated with a high-frequency tone. The combination of both tones notifies the telephone company of the number being called, thus the term “dual tone multifrequency” (DTMF).
- **Pulse:** The large numeric dial-wheel on a rotary-dial telephone spins to send digits to place a call. These digits must be produced at a specific rate and within a certain level of tolerance. Each pulse consists of a “break” and a “make,” which are achieved by opening and closing the local loop circuit. The break segment is the time during which the circuit is open. The make segment is the time during which the circuit is closed. The break-and-make cycle must correspond to a ratio of 60 percent break to 40 percent make.

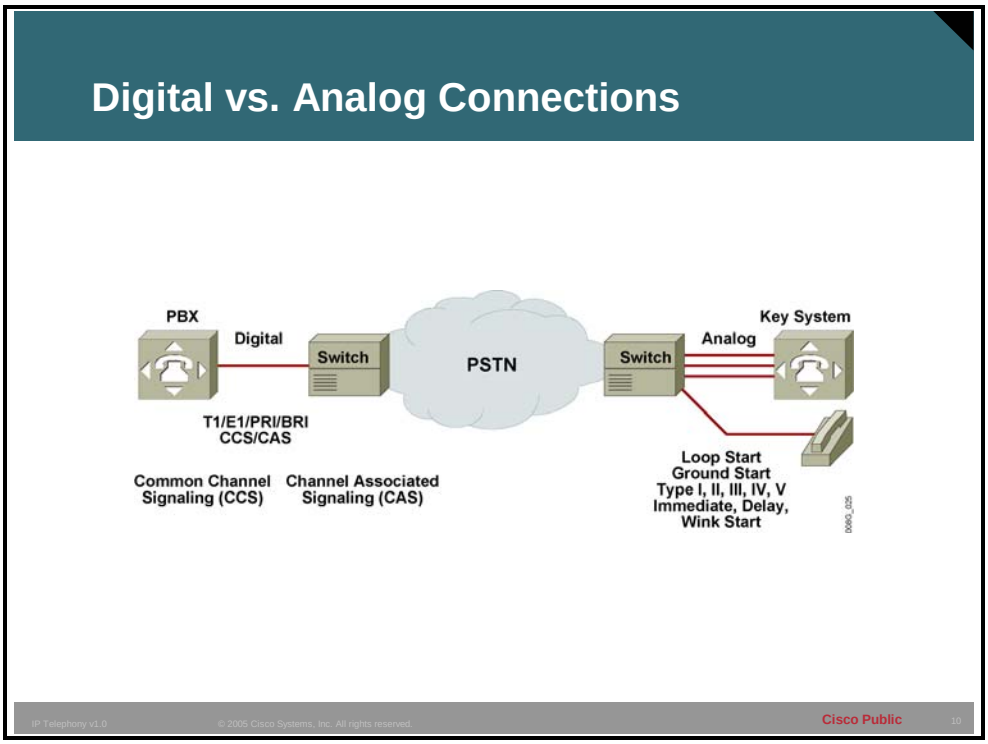
  A governor inside the dial controls the rate at which the digits are pulsed; for example, when a subscriber calls someone by dialing a digit on the rotary dial, a spring winds. When the dial is released, the spring rotates the dial back to its original position. While the spring rotates the dial back to its original position, a cam-driven switch opens and closes the connection to the telephone company. The number of consecutive opens and closes, or breaks and makes, represents the dialed digit.



Tone combinations indicate call progress and are used to notify subscribers of call status. Each combination of tones represents a different event in the call process. These events include the following:

- **Dial tone:** Indicates that the telephone company is ready to receive digits from the user telephone
- **Busy:** Indicates that a call cannot be completed because the telephone at the remote end is already in use
- **Ringback (normal or PBX):** Indicates that the telephone company is attempting to complete a call on behalf of a subscriber
- **Congestion:** Indicates that congestion in the long-distance telephone network is preventing a telephone call from being processed
- **Reorder tone:** Indicates that all the local telephone circuits are busy, thus preventing a telephone call from being processed
- **Receiver off hook:** Indicates that a receiver has been off hook for an extended period of time without placing a call
- **No such number:** Indicates that a subscriber has placed a call to a nonexistent number
- **Confirmation tone:** Indicates that the telephone company is attempting to complete a call

 Copyright © 2005, Cisco Systems, Inc.



Supervisory, address, and informational signaling must be carried across both analog and digital connections. Depending on your connection to the network, you must configure specific signaling to match the type of signaling required by the service provider.

Digital PBX connections to the network are common in many countries. They may be a T1 or E1 line carrying channel associated signaling (CAS) or a PRI using common channel signaling (CCS).

CAS is a signaling method that allows passing on-hook or off-hook status by setting bits that are associated with each specific voice channel. These bits are carried in band for T1 and out of band for E1.

An ISDN connection uses the D channel as the common channel to carry signaling messages for all other channels. CCS carries the signaling out of band, meaning that the signaling and the voice path do not share the same channel.

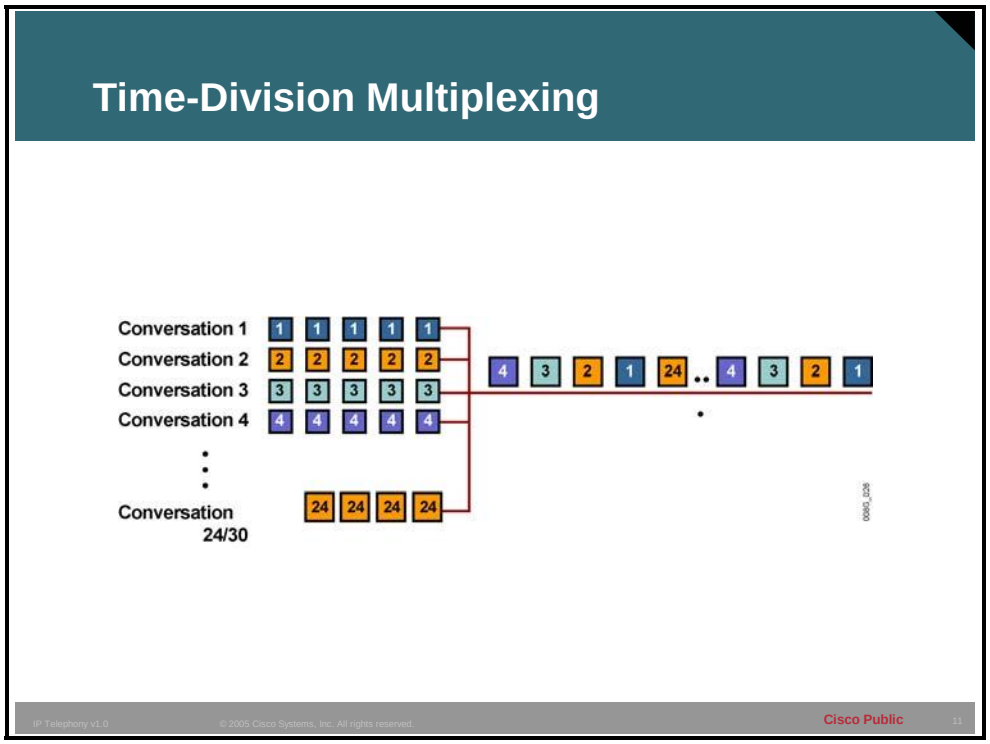
Analog interfaces require configuration of a specific signaling type to match the provider requirement. For interfaces that connect to the PSTN or to a telephone or similar edge device, the signaling is configured for either loop start or ground start. For analog trunk interfaces that connect two PBXs to each other, or a PBX to a CO switch, the signaling is either Wink Start, immediate start, or delay start with the signaling type set to 1, 2, 3, 4, or 5.

Example: Call Signaling at Home

A call placed from your residential telephone uses all three types of call signaling. When you lift the handset, a switch in your telephone closes to start current flow and notifies the telephone company that you want to make a call (supervisory signaling). The telephone company then sends dial tone to indicate that it is ready to receive your dialed digits (informational signaling). You then dial your digits by pressing the number on the keypad (address signaling).

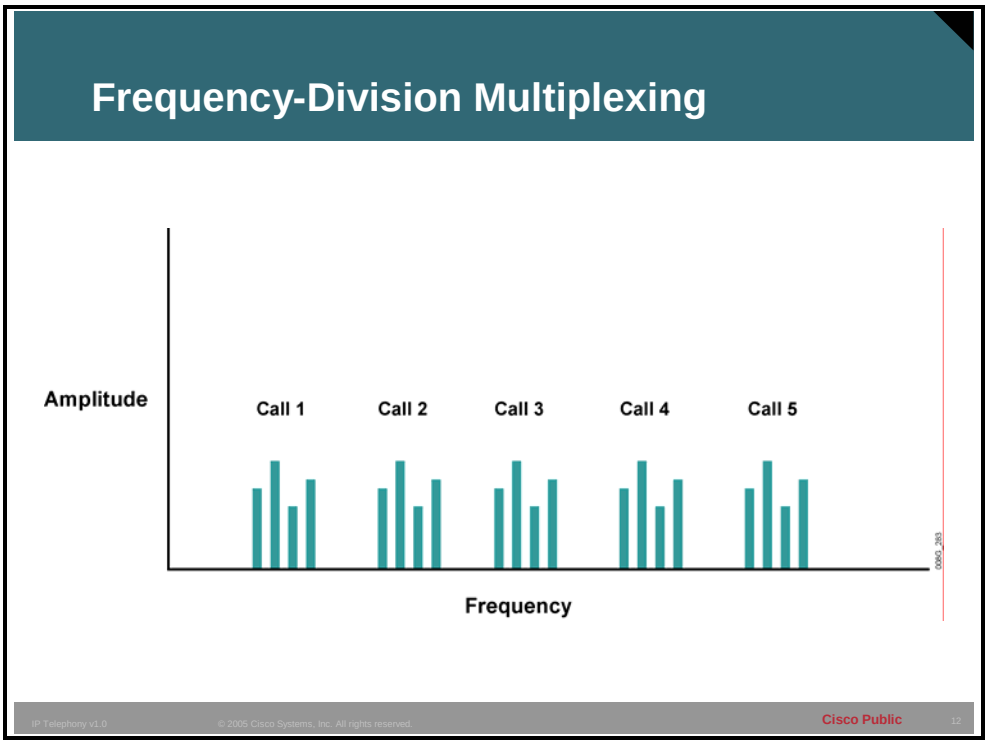
Multiplexing Techniques

A two-wire analog local loop typically carries one call at a time. To make better use of wiring facilities, different multiplexing techniques have been implemented to enable two-wire or four-wire connections to carry multiple conversations at the same time. This topic discusses two of these multiplexing techniques.



Time-division multiplexing (TDM) is used extensively in telephony networks to carry multiple conversations concurrently across a four-wire path. TDM involves simultaneously transmitting multiple separate voice signals over one communications medium by quickly interleaving pieces of each signal, one after another. Information from each data channel is allocated bandwidth based on preassigned timeslots, regardless of whether there is data to transmit.

 Copyright © 2005, Cisco Systems, Inc.



Frequency-division multiplexing (FDM) involves carrying multiple voice signals by allocating an individual frequency range to each call. FDM is typically used in analog connections, although its functionality is similar to that of TDM in digital connections. FDM is used in cable or digital subscriber line (DSL) connections to allow the simultaneous use of multiple channels over the same wire.

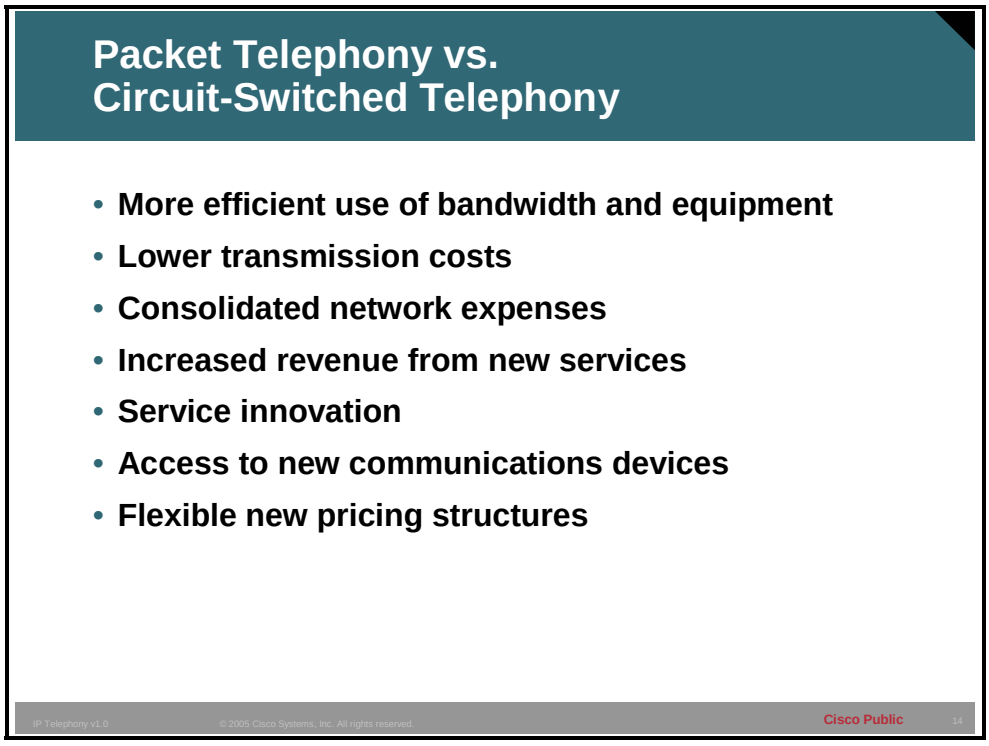
Example: Multiplexing Television Channels

If you have cable television service at your home, the television channels are all carried (and multiplexed) over a single pair of wires. This includes both the audio signals and the video signals. Your set-top cable tuner then determines which channel is sent to your television by way of selecting the channel you want to watch. All of the channels are present on the cable wires all of the time, but you tune your selected channel using the set-top tuner.

Packetized Telephony Networks

Benefits of Packet Telephony Networks

Traditionally, the potential savings on long-distance costs was the driving force behind the migration to converged voice and data networks. The cost of long-distance calls has dropped in recent years, and other factors have come to the forefront as benefits of converged networks. This topic describes some of these benefits.



The benefits of packet telephony versus circuit-switched telephony are as follows:

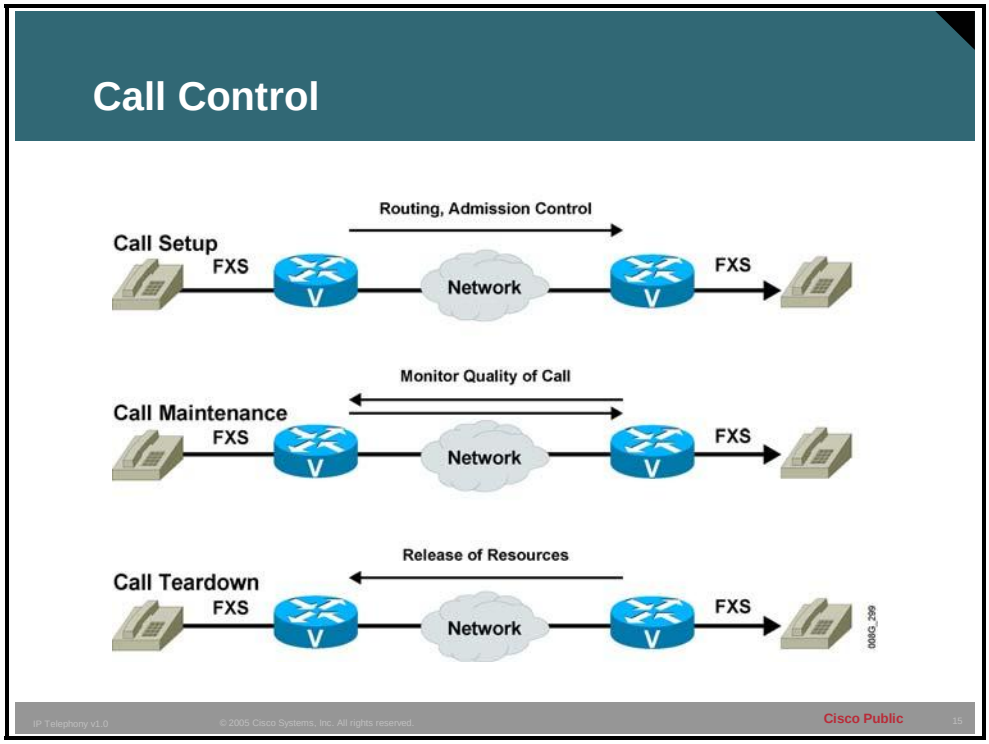
- **More efficient use of bandwidth and equipment:** Traditional telephony networks use a 64-kbps channel for every voice call. Packet telephony shares bandwidth among multiple logical connections and offloads traffic volume from existing voice switches.
- **Lower costs for telephony network transmission:** A substantial amount of equipment is needed to combine 64-kbps channels into high-speed links for transport across the network. Packet telephony statistically multiplexes voice traffic alongside data traffic. This consolidation represents substantial savings on capital equipment and operations costs.
- **Consolidated voice and data network expenses:** Data networks that function as separate networks to voice networks become major traffic carriers. The underlying voice networks are converted to utilize the packet-switched architecture to create a single integrated communications network with a common switching and transmission system. The benefit is significant cost savings on network equipment and operations.

 Copyright © 2005, Cisco Systems, Inc.

- **Increased revenues from new services:** Packet telephony enables new integrated services, such as broadcast-quality audio, unified messaging, and real-time voice and data collaboration. These services increase employee productivity and profit margins well above those of basic voice services. In addition, these services enable companies and service providers to differentiate themselves and improve their market position.
- **Greater innovation in services:** Unified communications use the IP infrastructure to consolidate communication methods that were previously independent; for example, fax, voice mail, e-mail, wireline telephones, cellular telephones, and the web. The IP infrastructure provides users with a common method to access messages and initiate real-time communications—independent of time, location, or device.
- **Access to new communications devices:** Packet technology can reach devices that are largely inaccessible to the TDM infrastructures of today. Examples of such devices are computers, wireless devices, household appliances, personal digital assistants, and cable set-top boxes. Intelligent access to such devices enables companies and service providers to increase the volume of communications they deliver, the breadth of services they offer, and the number of subscribers they serve. Packet technology, therefore, enables companies to market new devices, including videophones, multimedia terminals, and advanced IP Phones.
- **Flexible new pricing structures:** Companies and service providers with packet-switched networks can transform their service and pricing models. Because network bandwidth can be dynamically allocated, network usage no longer needs to be measured in minutes or distance. Dynamic allocation gives service providers the flexibility to meet the needs of their customers in ways that bring them the greatest benefits.

Call Control

Call control allows users to establish, maintain, and disconnect a voice flow across a network. This topic describes call control services.



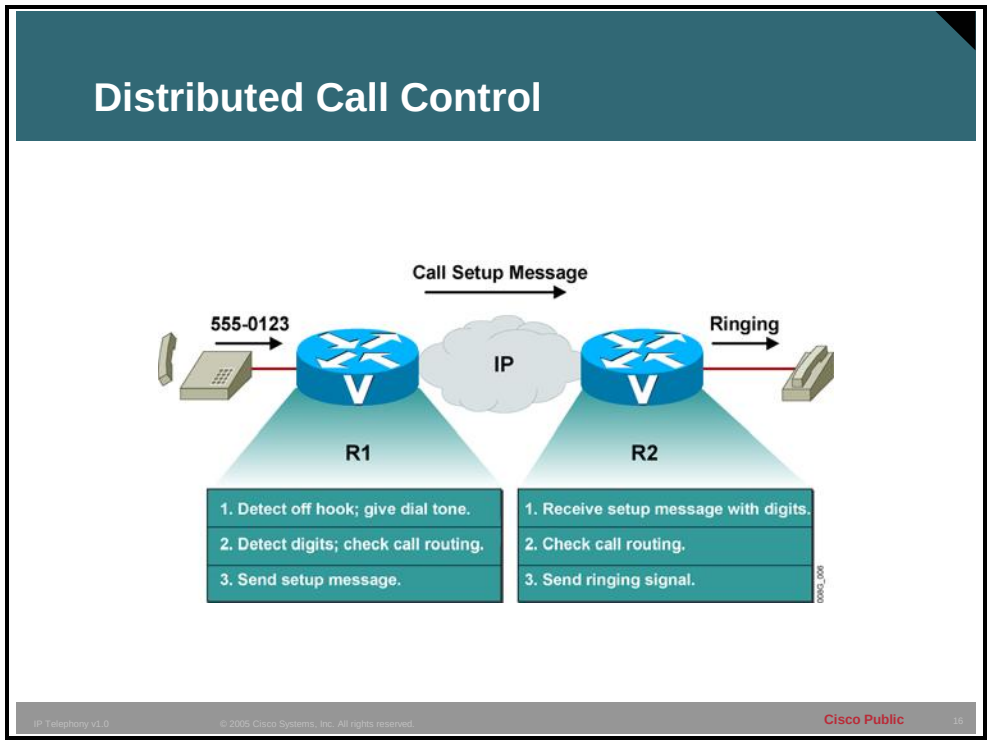
Although different protocols address call control in different ways, they all provide a common set of services. The following are basic components of call control:

- **Call setup:** Checks call-routing configuration to determine the destination of a call. The configuration specifies the bandwidth requirements for the call. When the bandwidth requirements are known, Call Admission Control (CAC) determines if sufficient bandwidth is available to support the call. If bandwidth is available, call setup generates a setup message and sends it to the destination. If bandwidth is not available, call setup notifies the initiator by presenting a busy signal. Different call control protocols, such as H.323, Media Gateway Control Protocol (MGCP), and session initiation protocol (SIP), define different sets of messages to be exchanged during setup.
- **Call maintenance:** Tracks packet count, packet loss, and interarrival jitter or delay when the call is set up. Information passes to the voice-enabled devices to determine if connection quality is good or if it has deteriorated to the point where the call should be dropped.
- **Call teardown:** Notifies voice-enabled devices to free resources and make them available for the next call when either side terminates a call.

 Copyright © 2005, Cisco Systems, Inc.

Distributed vs. Centralized Call Control

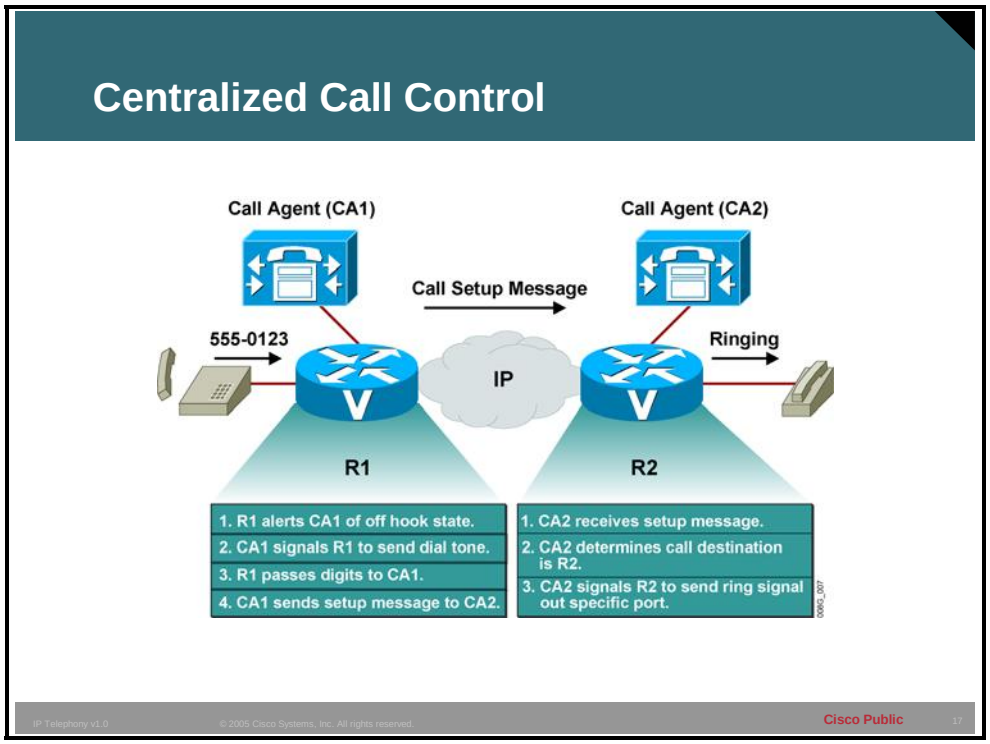
This topic compares distributed and centralized call control.



This figure shows an environment where call control is handled by multiple components in the network. Distributed call control is possible where the voice-capable device is configured to support call control directly. This is the case with a voice gateway when protocols, such as H.323 or SIP, are enabled on the device.

Distributed call control enables the gateway to perform the following procedure:

1. Recognize the request for service
2. Process dialed digits
3. Route the call
4. Supervise the call
5. Terminate the call



Centralized call control allows an external device (call agent) to handle the signaling and call processing, leaving the gateway to translate audio signals into voice packets after call setup. The call agent is responsible for all aspects of signaling, thus instructing the gateways to send specific signals at specific times.

When the call is set up:

- The voice path runs directly between the two gateways and does not involve the call agent.
- When either side terminates the call, the call agent signals the gateways to release resources and wait for another call.

The use of centralized call control devices is beneficial in several ways:

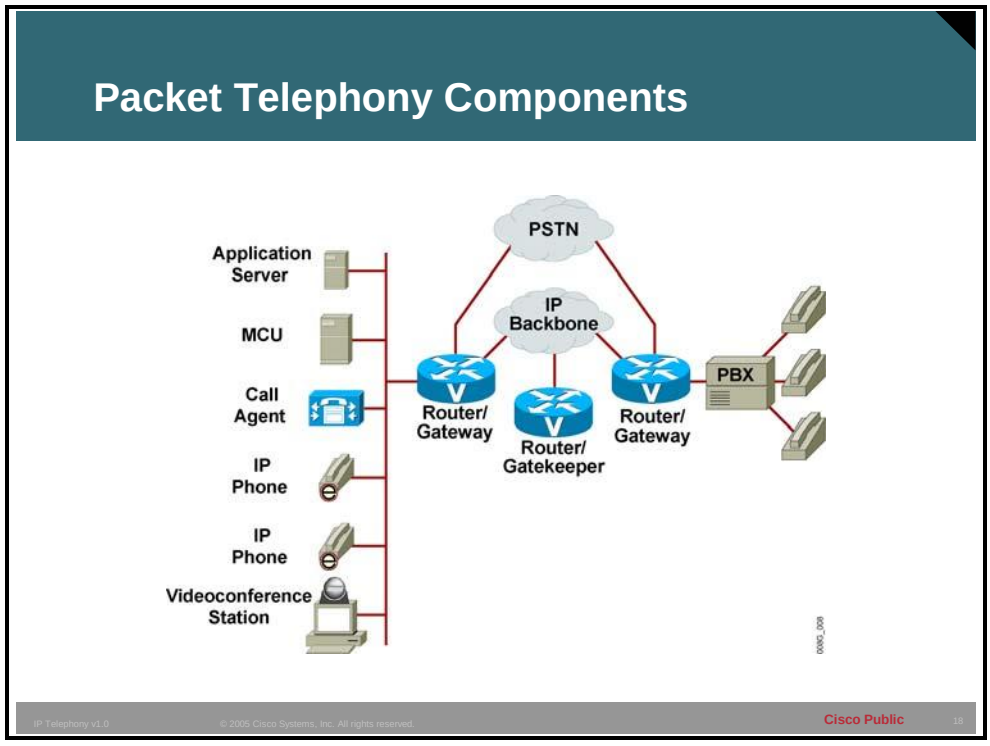
- It centralizes the configuration for call routing and CAC. In a large voice environment, centralization can be extremely beneficial.
- The call agent is the only device that needs the intelligence to understand and participate in call control functions. These call control functions enable the customer to purchase less expensive voice-gateway devices and point to a single device to handle call control.

MGCP is one example of a centralized call control model.

 Copyright © 2005, Cisco Systems, Inc.

Packet Telephony Components

This topic introduces the basic components of a packet voice network.



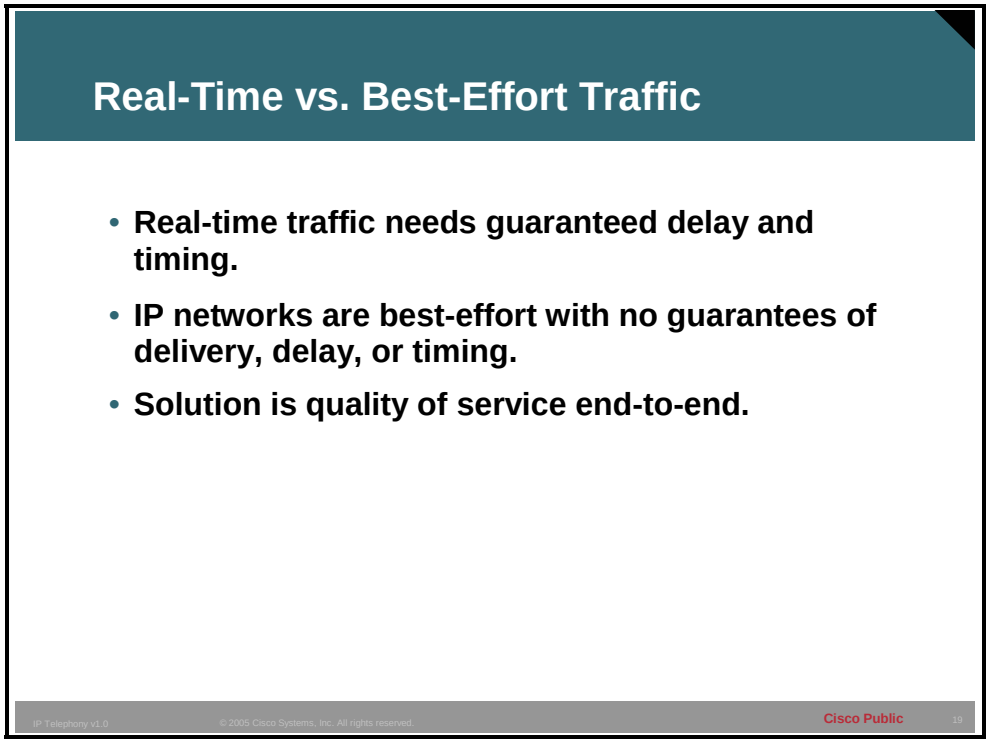
The basic components of a packet voice network include the following:

- **IP Phones:** Provide IP voice to the desktop.
- **Gatekeeper:** Provides CAC, bandwidth control and management, and address translation.
- **Gateway:** Provides translation between VoIP and non-VoIP networks, such as the PSTN. It also provides physical access for local analog and digital voice devices, such as telephones, fax machines, key sets, and PBXs.
- **Multipoint control unit (MCU):** Provides real-time connectivity for participants in multiple locations to attend the same videoconference or meeting.
- **Call agent:** Provides call control for IP Phones, CAC, bandwidth control and management, and address translation.
- **Application servers:** Provide services such as voice mail, unified messaging, and Cisco CallManager Attendant Console.
- **Videoconference station:** Provides access for end-user participation in videoconferencing. The videoconference station contains a video capture device for video input and a microphone for audio input. The user can view video streams and hear the audio that originates at a remote user station.

Other components, such as software voice applications, interactive voice response (IVR) systems, and softphones, provide additional services to meet the needs of enterprise sites.

Best-Effort Delivery of Real-Time Traffic

Voice and data can share the same medium; however, their traffic characteristics differ widely: voice is real-time traffic and data is typically sent as best-effort traffic. This topic compares real-time requirements versus best-effort delivery.



Traditional telephony networks were designed for real-time voice transmission, and therefore cater to the need for a constant voice flow over the connection. Resources are reserved end to end on a per-call basis and are not released until the call is terminated. These resources guarantee that voice flows in an orderly manner. Good voice quality depends on the capacity of the network to deliver voice with guaranteed delay and timing—the requirement for delivery of real-time traffic.

Traditional data networks were designed for best-effort packet transmission. Packet Telephony Networks transmit with no guarantee of delivery, delay, or timing. Data handling is effective in this scenario because upper-layer protocols, such as TCP, provide for reliable—although untimely—packet transmission. TCP trades delay for reliability. Data can typically tolerate a certain amount of delay and is not affected by interpacket jitter.

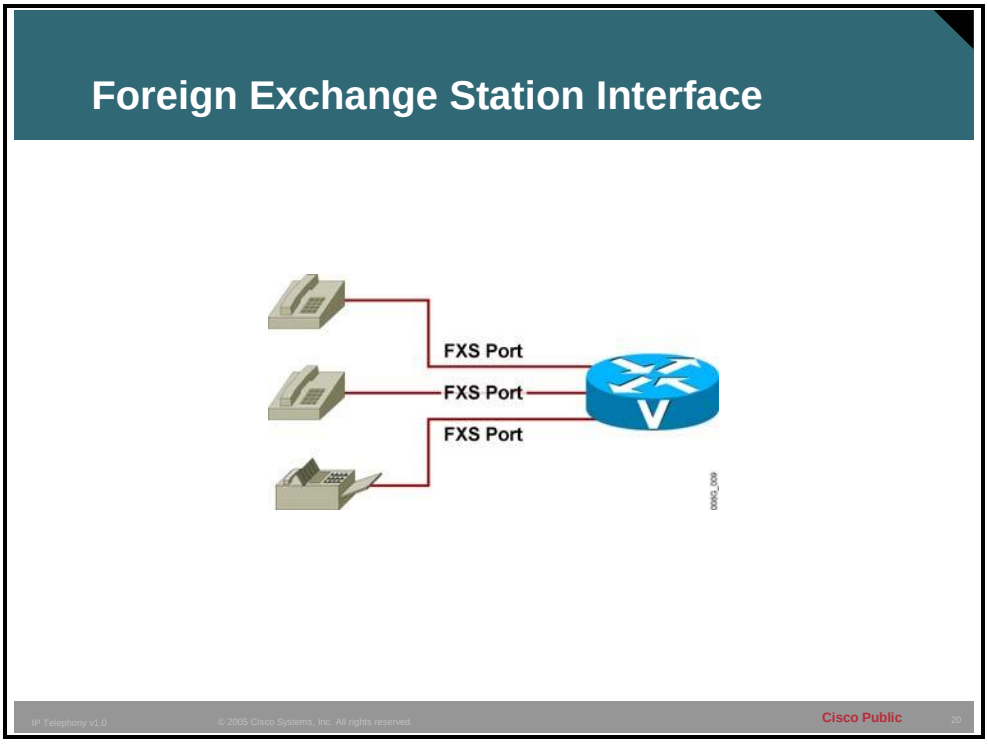
A well-engineered, end-to-end network is required when converging delay-sensitive traffic, such as VoIP, with best-effort data traffic. Fine-tuning the network to adequately support VoIP involves a series of protocols and features to improve quality of service (QoS). Because the IP network is, by default, best-effort, steps must be taken to ensure proper behavior of both the real-time and best-effort traffic. Packet Telephony Networks succeed, in large part, based on the QoS parameters that are implemented networkwide.

 Copyright © 2005, Cisco Systems, Inc.

IP Telephony Applications

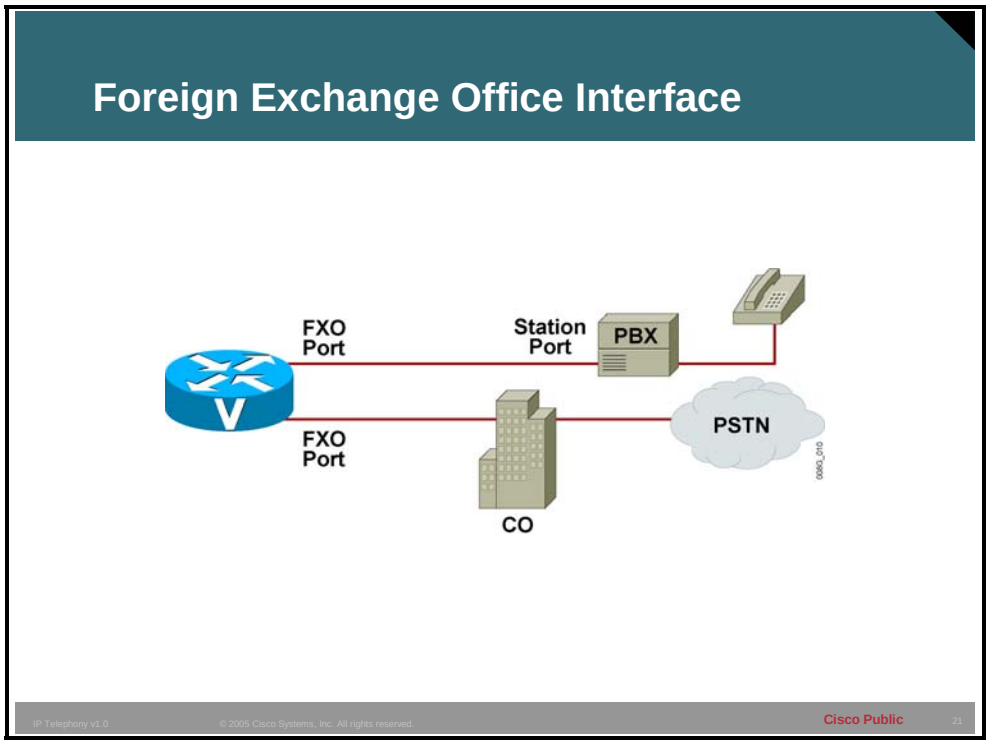
Analog Interfaces

This topic defines three analog interfaces: Foreign Exchange Station (FXS), Foreign Exchange Office (FXO), and ear and mouth (E&M). It also discusses how each of these interfaces is used.



This figure depicts an FXS interface. The FXS interface provides a direct connection to an analog telephone, a fax machine, or a similar device. From a telephone perspective, the FXS interface functions like a switch; therefore, it must supply line power, ring voltage, and dial tone.

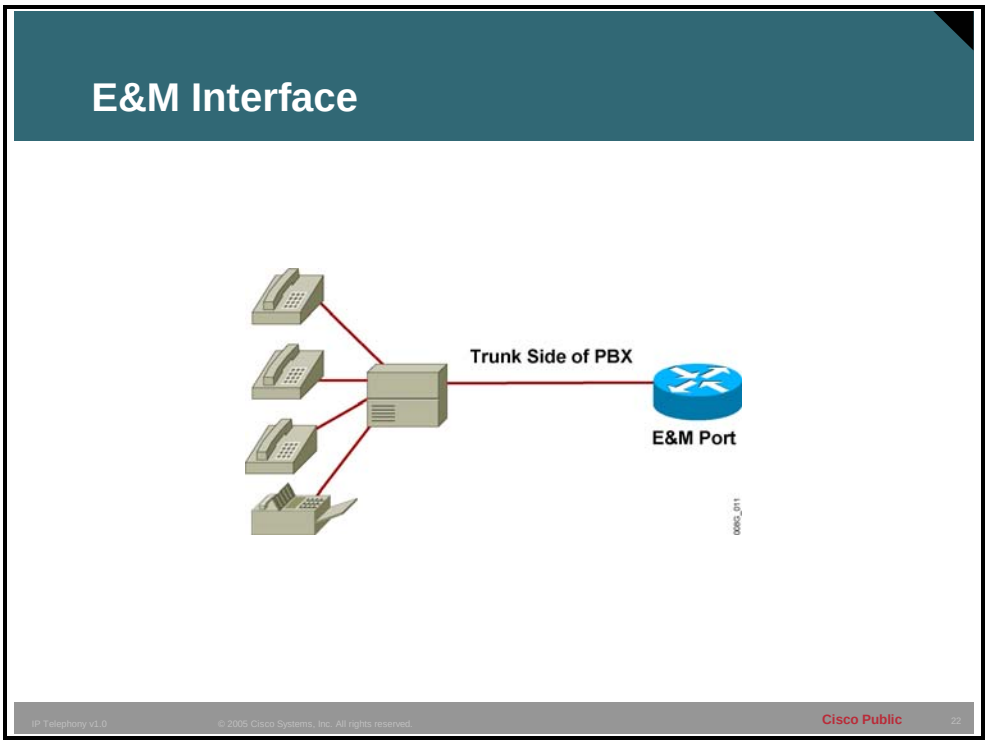
The FXS interface contains the coder-decoder (codec), which converts the spoken analog voice wave into a digital format for processing by the voice-enabled device.



This figure depicts an FXO interface. The FXO interface allows an analog connection to be directed at the CO of a PSTN or to a station interface on a PBX. The switch recognizes the FXO interface as a telephone because the interface plugs directly into the line side of the switch. The FXO interface provides either pulse or DTMF digits for outbound dialing.

In PSTN terminology, an FXO-to-FXS connection is also referred to as a foreign exchange (FX) trunk. An FX trunk is a CO trunk that has access to a distant CO. Because this connection is FXS at one end and FXO at the other end, it acts as a long-distance extension of a local telephone line. In this instance, a local user can pick up the telephone and get a dial tone from a foreign city. Users in the foreign city can dial a local number and have the call connect to the user in the local city.

 Copyright © 2005, Cisco Systems, Inc.

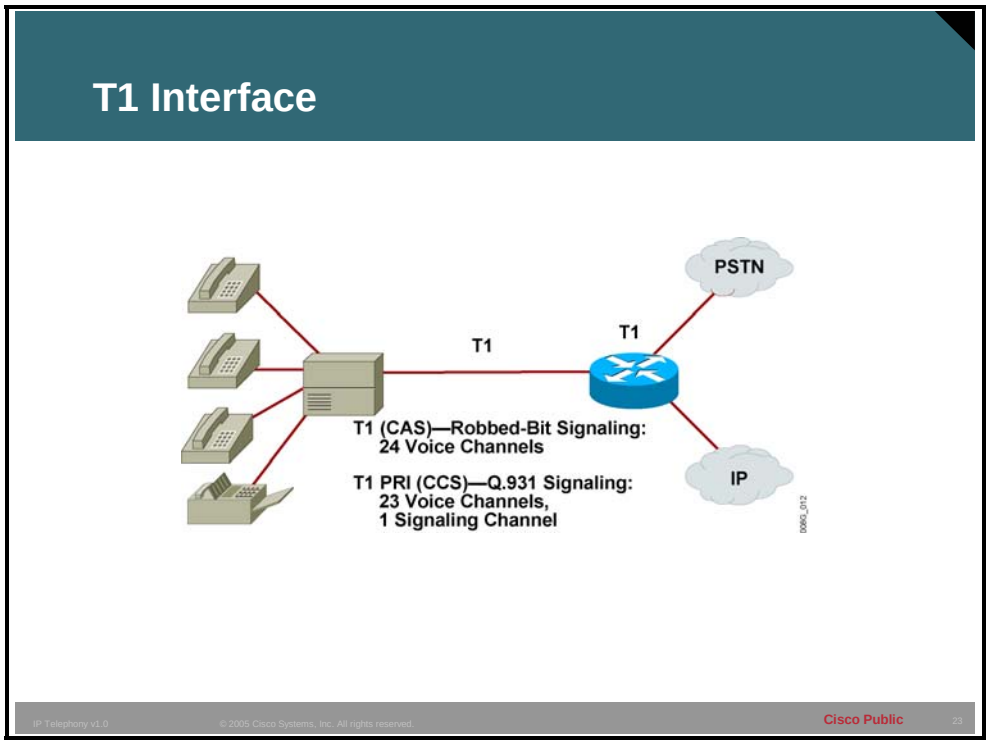


This figure depicts an E&M interface. The E&M interface provides signaling for analog trunking. Analog trunk circuits connect automated systems (PBXs) and networks (COs). E&M signaling is also referred to as “ear and mouth,” but its origin comes from the term “Earth and Magneto.” Earth represents the electrical ground and magneto represents the electromagnet used to generate tone.

E&M signaling defines a trunk-circuit side and a signaling-unit side for each connection, similar to the DCE and DTE reference types. The PBX is usually the trunk-circuit side and the telco, CO, channel bank, or Cisco voice-enabled platform is the signaling-unit side.

Digital Interfaces

This topic describes the three basic digital voice interfaces: T1, E1, and BRI.



This figure depicts a T1 interface. In a corporate environment with a large volume of voice traffic, connections to the PSTN and to PBXs are primarily digital.

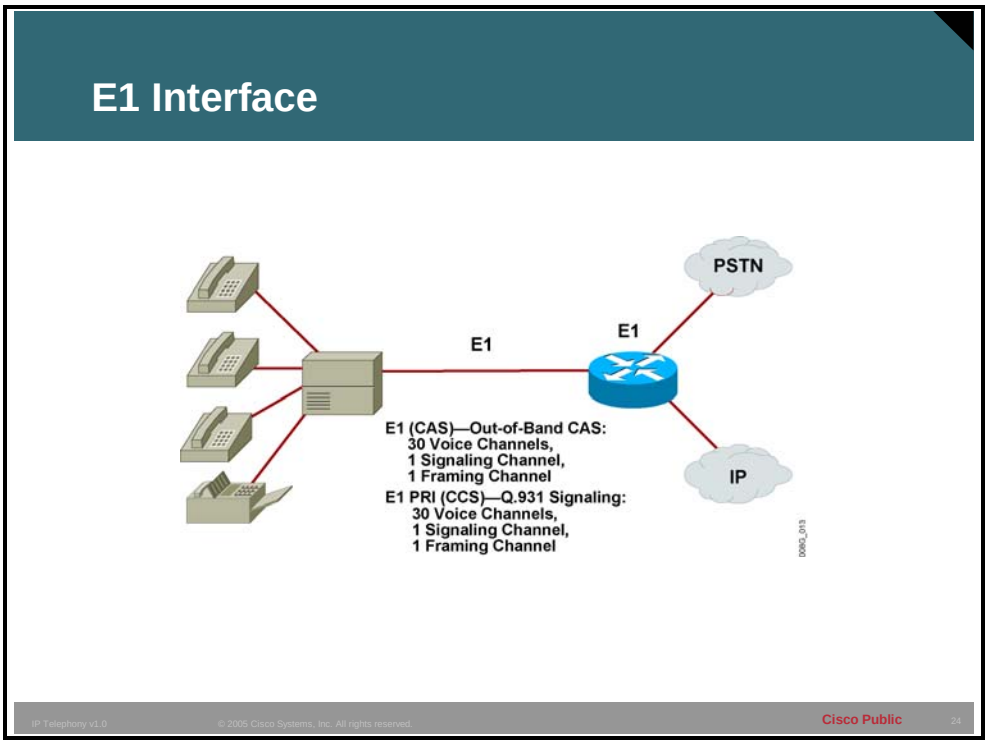
A T1 interface is a form of digital connection that can simultaneously carry up to 24 conversations using two-wire pairs. When a T1 link operates in full-duplex mode, one wire pair sends and the other wire pair receives. The 24 channels are grouped together to form a frame. The frames are then grouped together into Super Frames (groups of 12 frames) or into Extended Superframes (groups of 24 frames).

The T1 interface carries either CAS or CCS. When a T1 interface uses CAS, the signaling robs a sampling bit for each channel to convey in band. When a T1 interface uses CCS, Q.931 signaling is used on a single channel, typically the last channel.

To configure CAS you must:

- Specify the type of signaling that the robbed bits carry; for example, E&M Wink Start. This signaling must match the PSTN requirements or the PBX configuration. This is considered in-band signaling because the signal shares the same channel as the voice.
- Configure the interface for PRI signaling. This level of configuration makes it possible to use channels 1 to 23 (called B channels) for voice traffic. Channel 24 (called the D channel) carries the Q.931 call control signaling for call setup, maintenance, and teardown. This type of signaling is considered out-of-band signaling because the Q.931 messages are sent in the D channel only.

 Copyright © 2005, Cisco Systems, Inc.



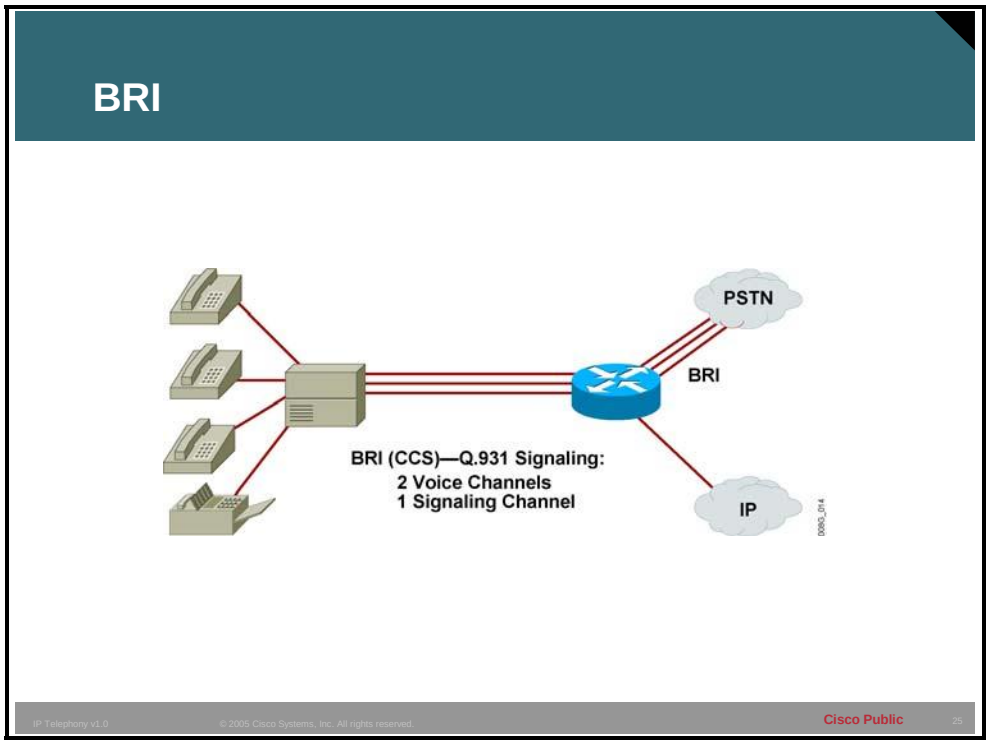
This figure depicts an E1 interface. An E1 interface has 32 channels and simultaneously carries up to 30 conversations. The other two channels are used for framing and signaling. The 32 channels are grouped to form a frame. The frames are then grouped together into multiframes (groups of 16 frames). Europe and Mexico use the E1 interface.

Although you can configure the E1 interface for either CAS or CCS, the most common usage is CCS.

When an E1 interface uses CAS, signaling travels out of band in the signaling channel but follows a strict association between the signal carried in the signaling channel and the channel to which the signaling is being applied. The signaling channel is channel 16.

In the first frame, channel 16 carries 4 bits of signaling for channel 1 and 4 bits of signaling for channel 17. In the second frame, channel 16 carries 4 bits of signaling for channel 2 and 4 bits for channel 18, and so on. This process makes it out-of-band CAS.

When an E1 interface uses CCS, Q.931 signaling is used on a single channel, typically channel 17. When configuring for CCS, configure the interface for PRI signaling. When E1 is configured for CCS, channel 16 carries Q.931 signaling messages only.



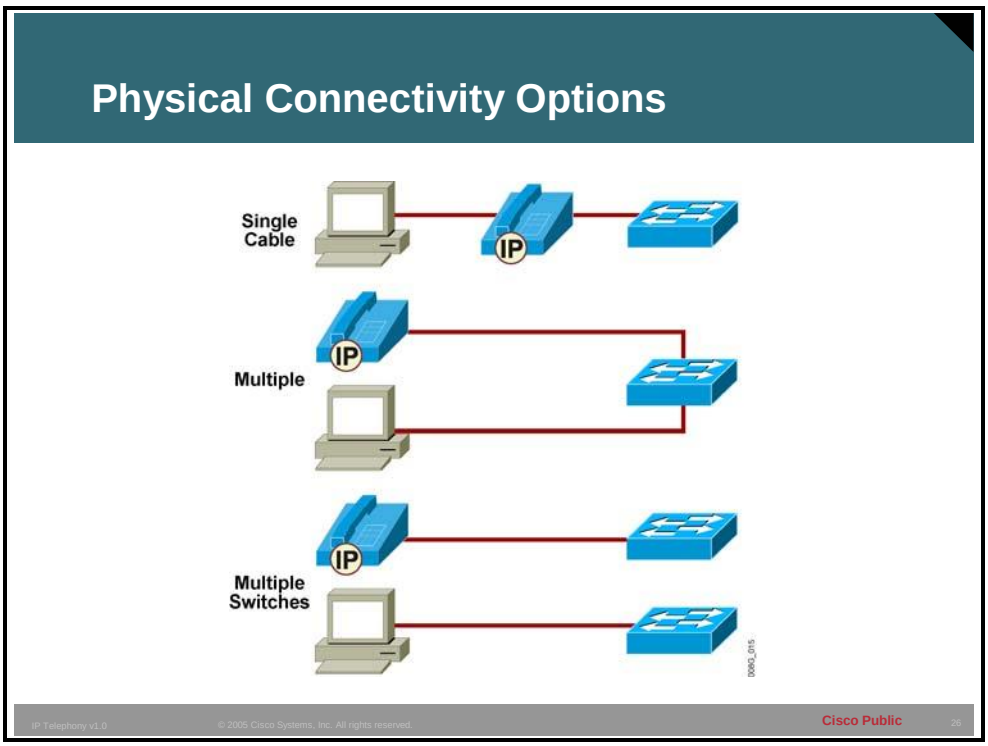
This figure depicts a Basic Rate Interface (BRI). You can use a BRI to connect the PBX voice into the network. Used primarily in Europe for PBX connectivity, BRI provides a 16-kbps D channel for signaling and two 64-kbps B channels for voice. BRI uses Q.931 signaling in the D channel for call signaling.

Note	Cisco Systems does not officially support ISDN telephones.

 Copyright © 2005, Cisco Systems, Inc.

IP Phones

This topic describes scenarios for desktop telephone connections and the IP Phone built-in switch ports.



This figure depicts physical connection options for IP Phones. The IP Phone connects to the network through a Category 5 or better cable that has RJ-45 connectors. The power-enabled switch port or an external power supply provides power to an IP Phone. The IP Phone functions like other IP-capable devices sending IP packets to the IP network. Because these packets are carrying voice, you must consider both logical and physical configuration issues.

At the physical connection level, there are three options for connecting the IP Phone:

- **Single cable:** A single cable connects the telephone and the PC to the switch. Most enterprises install IP Phones on their networks using a single cable for both the telephone and a PC. Reasons for using a single cable include ease of installation and cost savings on cabling infrastructure and wiring-closet switch ports.
- **Multiple cables:** Separate cables connect the telephone and the PC to the switch. Users often connect the IP Phone and PC using separate cables. This connection creates a physical separation between the voice and data networks.
- **Multiple switches:** Separate cables connect the telephone and the PC to separate switches. With this option, IP Phones are connected to separate switches in the wiring closet. By using this approach, you can avoid the cost of upgrading the current data switches and keep the voice and data networks completely separate.

Multiple switches are used to do the following:

- Provide inline power to IP Phones without having to upgrade the data infrastructure
- Limit the number of switches that need an uninterruptible power supply (UPS)
- Reduce the amount of Cisco IOS Catalyst software upgrades needed in the network
- Limit the spanning-tree configuration in the wiring-closet switches

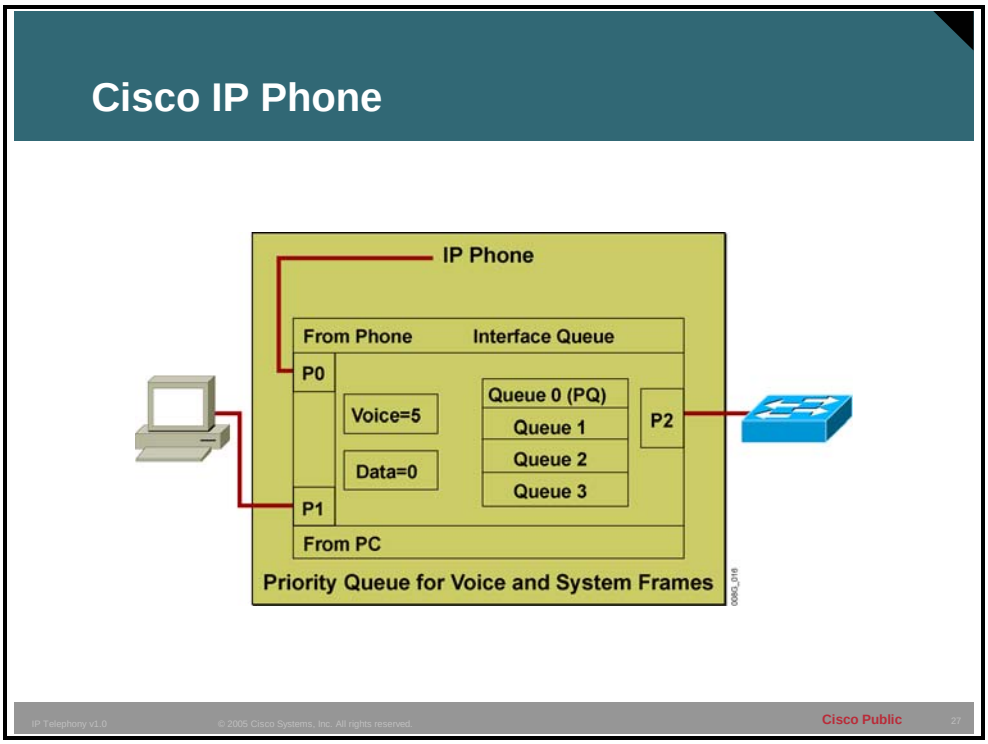
The physical configuration for connecting an IP Phone must address the following issues:

- Speed and duplex settings
- Inline power settings

The logical configuration for connecting an IP Phone must address the following issues:

- IP addressing
- VLAN assignment
- Spanning tree
- Classification and queuing

 Copyright © 2005, Cisco Systems, Inc.



The basic function of a Cisco IP Phone depends on a three-port 10/100 switch. Port P0 is an internal port that connects the voice electronics in the telephone. Port P1 connects a daisy-chained PC. Port P2 uplinks to the Ethernet switch in the wiring closet.

Each port contains four queues with a single threshold. One of these queues is a high-priority queue used for system frames. By default, voice frames are classified for processing in the high-priority queue, and data frames are classified for processing in the low-priority queue.

The internal Ethernet switch on the Cisco IP Phone switches incoming traffic to either the access port or the network port.

If a computer is connected to the port P1, data packets traveling to and from the computer, and to and from the phone, share the same physical link to the access layer switch connected to port P2, and to the same port on the access layer switch. This shared physical link has the following implications for the VLAN network configuration:

- Current VLANs may be configured on an IP subnet basis. However, additional IP addresses may not be available for assigning the telephone to the same subnet as the other devices that are connected to the same port.
- Data traffic that is supporting phones on the VLAN may reduce the quality of VoIP traffic.

You can resolve these issues by isolating the voice traffic on a separate VLAN for each of the ports connected to a telephone. The switch port configured for connecting a telephone would have separate VLANs configured to carry the following types of traffic:

- Voice traffic to and from the IP Phone (auxiliary VLAN)
- Data traffic to and from the PC connected to the switch through the IP Phone access port (native VLAN)

Isolating the telephones on a separate auxiliary VLAN increases voice-traffic quality and allows a large number of telephones to be added to an existing network that has a shortage of IP addresses.

Note	For more information, refer to the documentation included with the Cisco Catalyst switch.

Example: IP Phone Installations

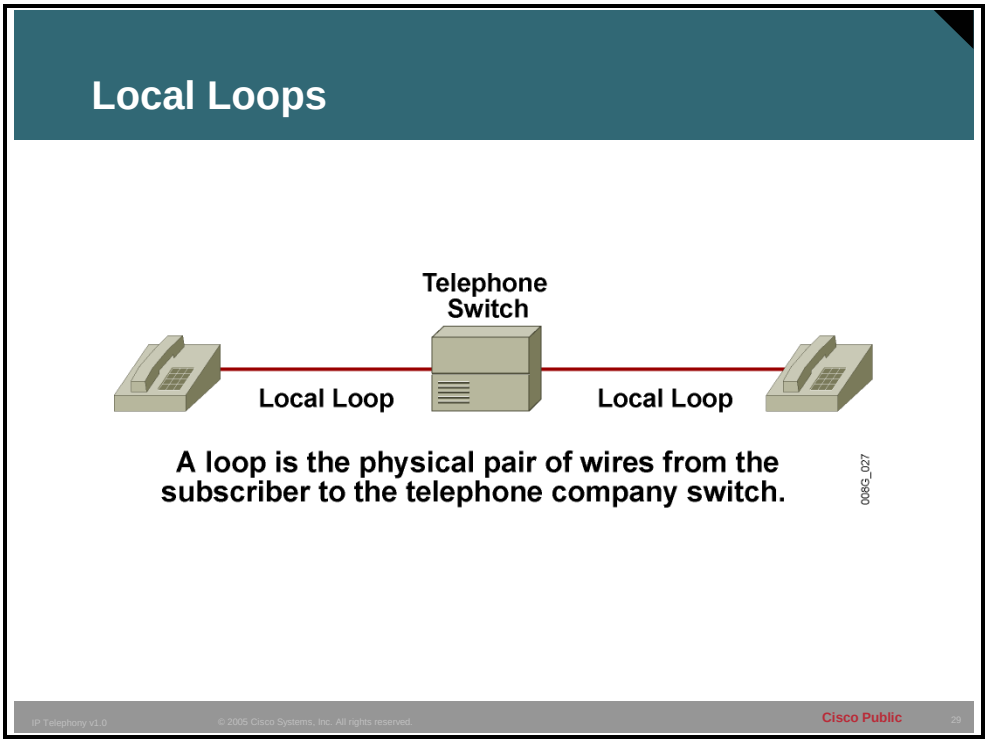
Cisco IP Phones deployed in an office environment attach to Ethernet switches. The IP Phone uses the existing cable infrastructure, or the infrastructure is updated to allow one connection for the phone and one for the desktop PC. The connections from the phone and the PC may lead to the same switch or to different switches. In either case, the IP Phone has the capability to prioritize voice frames.

 Copyright © 2005, Cisco Systems, Inc.

Analog Voice Basics

Local-Loop Connections

This topic describes the parts of a traditional telephony local-loop connection between a telephone subscriber and the telephone company.



A subscriber home telephone connects to the telephone company central office (CO) via an electrical communication path called a local loop, as depicted in the figure. The loop consists of a pair of twisted wires—one is called *tip*, the other is called *ring*.

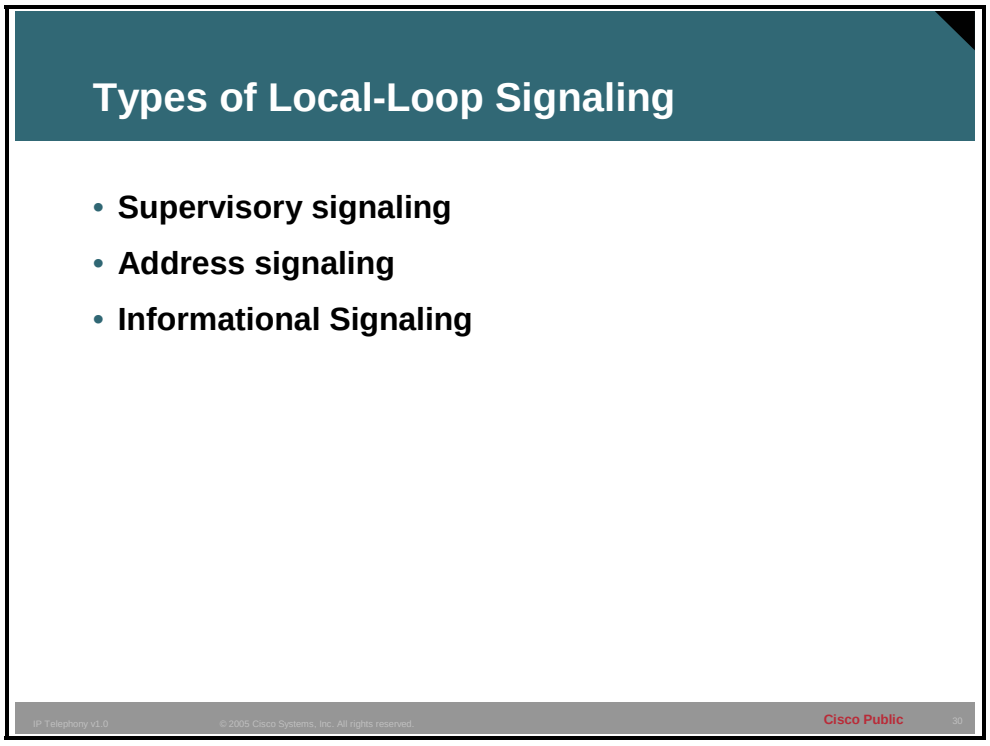
In most arrangements, the ring wire ties to the negative side of a power source, called the *battery*, while the tip wire connects to the ground. When you take your telephone off hook, current flows around the loop, allowing dial tone to reach your handset. Your local loop, along with all others in your neighborhood, connects to the CO in a cable bundle, either buried underground or strung on poles.

Example: Residential Telephone Service

Your home telephone service is provided to you from your service provider by way of two wires. Your home telephone controls whether or not the service on these wires is activated via the switch hook inside the telephone.

Types of Local-Loop Signaling

This topic explains local-loop signaling and lists some of the signaling types.

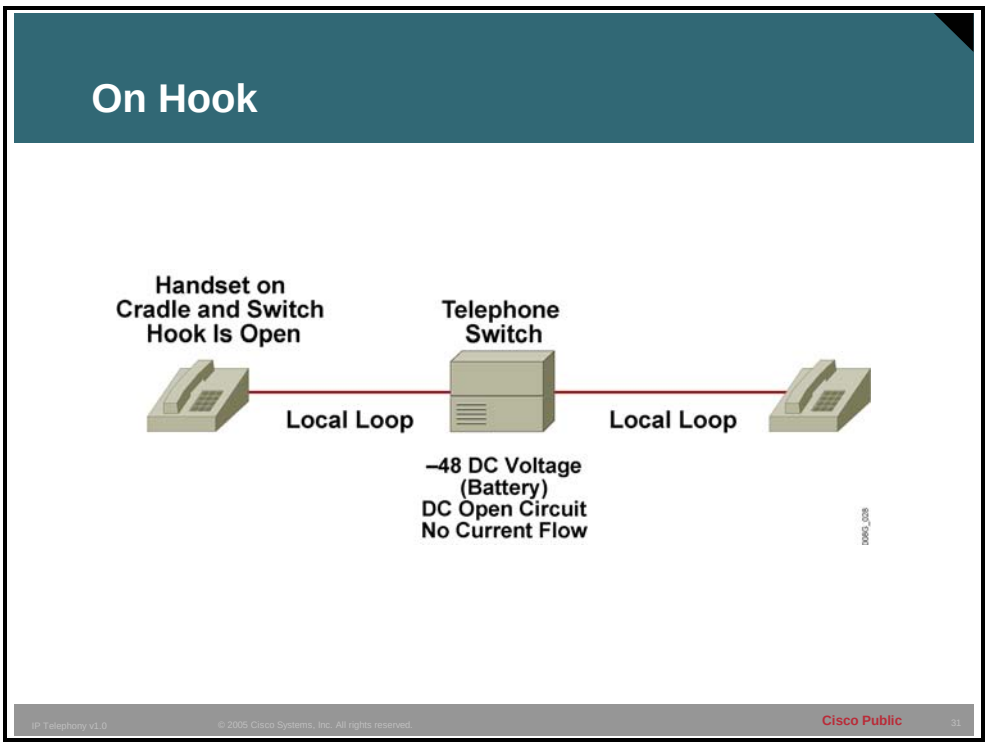


A subscriber and telephone company notify each other of the call status through audible tones and an exchange of electrical current. This exchange of information is called local-loop signaling. Local-loop signaling consists of supervisory signaling, address signaling, and informational signaling, each of which has their own characteristics and purpose. The three types of local-loop signaling appear on the local loop and serve to prompt the subscriber and the switch into a certain action.

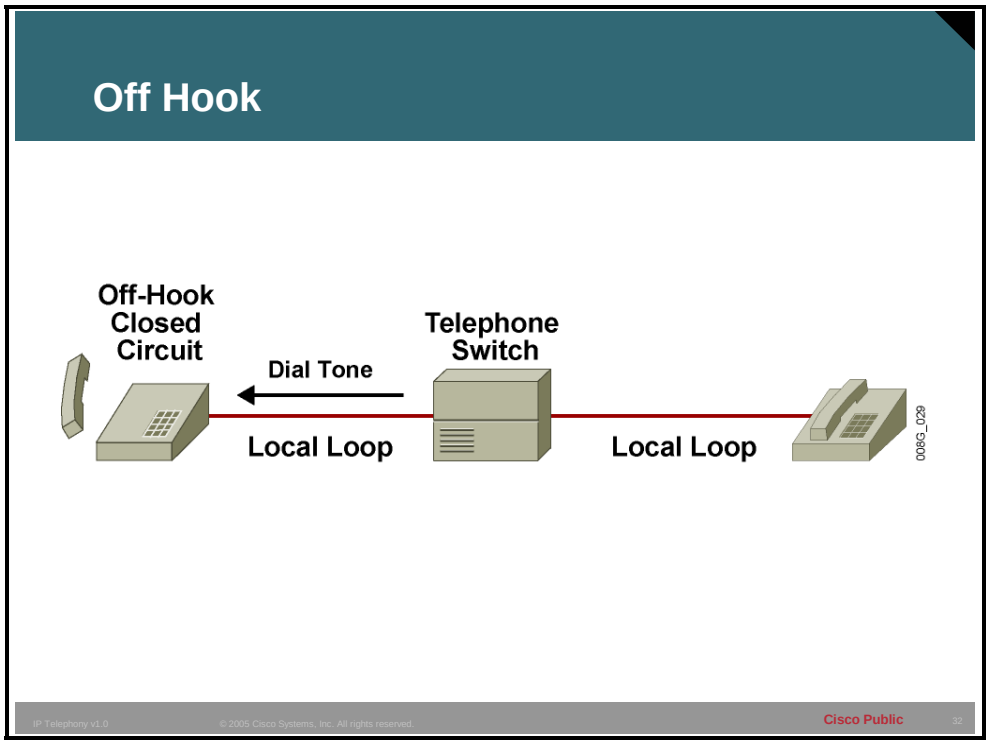
 Copyright © 2005, Cisco Systems, Inc.

Supervisory Signaling

This topic describes on-hook, off-hook, and ringing supervisory signaling. Supervisory signaling serves to initiate the interaction between the subscriber and the attached switch.

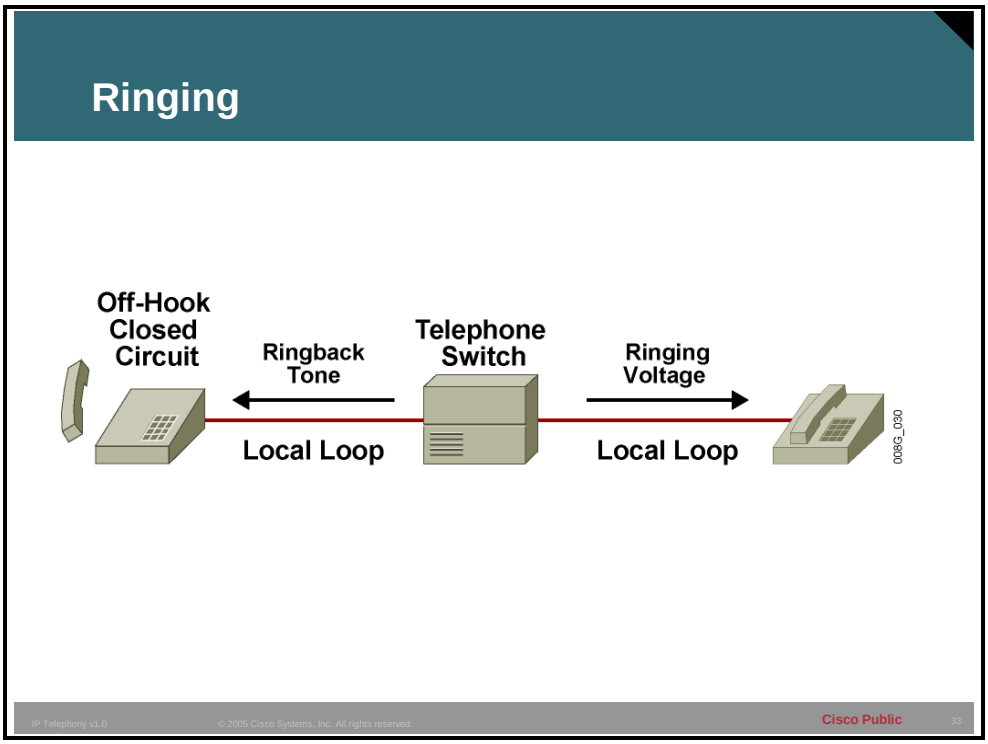


Resting the handset on the telephone cradle opens the switch hook and prevents the circuit current from flowing through the telephone. Regardless of the signaling type, a circuit goes on hook when the handset is placed on the telephone cradle and the switch hook is toggled to an open state. When the telephone is in this position, only the ringer is active.

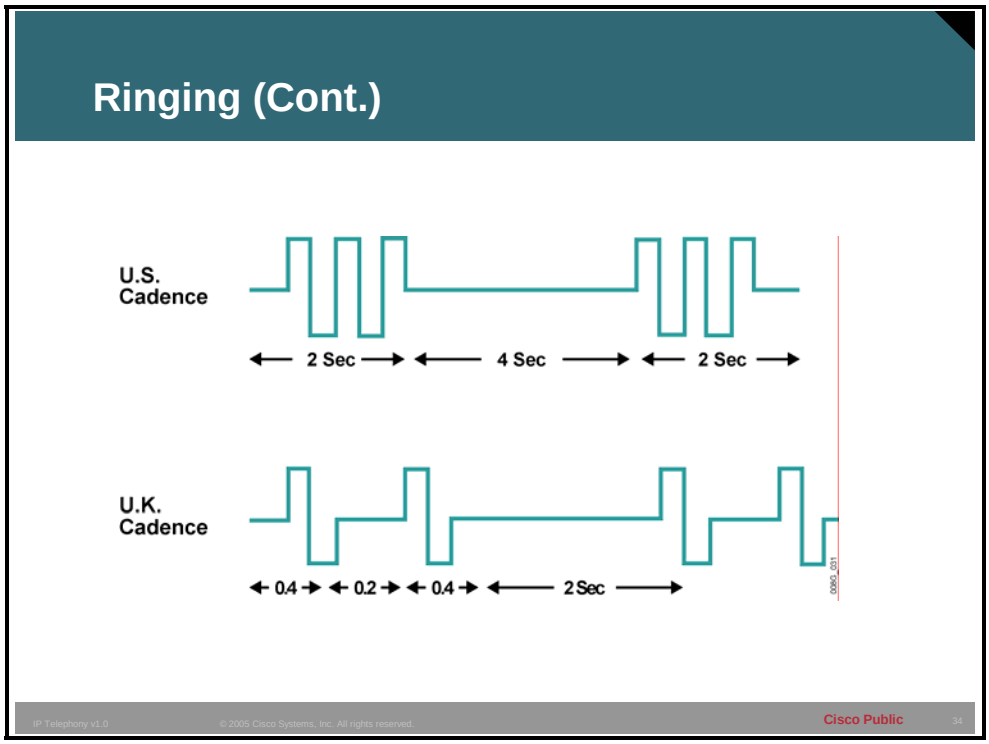


To place a call, a subscriber must lift the handset from the telephone cradle. Removing the handset from the cradle places the circuit off hook. The switch hook is then toggled to a closed state, causing circuit current to flow through the electrical loop. The current notifies the telephone company that someone is requesting to place a telephone call. When the telephone network senses the off-hook connection by the flow of current, it provides a signal in the form of the dial tone to indicate that it is ready.

 Copyright © 2005, Cisco Systems, Inc.



When a subscriber makes a call, the telephone sends voltage to the ringer to notify the other subscriber of an inbound call. The telephone company also sends a ringback tone to the caller, alerting the caller that it is sending ringing voltage to the recipient telephone. Although ringback tone is not the same as ringing voltage, it sounds similar.



As depicted in the figure, the ringing supervisory tone in the United States is 2 seconds of tone followed by 4 seconds of silence. The United Kingdom uses a double ring of 0.4 seconds separated by 0.2 seconds of silence, followed by 2 seconds of silence.

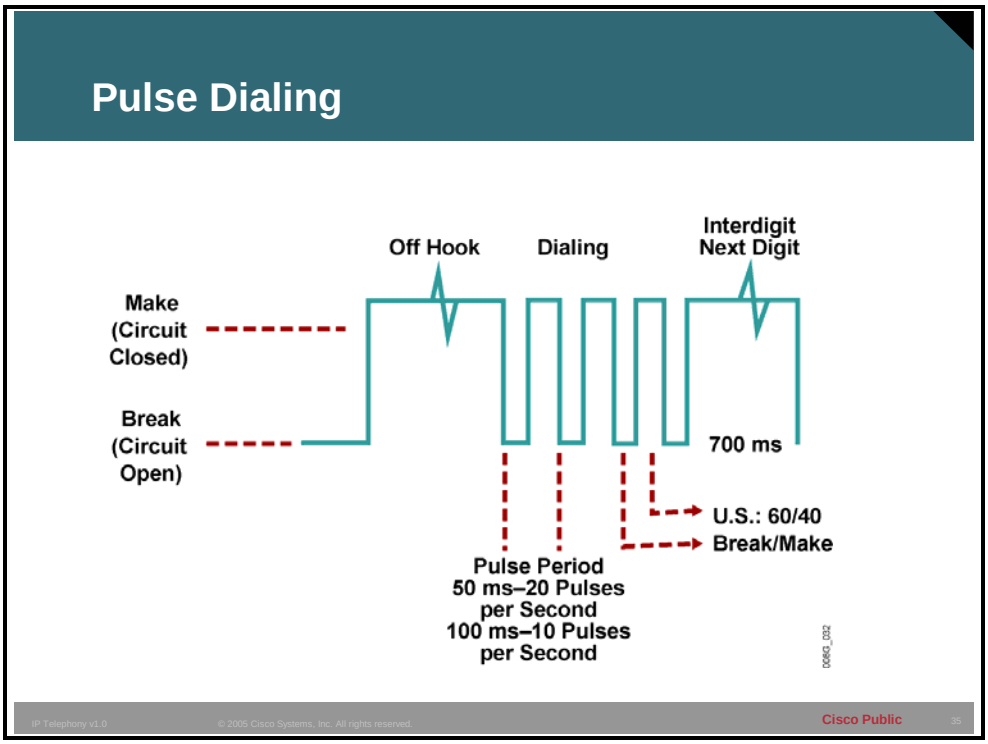
Example: Ringing Cadences

The pattern of the ring signal, or ring cadence, varies around the world. In the United States, the ring signal, sent by the local service provider, is 2 seconds of ring followed by 4 seconds of silence. Your home telephone rings with this cadence when you have an incoming call.

 Copyright © 2005, Cisco Systems, Inc.

Address Signaling

This topic describes pulse dialing and dual-tone multifrequency (DTMF) signaling.

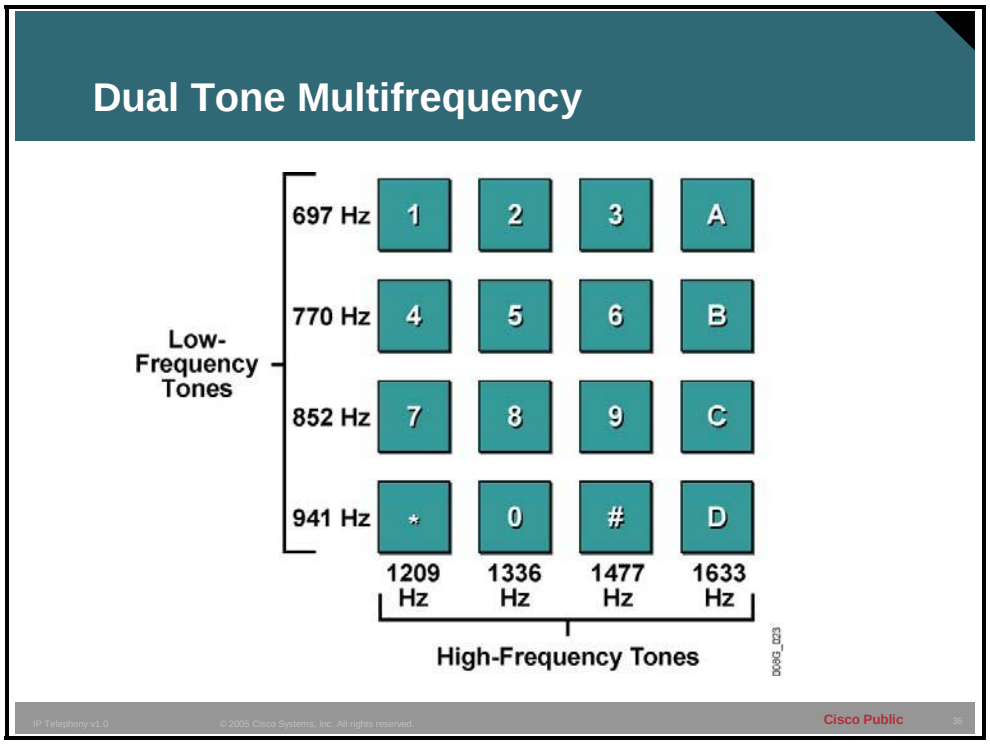


Although somewhat outdated, rotary-dial telephones are still in use and easily recognized by their large numeric dial-wheel. When placing a call, the subscriber spins the large numeric dial-wheel to send digits. These digits must be produced at a specific rate and within a certain level of tolerance. Each pulse consists of a “break” and a “make.” The break segment is the time that the circuit is open. The make segment is the time during which the circuit is closed. In the United States, the break-and-make cycle must correspond to a ratio of 60 percent break to 40 percent make.

A governor inside the dial controls the rate at which the digits are pulsed.

The dial pulse signaling process occurs as follows:

1. When a subscriber calls someone by dialing a digit on the rotary dial, a spring winds.
2. When the dial is released, the spring rotates the dial back to its original position.
3. While the spring rotates the dial back to its original position, a cam-driven switch opens and closes the connection to the telephone company. The number of consecutive opens and closes—or breaks and makes—represents the dialed digit.



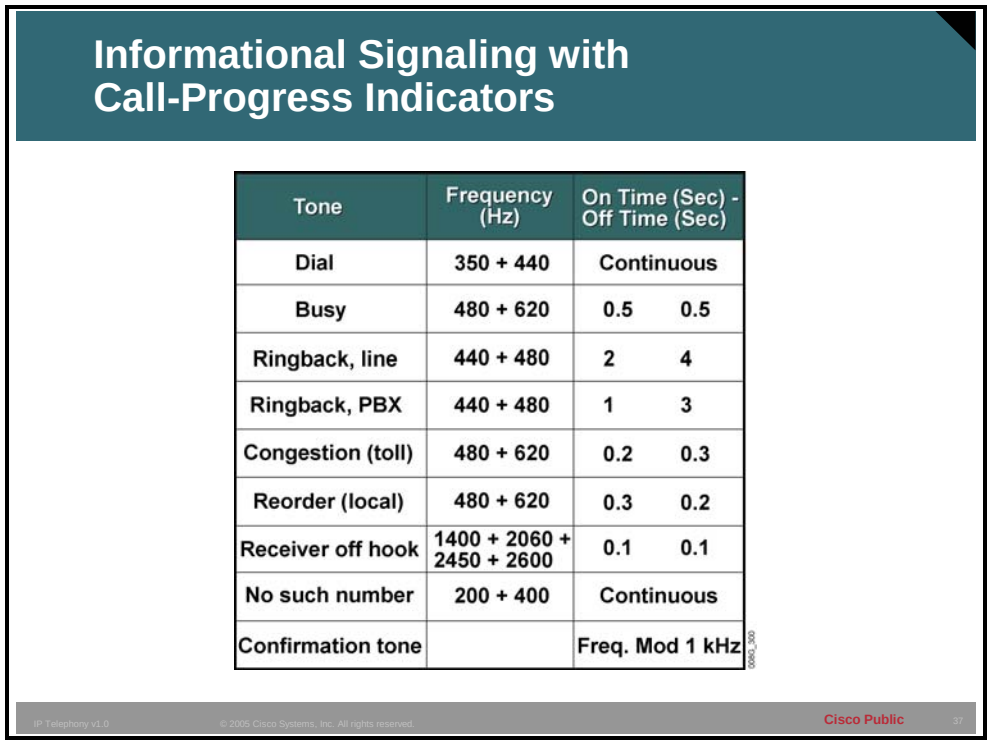
Users who have a touch-tone pad or a push-button telephone must push the keypad buttons to place a call. Each button on the keypad is associated with a set of high and low frequencies. Each row of keys on the keypad is identified by a low-frequency tone; each column of keys on the keypad is identified by a high-frequency tone. The combination of both tones notifies the telephone company of the number being called, hence the term dual tone multifrequency (DTMF).

The figure illustrates the combination of tones generated for each button on the keypad.

 Copyright © 2005, Cisco Systems, Inc.

Informational Signaling

This topic lists the call-progress indicators and describes their functions.

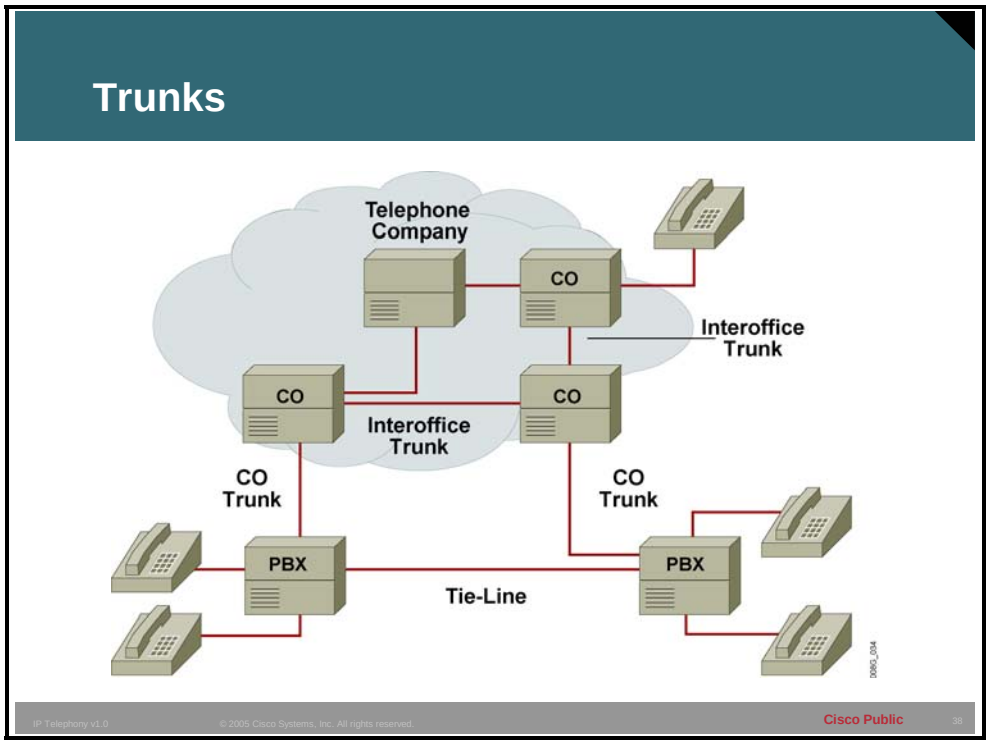


Call-progress indicators in the form of tone combinations are used to notify subscribers of call status. Each combination of tones represents a different event in the call process, as follows:

- **Dial tone:** Indicates that the telephone company is ready to receive digits from the user telephone. The Cisco routers provide dial tone as a method of showing that the hardware is installed. In a PBX or key telephone system, the dial tone indicates that the system is ready to receive digits.
- **Busy tone:** Indicates that a call cannot be completed because the telephone at the remote end is already in use.
- **Ringback (normal or PBX):** Indicates that the telephone company is attempting to complete a call on behalf of a subscriber.
- **Congestion:** Indicates that congestion in the long-distance telephone network is preventing a telephone call from being processed. The congestion tone is sometimes known as the all-circuits-busy tone.
- **Reorder tone:** Indicates that all of the local telephone circuits are busy, thus preventing a telephone call from being processed. The reorder tone is known to the user as fast-busy, and is familiar to anyone who operates a telephone from a PBX.
- **Receiver off hook:** Indicates that the receiver has been off hook for an extended period without placing a call.
- **No such number:** Indicates that a subscriber placed a call to a nonexistent number.
- **Confirmation tone:** Indicates that the telephone company is working on completing the call.

Trunk Connections

This topic describes the different types of trunks on a voice network and how they operate.



Before a telephone call terminates at its final destination, it is routed through multiple switches. When a switch receives a call, it determines whether the destination telephone number is within a local switch or if the call needs to go through another switch to a remote destination. Trunks connect the telephone company and PBX switches.

The primary function of the trunk is to provide the path between switches. The switch must route the call to the correct trunk or telephone line. Although many different subscribers share a trunk, only one subscriber uses it at any given time. As telephone calls end, they release trunks and make them available to the switch for subsequent calls. There can be several trunks between two switches.

The following are examples of the more common trunk types:

- **Private trunk lines:** Companies with multiple PBXs often connect them with tie trunk lines. Generally, tie trunk lines serve as dedicated circuits that connect PBXs. On a monthly basis, subscribers lease trunks from the telephone company to avoid the expense of using telephone lines on a per-call basis. These types of connections, known as tie-lines, typically use special interfaces called recEive and transMit, or ear and mouth (E&M), interfaces.
- **CO trunks:** A CO trunk is a direct connection between a PBX and the local CO that routes calls; for example, the connection from a private office network to the public switched telephone network (PSTN). When users dial **9**, they are connecting through their PBX to the CO trunk to access the PSTN. CO trunks typically use Foreign Exchange Office (FXO) interfaces. Certain specialized CO trunks are frequently used on the telephony network. A direct inward dialing (DID) trunk, for example, allows outside callers to reach specific internal destinations without having to be connected via an operator.

 Copyright © 2005, Cisco Systems, Inc.

- **Interoffice trunks:** An interoffice trunk is a circuit that connects two local telephone company COs.



Foreign exchange (FX) trunks are interfaces that are connected to switches that support connection to either office equipment or station equipment. Office equipment includes other switches (to extend the connection) and Cisco devices. Station equipment includes telephones, fax machines, and modems.

- **Foreign Exchange Office (FXO) interfaces:** An FXO interface connects a PBX to another switch or Cisco device. The purpose of an FXO interface is to extend the telephony connection to a remote site; for example, if a user on a corporate PBX wanted a telephone installed at home instead of in the local office where the PBX is located, an FXO interface would be used. The FXO interface would connect to a Cisco voice router, which would serve to extend the connection to the user home. This connection is an Off-Premises eXtension (OPX).
- **Foreign Exchange Station (FXS) interfaces:** An FXS interface connects station equipment: telephones, fax machines, and modems. A telephone connected directly to a switch or Cisco device requires an FXS interface. Because a home telephone connects directly to the telephone company CO switch, an FXS interface is used.

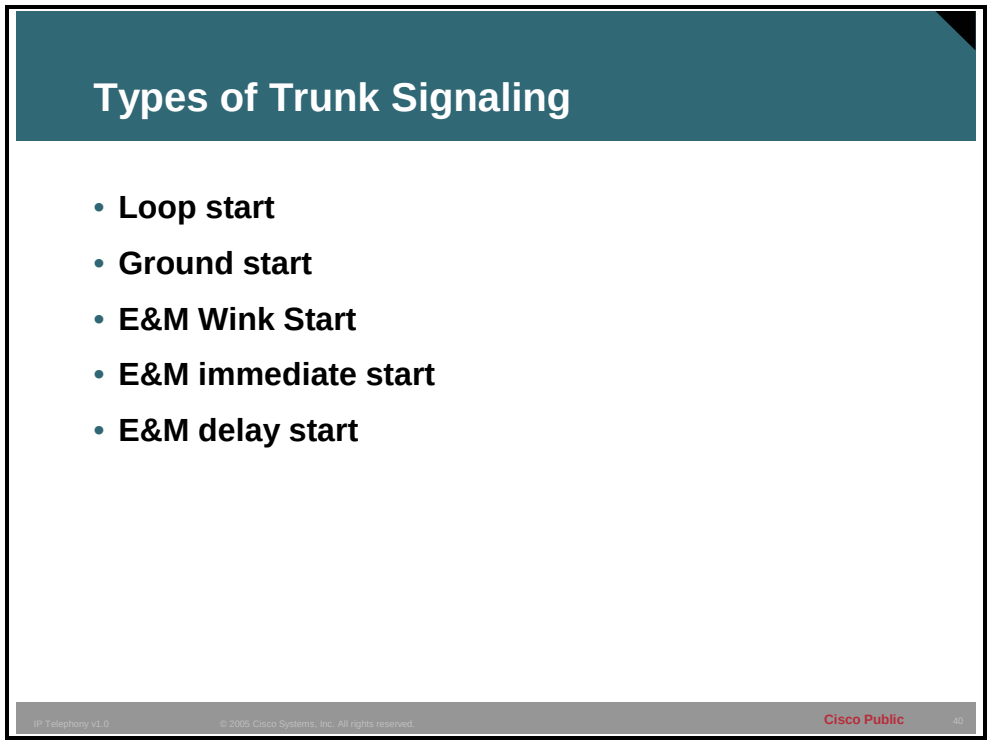
Example: Foreign Exchange Interfaces

The service provided by local telephone companies for residential phones uses a foreign exchange interface—specifically FXS. This service is provided on two wires. The service is considered a station-side connection because the interface terminates with a telephone.

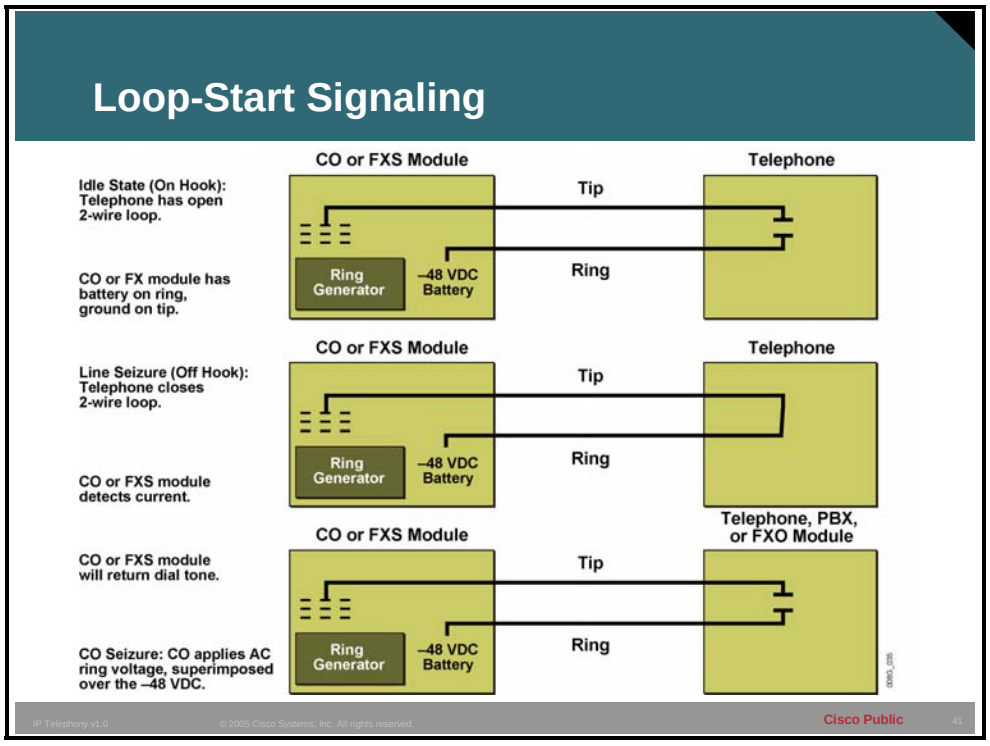
 Copyright © 2005, Cisco Systems, Inc.

Types of Trunk Signaling

This topic describes the trunk and line-seizure signaling types.



There must be signaling standards between the lines and trunks of a telephone network, just as there are signaling standards between a telephone and the telephone company. Trunk signaling serves to initiate the connection between the switch and the network. There are five different types of trunk signaling and each applies to different kinds of interfaces, such as FXS, FXO, and E&M.



Loop-start signaling allows a user or the telephone company to seize a line or trunk when a subscriber is initiating a call. It is primarily used on local loops rather than on trunks.

A telephone connection exists in one of the following states:

- Idle (on hook)
- Telephone seizure (off hook)
- CO seizure (ringing)

A summary of the loop-start signaling process is as follows:

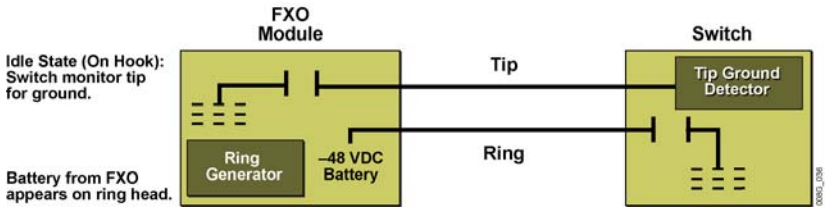
1. When the line is in the idle state, or on hook, the telephone or PBX opens the two-wire loop. The CO or FXS has battery on ring and ground on tip.
2. If a user lifts the handset off the cradle to place a call, the switch hook goes off hook and closes the loop (line seizure). The current can now flow through the telephone circuit. The CO or FXS module detects the current and returns a dial tone.
3. When the CO or FXS module detects an incoming call, it applies AC ring voltage superimposed over the –48 VDC battery, causing the ring generator to notify the recipient of a telephone call. When the telephone or PBX answers the call, thus closing the loop, the CO or FXS module removes the ring voltage.

Loop-start signaling is a poor solution for high-volume trunks because it leads to glare incidents, or the simultaneous seizure of the trunk from both ends. Glare occurs, for example, when you pick up your home telephone and find that someone is already at the other end.

Glare is not a significant problem at home. It is, however, a major problem when it occurs between switches at high-volume switching centers, such as long-distance carriers.

 Copyright © 2005, Cisco Systems, Inc.

Ground-Start Signaling



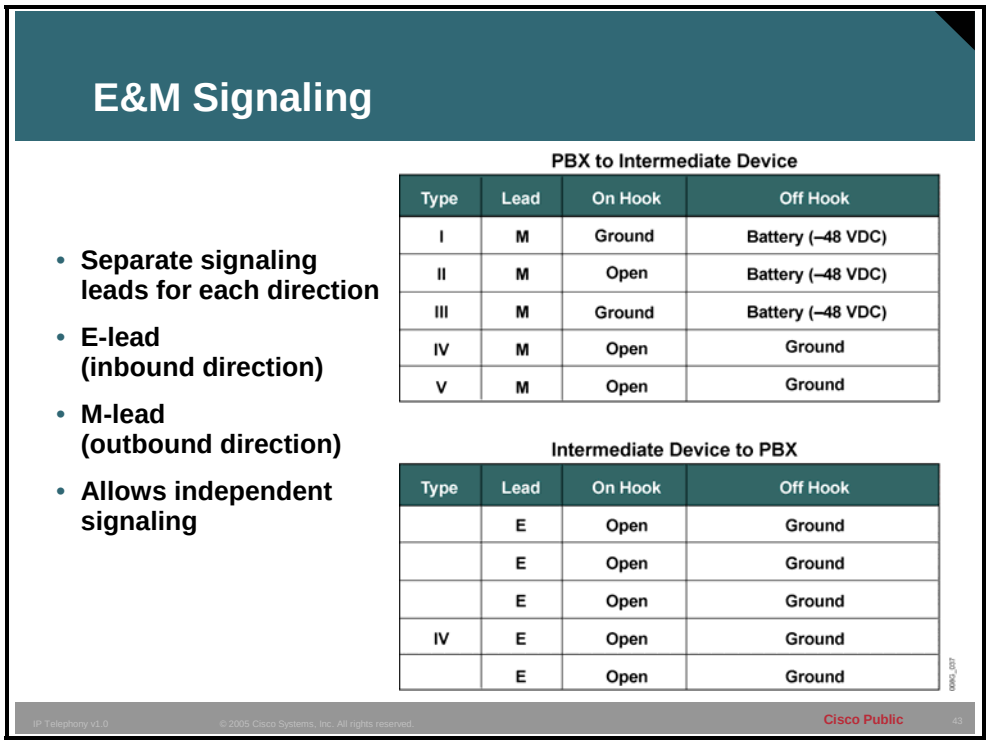
IP Telephony v1.0 © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 42

Ground-start signaling is a modification of loop-start signaling that corrects for the probability of glare. It solves the problem by providing current detection at both ends.

Although loop-start signaling works when you use your telephone at home, ground-start signaling is preferable when there are high-volume trunks involved at telephone switching centers. Because ground-start signaling uses a request or confirm switch at both ends of the interface, it is preferable over other signaling methods on high-usage trunks, such as FXOs.

FXOs require implementation of answer supervision (reversal or absence of current) on the interface for the confirmation of on hook or off hook.

Ground-start signaling is not common in Voice over IP (VoIP) networks.



E&M signaling supports tie-line type facilities or signals between voice switches. Instead of superimposing both voice and signaling on the same wire, E&M uses separate paths, or leads, for each.

Example: E&M Signaling

To call a remote office, your PBX must route a request for use of the trunk over its signal leads between the two sites. Your PBX makes the request by activating its M-lead. The other PBX detects the request when it detects current flowing on its E-lead. It then attaches a dial register to the trunk and your PBX, which sends the dialed digits. The remote PBX activates its M-lead to notify the local PBX that the call has been answered.

Types of E&M Signaling

There are five types of E&M signaling: Type I, Type II, Type III, Type IV, and Type V. The E&M leads operate differently with each wiring scheme, as shown in the table.

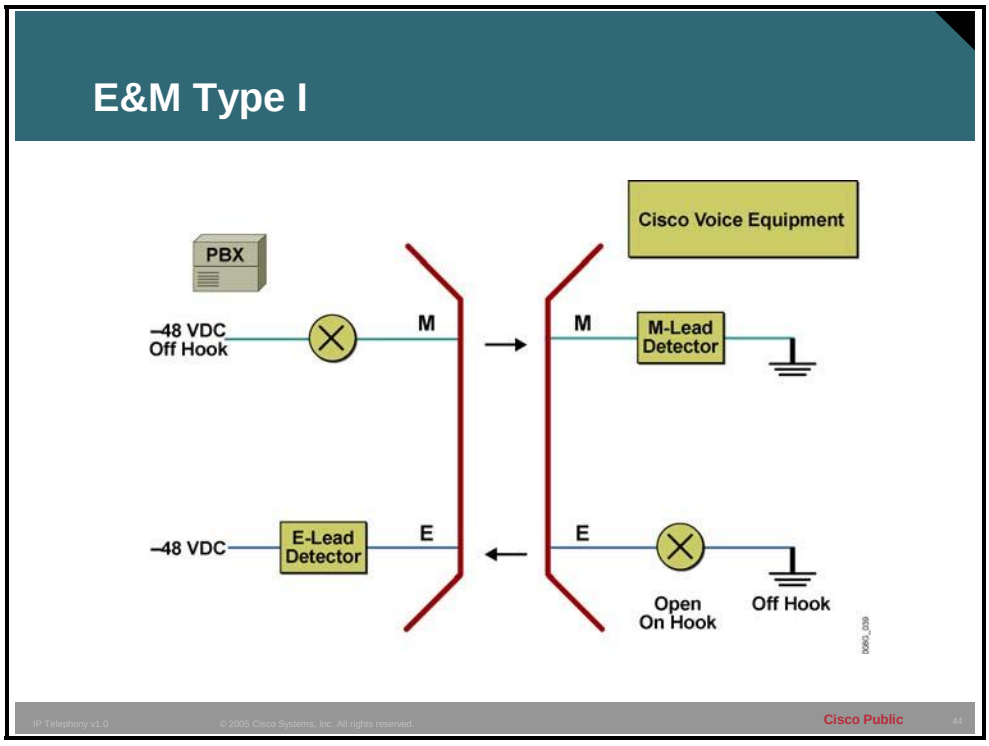
 Copyright © 2005, Cisco Systems, Inc.

Types of E&M Signaling

E&M Signaling Type	PBX to Intermediate Device			Intermediate Device to PBX		
	Lead	On Hook	Off Hook	Lead	On Hook	Off Hook
Type I	M	Ground	Battery (–48 VDC)	E	Open	Ground
Type II	M	Open	Battery (–48 VDC)	E	Open	Ground
Type III	M	Ground	Battery (–48 VDC)	E	Open	Ground
Type IV	M	Open	Ground	E	Open	Ground
Type V	M	Open	Ground	E	Open	Ground

E&M Signaling Types

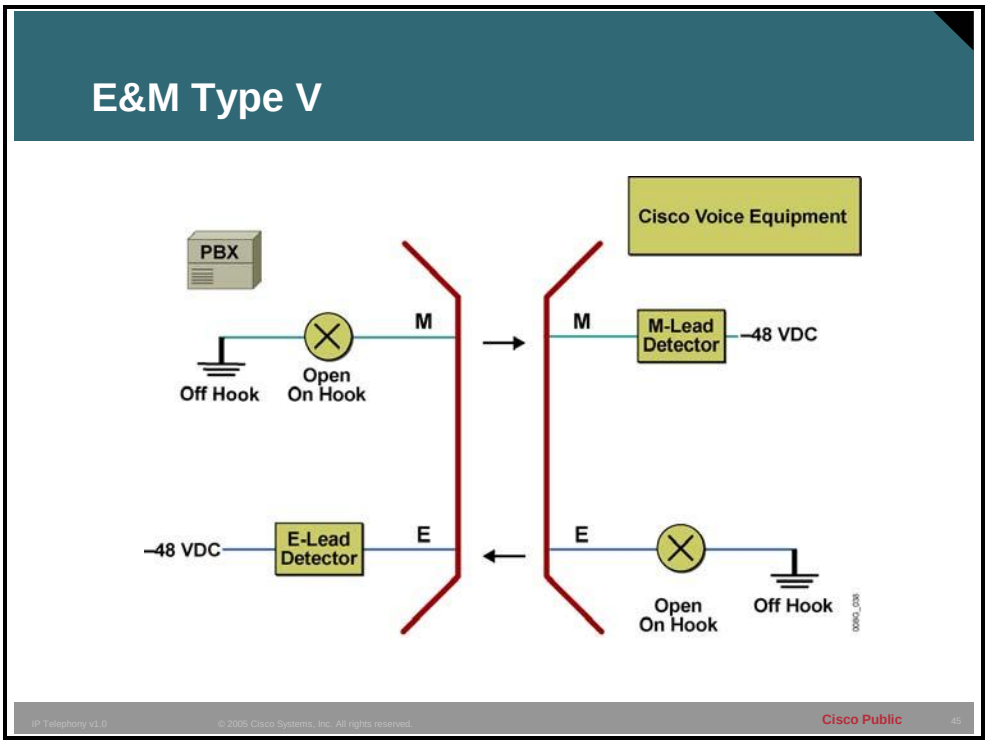
This topic identifies the five E&M signaling types and provides a description of each.



Four-wire E&M Type I signaling is actually a six-wire E&M signaling interface common in North America. One wire is the E-lead; the second wire is the M-lead, and the remaining two pairs of wires serve as the audio path. In this arrangement, the PBX supplies power, or *battery*, for both the M-leads and E-leads. This arrangement also requires that a common ground be connected between the PBX and the Cisco voice equipment.

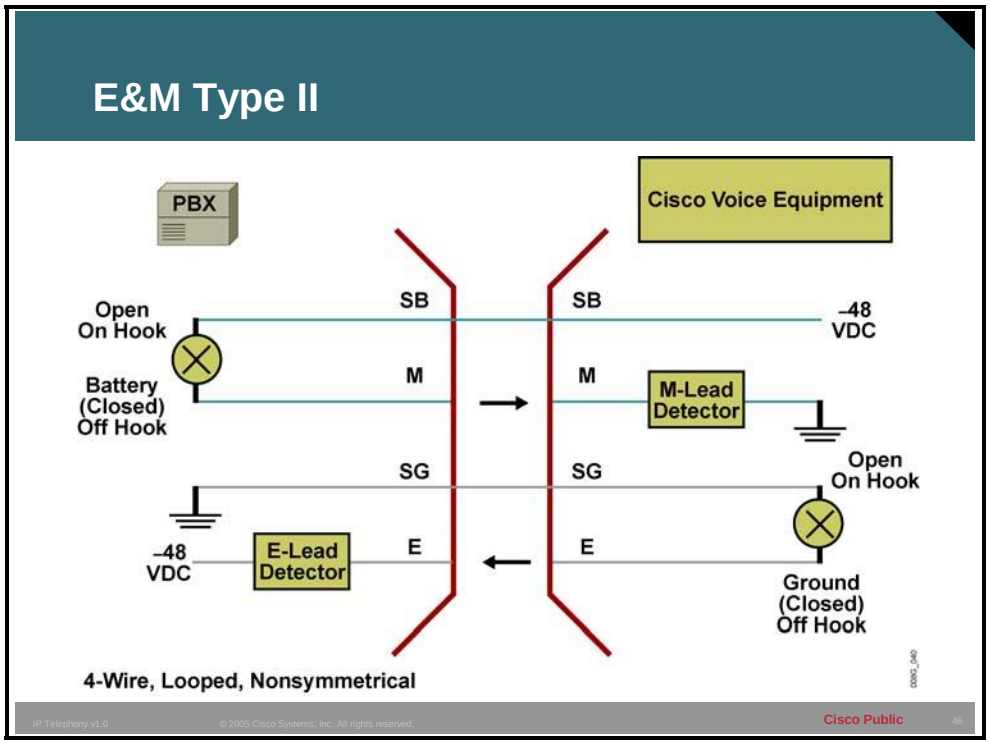
With the Type I interface, the Cisco voice equipment (tie-line equipment) generates the E signal to the PBX by grounding the E-lead. The PBX detects the E signal by sensing the increase in current through a resistive load. Similarly, the PBX generates the M signal by sourcing a current to the Cisco voice equipment (tie-line equipment), which detects it via a resistive load.

 Copyright © 2005, Cisco Systems, Inc.



Type V is another six-wire E&M signaling type and the most common E&M signaling form outside of North America. In Type V, one wire is the E-lead and the other wire is the M-lead.

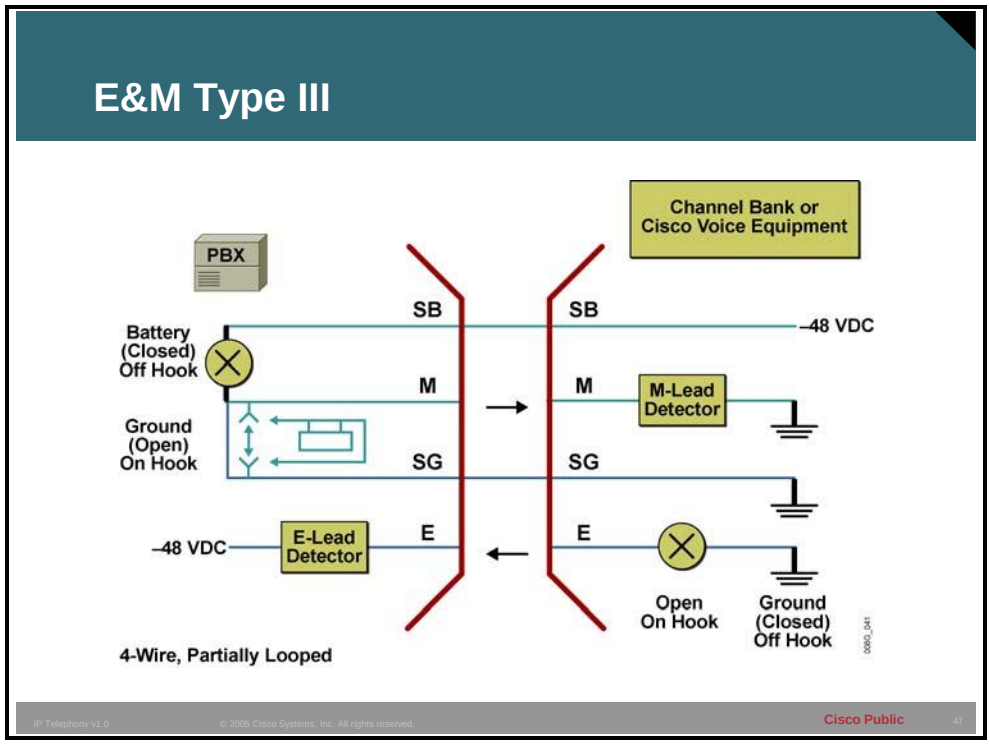
Type V is a modified version of the Type I interface. In the Type V interface, the Cisco voice equipment (tie-line equipment) supplies battery for the M-lead while the PBX supplies battery for the E-lead. As in Type I, Type V requires that a common ground be connected between the PBX and the Cisco voice equipment.



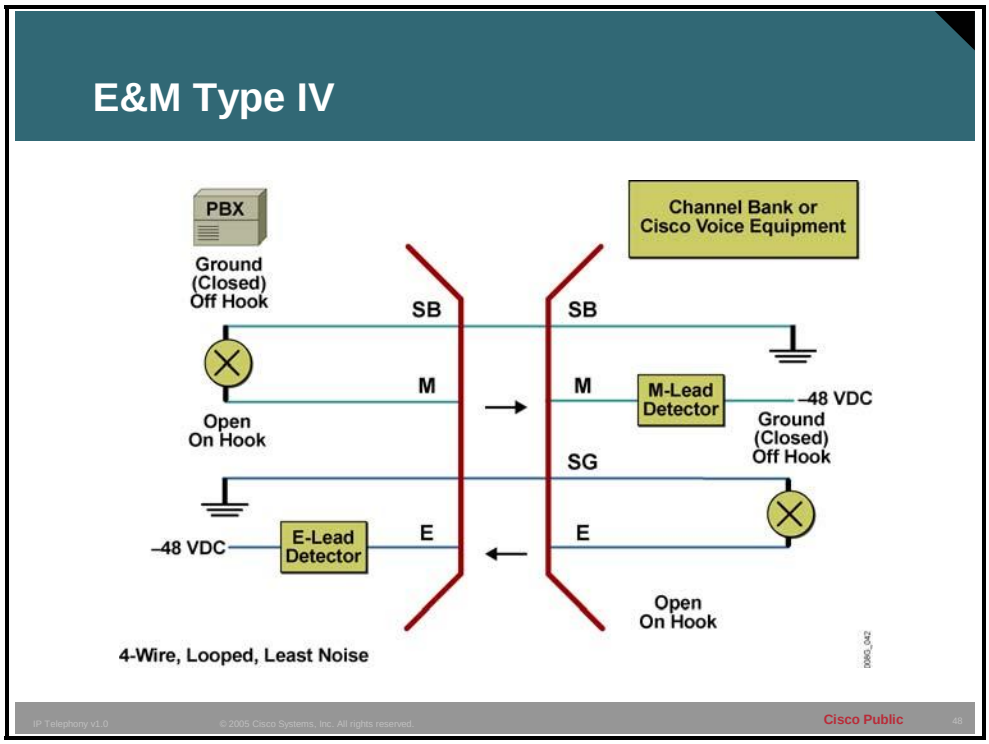
Types II, III, and IV are eight-wire interfaces. One wire is the E-lead, the other wire is the M-lead. Two other wires are signal ground (SG) and signal battery (SB). In Type II, SG and SB are the return paths for the E-lead and M-lead, respectively.

The Type II interface exists for applications where a common ground between the PBX and the Cisco voice equipment (tie-line equipment) is not possible or practical; for example, the PBX is in one building on a campus and the Cisco equipment is in another. Because there is no common ground, each of the signals has its own return. For the E signal, the tie-line equipment permits the current to flow from the PBX; the current returns to the PBX SG lead or reference. Similarly, the PBX closes a path for the current to generate the M signal to the Cisco voice equipment (tie-line equipment) on the SB lead.

 Copyright © 2005, Cisco Systems, Inc.



Type III is useful for environments where the M-lead is likely to experience electrical interference and falsely signal its attached equipment. When idle, Type III latches the M-lead via an electrical relay to the SG lead. When the PBX activates the M-lead, it first delatches the SG lead via the relay and signals normally, as in Type II. Type III is not a common implementation.



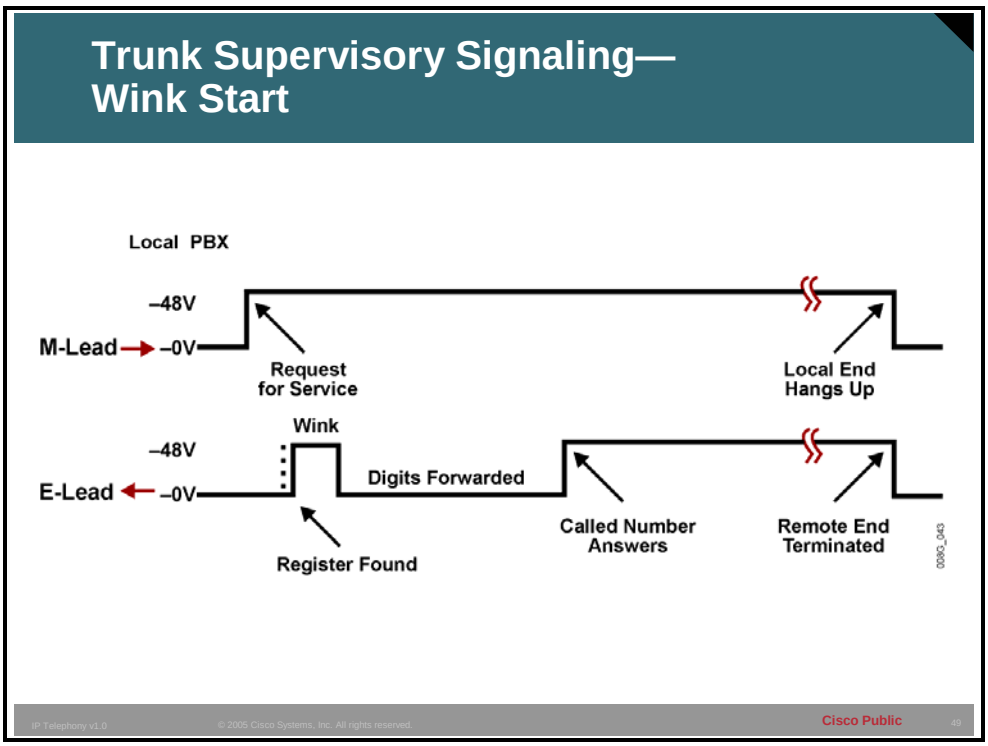
Type IV is a variation of Type II. In this arrangement, the battery source and ground are reversed on the SB and M wires (as compared to Type II). This means that both the SB and SG wires are grounded. Type IV signaling is symmetric and requires no common ground. Each side closes a current loop to signal, which detects the flow of current through a resistive load to indicate the presence of the signal. Cisco voice equipment does not support Type IV.

The most common E&M signaling interface in the United States is Type I, and the most common in European countries is Type V. Other variations exist for special applications and purposes. Cisco does not support Type IV.

 Copyright © 2005, Cisco Systems, Inc.

Trunk Signal Types Used by E&M

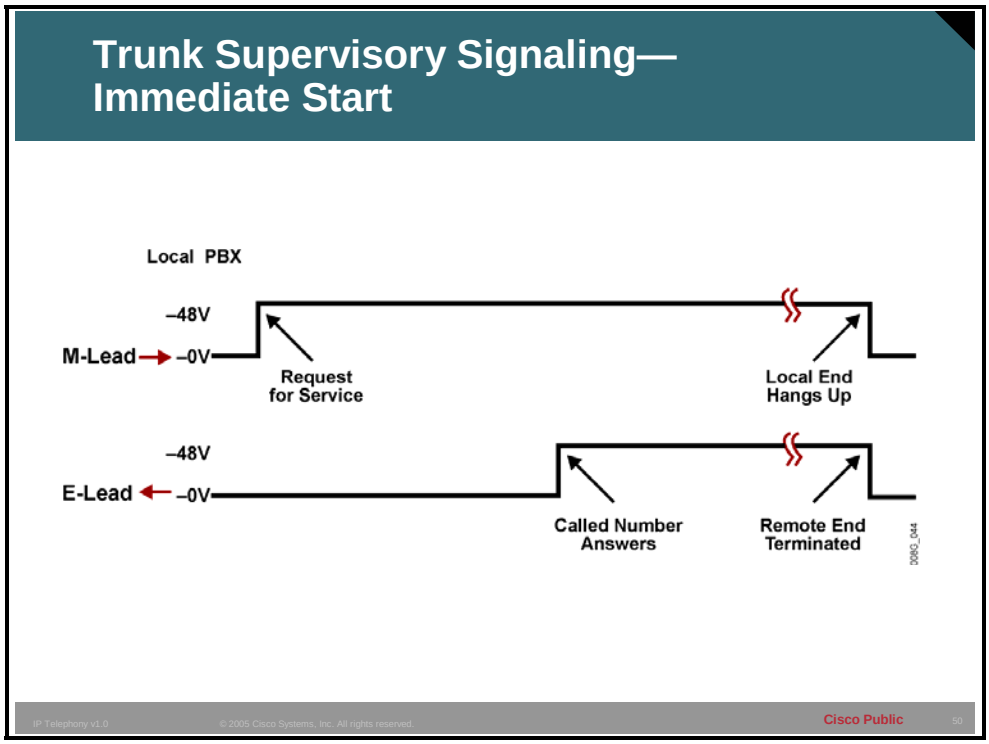
This topic describes Wink-Start, immediate-start, and delay-start signaling as used by E&M signaling.



Tie trunks have bidirectional supervisory signaling that allows either end to initiate a trunk seizure. In this way, one PBX seizes the trunk, which then waits for an acknowledgment reply from the remote end. The local end must differentiate between a return acknowledgment and a remote-end request for service. Wink-Start signaling is the most common E&M trunk seizure signal type.

The following scenario summarizes the Wink-Start protocol event sequence:

1. The calling office seizes the line by activating its M-lead.
2. Instead of returning an off-hook acknowledgment immediately, the called switch allocates memory for use as a dial register, in the area of memory it uses to store incoming digits.
3. The called switch toggles its M-lead on and off for a specific time (usually 170 to 340 ms). (This on-hook/off-hook/on-hook sequence constitutes the wink.)
4. The calling switch receives the wink on its E-lead and forwards the digits to the remote end. DTMF tones are forwarded across the E&M link in the audio path, not on the M-lead.
5. The called party answers the telephone, and the called PBX raises its M-lead for the duration of the call.

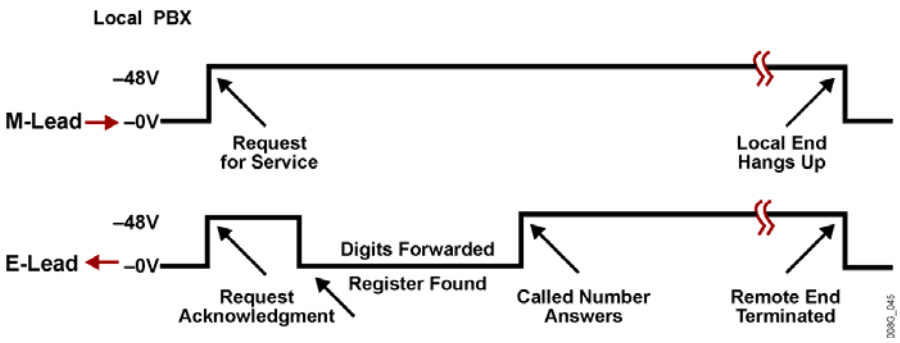


If the timing of the returned wink is too short or impossible to detect, the trunk uses immediate start. This occurs occasionally if a PBX vendor implements Wink Start but does not conform to the standards. The following scenario summarizes the sequence of events for the immediate-start protocol:

1. The calling PBX seizes the line by activating its M-lead.
2. Instead of receiving an acknowledgment, the calling PBX waits a predetermined period (a minimum of 150 ms) and forwards the digits blindly. DTMF tones are forwarded across the E&M link in the audio path, not on the M-lead.
3. The called PBX acknowledges the calling PBX only after the called party answers the call by raising its M-lead.

 Copyright © 2005, Cisco Systems, Inc.

Trunk Supervisory Signaling—Delay Start



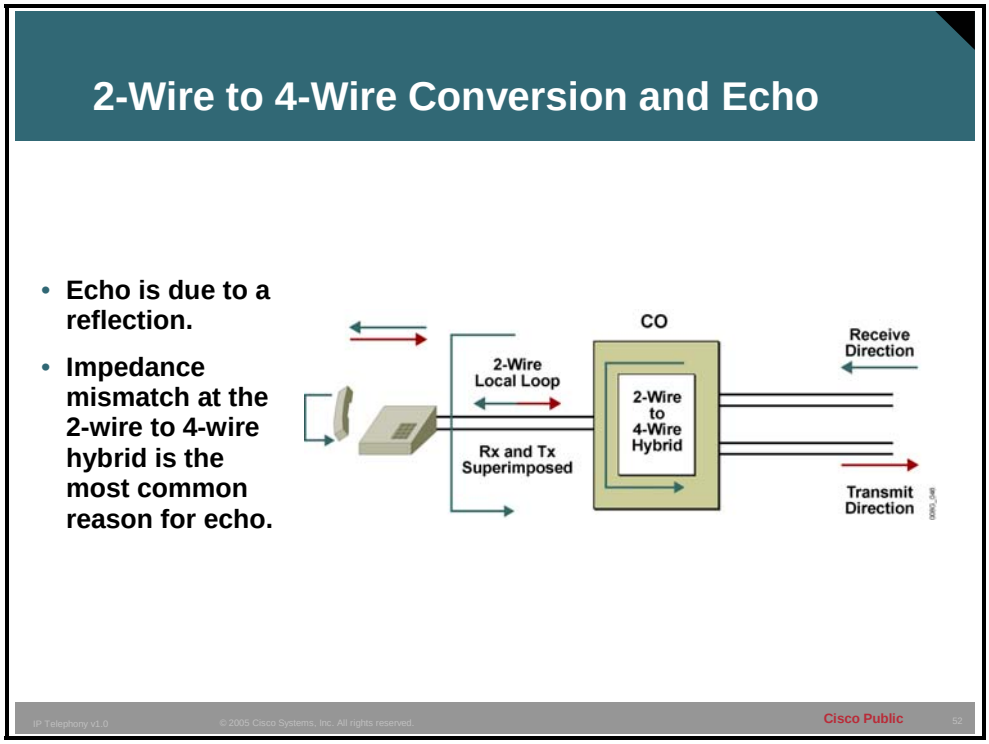
IP Telephony v1.0 © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 51

Delay start is the original start protocol for E&M. It is used when all of the equipment is mechanical and requires time to process requests. The following scenario summarizes delay-start signaling:

1. When you place a call, your calling switch goes off hook by activating its M-lead.
2. The called switch acknowledges the request by activating its M-lead, and then rotates armatures and gears to reset its dial register to zero.
3. When the dial register at the called switch is in the ready state, the called switch deactivates its M-lead.
4. The calling switch then sends dialed digits. DTMF tones are forwarded across the E&M link in the audio path, not on the M-lead.
5. When the called party answers, the called switch again activates its M-lead.

Line Quality

This topic describes impairments commonly found in analog telephone circuits and offers solutions to the problem of echo.

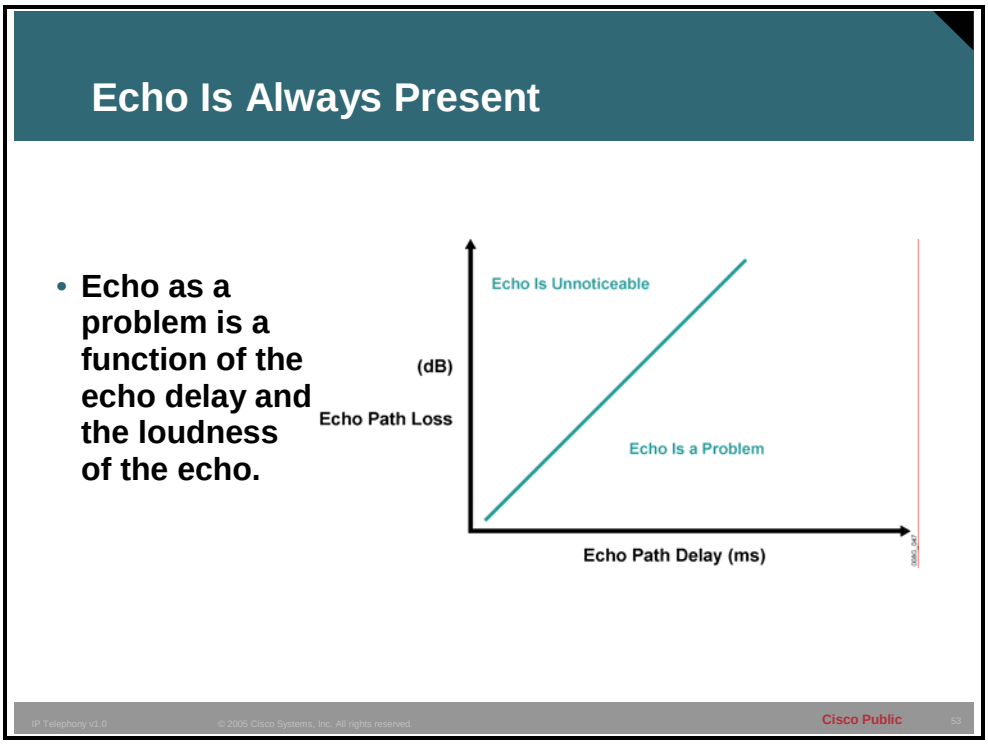


Although a local loop consists of two wires, when it reaches the switch, the connection changes to four wires with a two- to four-wire hybrid converter. Trunks then transport the signal across the network.

Telephone networks can experience two types of echo: acoustic echo and electrical echo. Acoustic echo frequently occurs with speakerphones, when the received voice on the speaker excites the microphone and travels back to the speaker. Electrical echo occurs when there is an electrical inconsistency in the telephony circuits. This electrical inconsistency is called impedance mismatch.

If the lines have a good impedance match, the hybrid is considered balanced, with little or no reflected energy. However, if the hybrid is inadequately balanced, and a portion of the transmit voice is reflected back toward the receive side, echo results.

 Copyright © 2005, Cisco Systems, Inc.



Some form of echo is always present. However, echo can become a problem under the following conditions:

- The magnitude or loudness of the echo is high.
- The delay time between when you speak and when you hear your voice reflected is significant.
- The listener hears the speaker twice.

The two components of echo are loudness and delay. Reducing either component reduces overall echo. When a user experiences delay, the conversation can get choppy, and the words of the participants sometimes overlap.

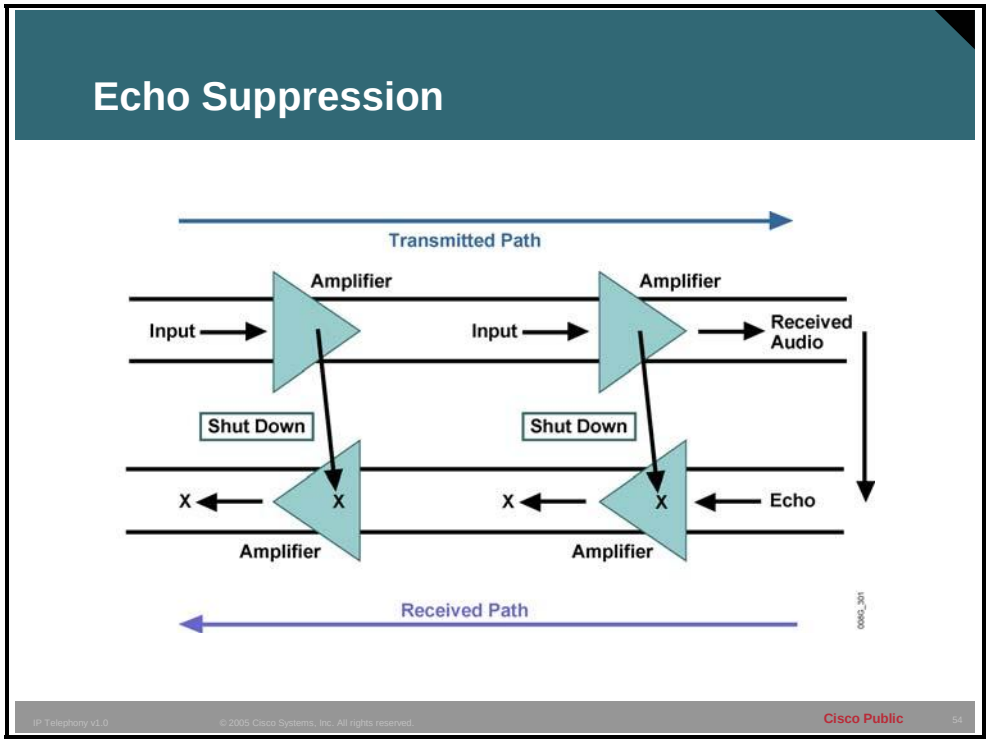
Note	Echo tolerance varies. For most users, however, echo delay over 50 ms is generally problematic.

Management of Echo

There are two ways to solve an echo problem in your telephone network:

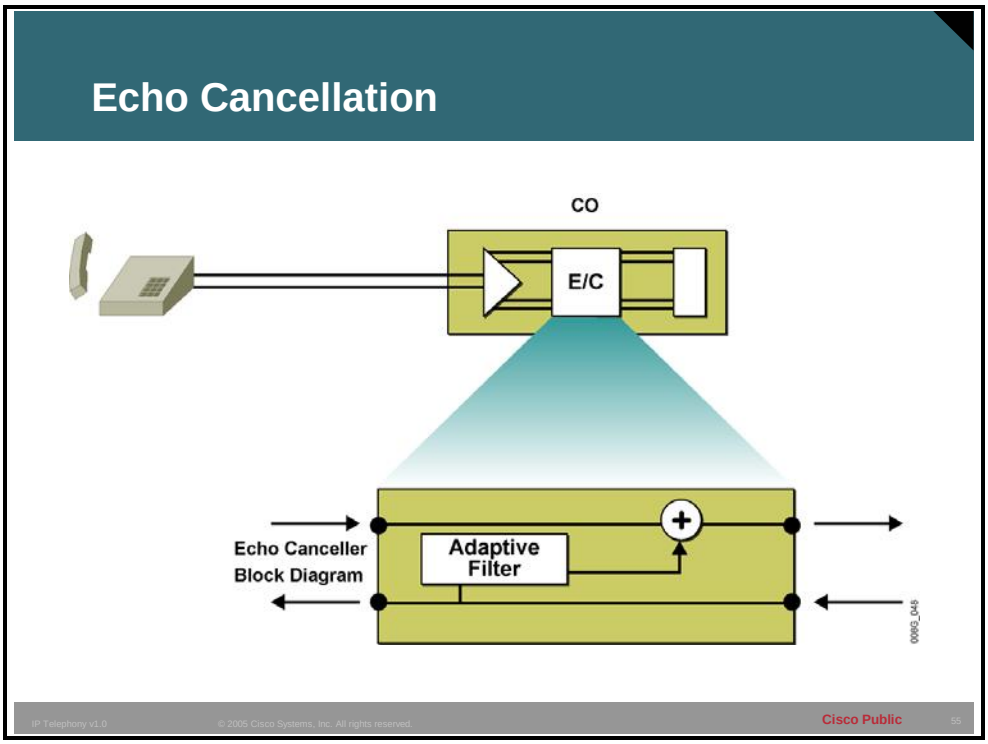
- Echo suppression
- Echo cancellation

This topic explains and compares the two approaches to echo management.



The echo suppressor works by transmitting speech in the forward direction and prohibiting audio in the return direction. The echo suppressor essentially breaks the return transmission path. This solution works sufficiently for voice transmission. However, for full-duplex modem connections, the action of the echo suppressor prevents communication. Therefore, when modems handshake, the answering modem returns a tone of 2025 Hz to the calling modem, which serves to disable the echo suppressors along the transmission path.

 Copyright © 2005, Cisco Systems, Inc.



Echo suppression has shortcomings in addressing certain echo conflict situations. Echo cancellation is a more sophisticated method of eliminating echo.

Rather than breaking or attenuating the return path (as in echo suppression), echo cancellation uses a special circuit to build a mathematical model of the transmitted speech pattern and subtract it from the return path. This echo elimination method is depicted in the figure.

Note	Echo cancellation applies the same technology that is used in audio headphones to cancel ambient noise.

Echo cancellation is the most common method of removing echo in the telephone network today, and is used when it is necessary to adjust for echo on a Cisco device.

Note	The echo canceller removes the echo from one end of the circuit only. If echo is an issue at both ends of the circuit, you must apply another echo canceller at the other end.

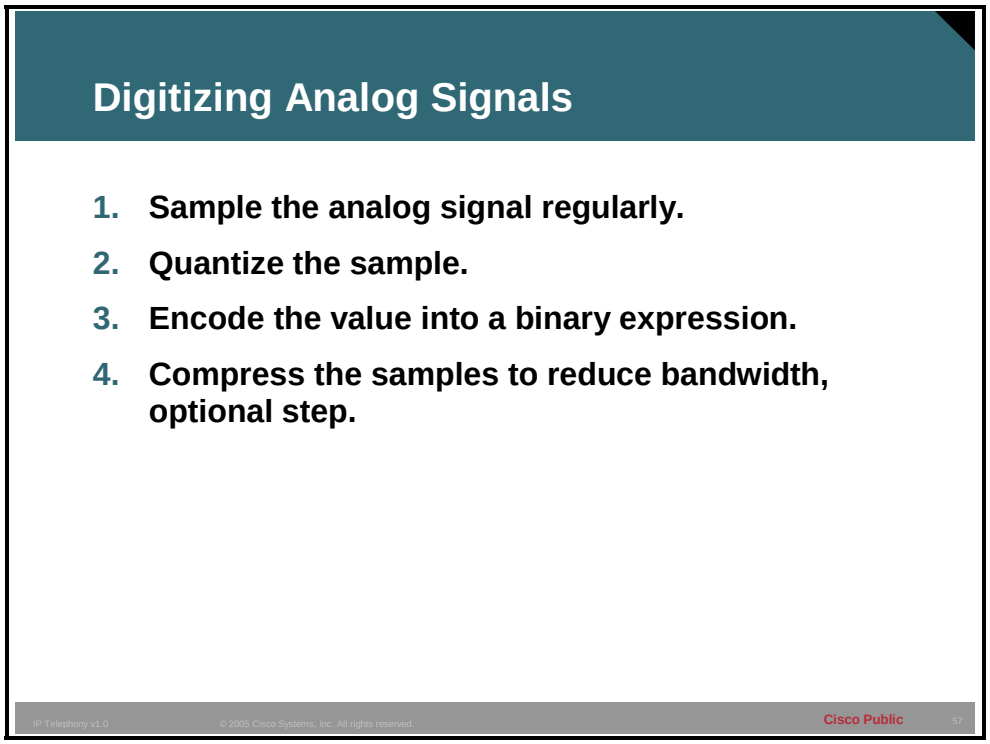
Example: Echo Cancellation

The headsets used by airline pilots feature a suppression circuit, which cancels ambient noise so that the pilot hears only the audio from the headset. Any ambient noise from the cockpit is cancelled. This is the same technology used in echo cancellers.

Analog-to-Digital Voice Encoding

Basic Voice Encoding: Converting Analog to Digital

This topic describes the process of converting analog signals to digital signals.



Digitizing speech was a project first undertaken by the Bell System in the 1950s. The original purpose of digitizing speech was to deploy more voice circuits with a smaller number of wires. This evolved into the T1 and E1 transmission methods of today.

 Copyright © 2005, Cisco Systems, Inc.

To convert an analog signal to a digital signal, you must perform these steps:

Analog-to-Digital Signal Conversion

Step	Procedure	Description
1.	Sample the analog signal regularly.	The sampling rate must be twice the highest frequency to produce playback that appears neither choppy nor too smooth.
2.	Quantize the sample.	Quantization consists of a scale made up of eight major divisions or chords. Each chord is subdivided into 16 equally spaced steps. The chords are not equally spaced but are actually finest near the origin. Steps are equal within the chords but different when they are compared between the chords. Finer graduations at the origin result in less distortion for low-level tones.
3.	Encode the value into 8-bit digital form.	PBX output is a continuous analog voice waveform. T1 digital voice is a snapshot of the wave encoded in ones and zeros.
4.	(Optional) Compress the samples to reduce bandwidth.	Although not essential to convert analog signals to digital, signal compression is widely used to reduce bandwidth.

The three components in the analog-to-digital conversion process are further described as follows:

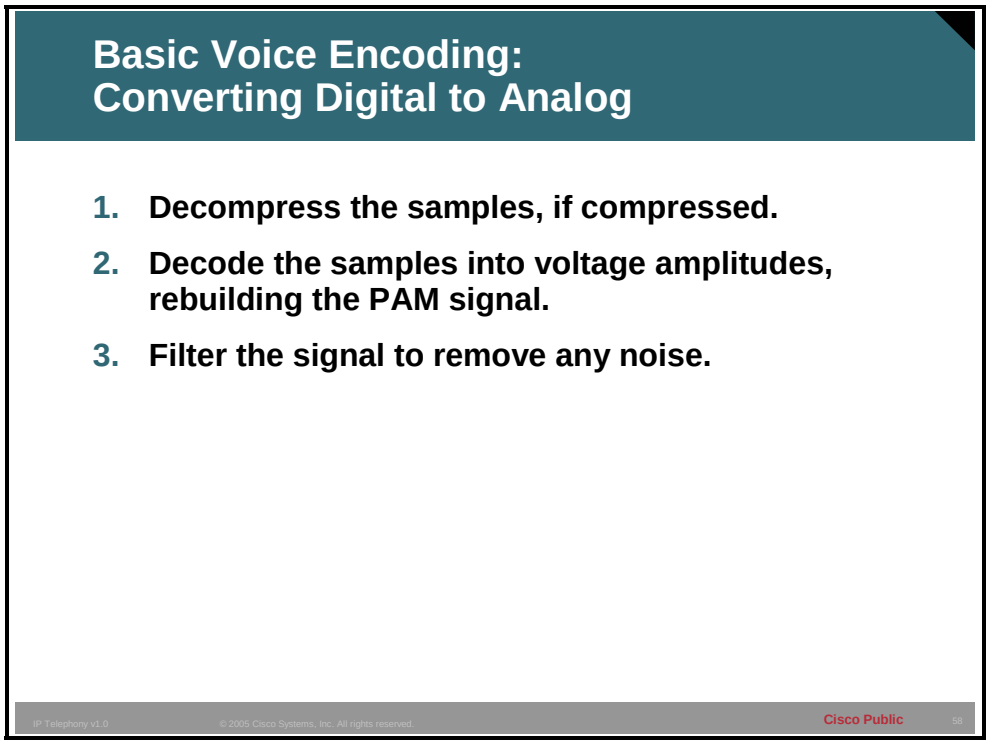
- **Sampling:** Sample the analog signal at periodic intervals. The output of sampling is a pulse amplitude modulation (PAM) signal.
- **Quantization:** Match the PAM signal to a segmented scale. This scale measures the amplitude (height) of the PAM signal and assigns an integer number to define that amplitude.
- **Encoding:** Convert the integer base-10 number to a binary number. The output of encoding is a binary expression in which each bit is either a 1 (pulse) or a 0 (no pulse).

This three-step process is repeated 8000 times per second for telephone voice-channel service. Use the fourth optional step—compression—to save bandwidth. This optional step allows a single channel to carry more voice calls.

Note The most commonly used method of converting analog to digital is pulse code modulation (PCM).

Basic Voice Encoding: Converting Digital to Analog

This topic describes the process of converting digital signals back to analog signals.



After the receiving terminal at the far end receives the digital PCM signal, it must convert the PCM signal back into an analog signal.

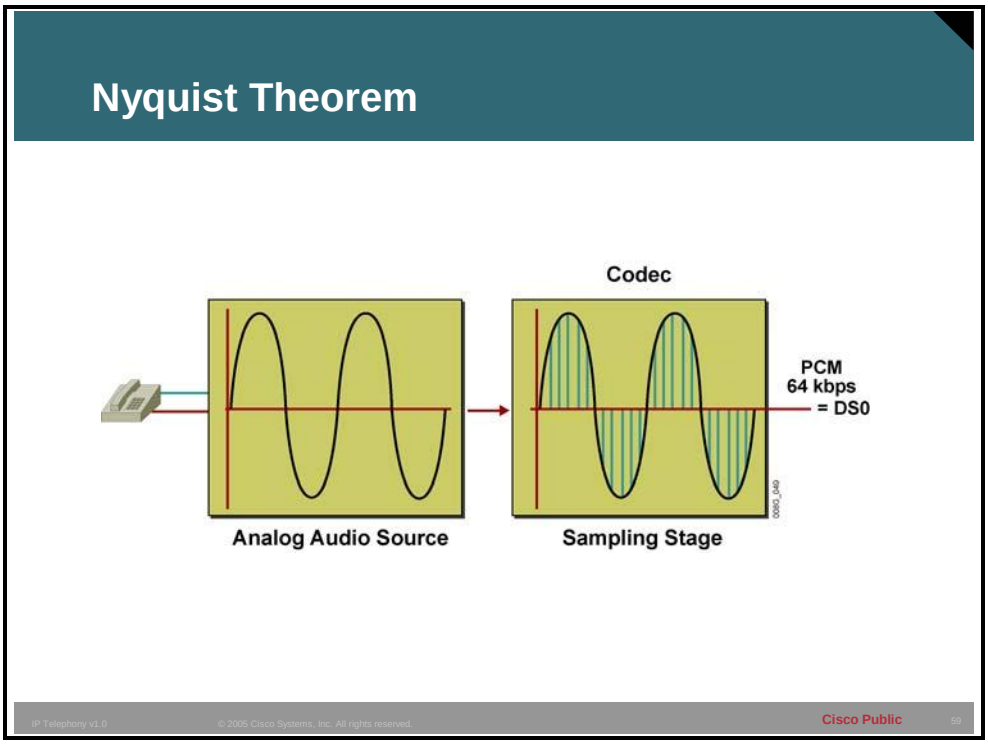
The process of converting digital signals back into analog signals includes the following two steps:

- **Decoding:** The received 8-bit word is decoded to recover the number that defines the amplitude of that sample. This information is used to rebuild a PAM signal of the original amplitude. This process is simply the reverse of the analog-to-digital conversion.
- **Filtering:** The PAM signal is passed through a properly designed filter that reconstructs the original analog wave form from its digitally coded counterpart.

 Copyright © 2005, Cisco Systems, Inc.

The Nyquist Theorem

This topic describes the Nyquist Theorem, which is the basis for digital signal technology.



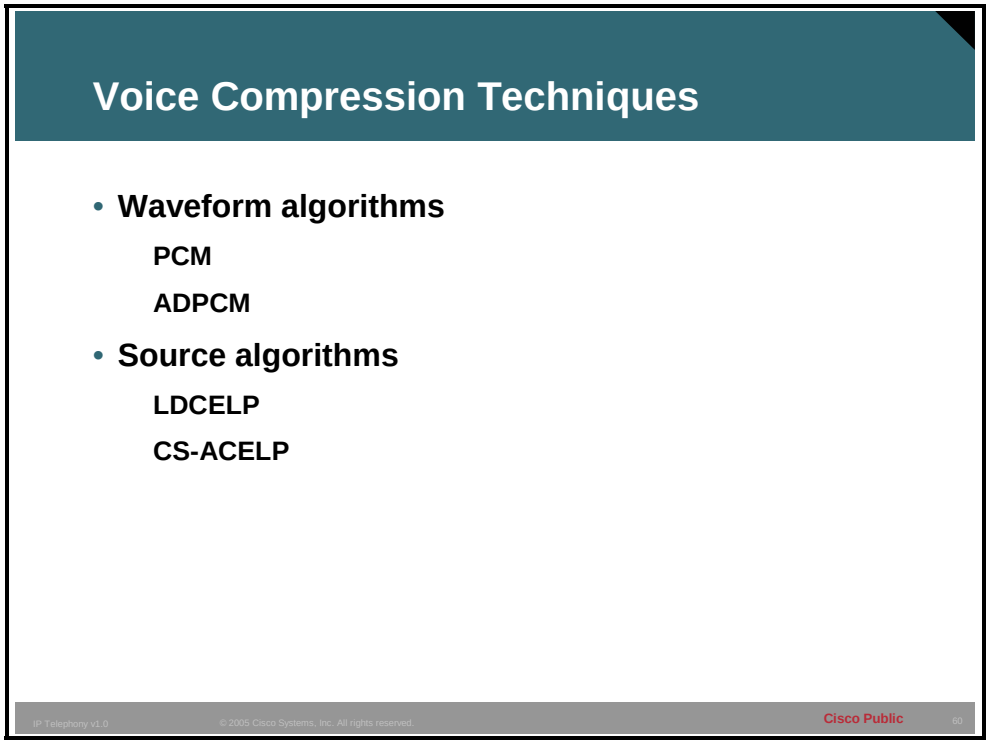
Digital signal technology is based on the premise stated in the Nyquist Theorem: when a signal is instantaneously sampled at the transmitter in regular intervals and has a rate of at least twice the highest channel frequency, then the samples will contain sufficient information to allow an accurate reconstruction of the signal at the receiver.

Example: Nyquist Theorem

While the human ear can sense sounds from 20 to 20,000 Hz, and speech encompasses sounds from about 200 to 9000 Hz, the telephone channel was designed to operate at about 300 to 3400 Hz. This economical range carries enough fidelity to allow callers to identify the party at the far end and sense their mood. Nyquist decided to extend the digitization to 4000 Hz, to capture higher-frequency sounds that the telephone channel may deliver. Therefore, the highest frequency for voice is 4000 Hz, or 8000 samples per second; that is, one sample every 125 microseconds.

Voice Compression and Codec Standards

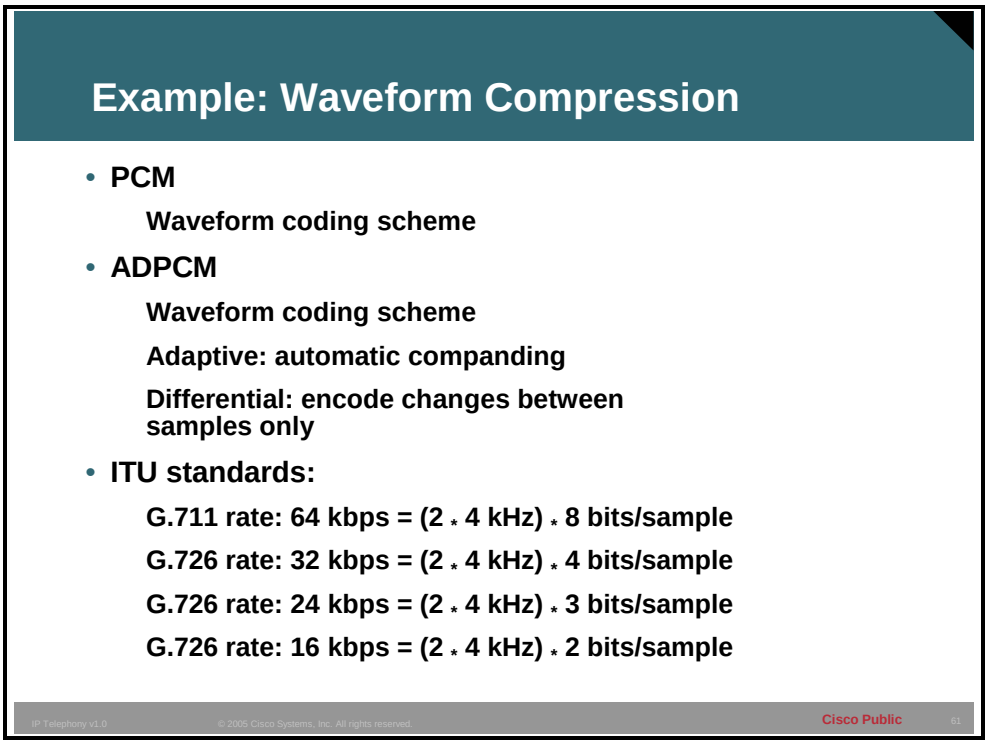
This topic describes two types of voice-compression schemes: waveform coding and source coding.



The following describes the two voice compression techniques:

- **Waveform algorithms (coders):** Waveform algorithms have the following functions and characteristics:
  - Sample analog signals at 8000 times per second
  - Use predictive differential methods to reduce bandwidth
  - Highly impact voice quality because of reduced bandwith
  - Do not take advantage of speech characteristics
- **Source algorithms (coders):** Source algorithms have the following functions and characteristics:
  - Source algorithm coders are called vocoders, or voice coders. A vocoder is a device that converts analog speech into digital speech, using a specific compression scheme that is optimized for coding human speech.
  - Vocoders take advantage of speech characteristics.
  - Bandwidth reduction occurs by sending linear-filter settings.
  - Codebooks store specific predictive waveshapes of human speech. They match the speech, encode the phrases, decode the waveshapes at the receiver by looking up the coded phrase, and match it to the stored waveshape in the receiver codebook.

 Copyright © 2005, Cisco Systems, Inc.



Standard PCM is known as ITU standard G.711.

Adaptive differential pulse code modulation (ADPCM) coders, like other waveform coders, encode analog voice signals into digital signals to adaptively predict future encodings by looking at the immediate past. The adaptive feature of ADPCM reduces the number of bits per second that the PCM method requires to encode voice signals.

ADPCM does this by taking 8000 samples per second of the analog voice signal and turning them into a linear PCM sample. ADPCM then calculates the predicted value of the next sample, based on the immediate past sample, and encodes the difference. The ADPCM process generates 4-bit words, thereby generating 16 specific bit patterns.

The ADPCM algorithm from the Consultative Committee for International Telegraph and Telephone (CCITT) transmits all 16 possible bit patterns. The ADPCM algorithm from the American National Standards Institute (ANSI) uses 15 of the 16 possible bit patterns. The ANSI ADPCM algorithm does not generate a 0000 pattern.

The ITU standards for compression are as follows:

- **G.711 rate:** 64 kbps = (2 * 4 kHz) * 8 bits/sample
- **G.726 rate:** 32 kbps = (2 * 4 kHz) * 4 bits/sample
- **G.726 rate:** 24 kbps = (2 * 4 kHz) * 3 bits/sample
- **G.726 rate:** 16 kbps = (2 * 4 kHz) * 2 bits/sample

Note	CCITT is now called International Telecommunication Union Telecommunication Standardization Sector (ITU-T).

G.729, G.729 Annex A (G.729A), G.729 Annex B (G.729B), and G.729A Annex B (G.729AB) are variations of CS-ACELP.

There is little difference between the ITU recommendations for G.729 and G.729A. All of the platforms that support G.729 also support G.729A.

G.729 is the compression algorithm that Cisco uses for high-quality 8-kbps voice. When properly implemented, G.729 sounds as good as the 32-kbps ADPCM. G.729 is a high-complexity, processor-intensive compression algorithm that monopolizes processing resources.

Although G.729A is also an 8-kbps compression, it is not as processor-intensive as G.729. It is a medium-complexity variant of G.729 with slightly lower voice quality. G.729A is not as high-quality as G.729 and is more susceptible to network irregularities, such as delay, variation, and tandeming. Tandeming causes distortion that occurs when speech is coded, decoded, and then coded and decoded again, much like the distortion that occurs when a videotape is repeatedly copied.

Example: Codec Complexity

On Cisco IOS gateways, you must use the variant (G.729 or G.729A) that is related to the codec complexity configuration on the voice card. This variant does not show up explicitly in the Cisco IOS command-line interface (CLI) codec choice. For example, the CLI does not display **g729r8** (alpha code) as a codec option. However, if the voice card is defined as medium-complexity, then the **g729r8** option is the G.729A codec.

G.729B is a high-complexity algorithm, and G.729AB is a medium-complexity variant of G.729B with slightly lower voice quality. The difference between the G.729 and G.729B codec is that the G.729B codec provides built-in Internet Engineering Task Force (IETF) VAD and comfort noise generation (CNG).

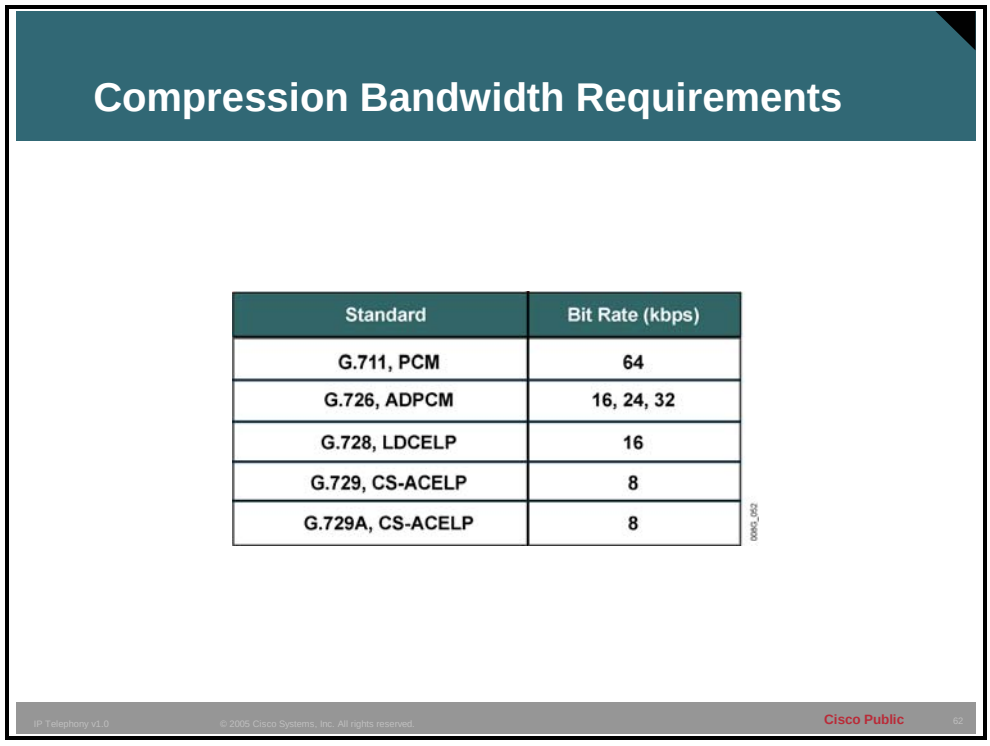
The following G.729 codec combinations interoperate:

- G.729 and G.729A
- G.729 and G.729
- G.729A and G.729A
- G.729B and G.729AB
- G.729B and G.729B
- G.729AB and G.729AB

 Copyright © 2005, Cisco Systems, Inc.

Compression Bandwidth Requirements

This topic lists the bandwidth requirements for various ITU compression standards.



The following three common voice compression techniques are standardized by the ITU-T:

- **PCM:** Amplitude of voice signal is sampled and quantized at 8000 times per second. Each sample is then represented by one octet (8 bits) and transmitted. For sampling, you must use either a-law or μ-law to reduce the signal-to-noise ratio.
- **ADPCM:** The difference between the current sample and its predicted value (based on past samples). ADPCM is represented by 2, 3, 4, or 5 bits. This method reduces the bandwidth requirement at the expense of signal quality.
- **CELP:** Excitation value and a set of linear-predictive filters (settings) are transmitted. The filter setting transmissions are less frequent than excitation values and are sent on an as-needed basis.

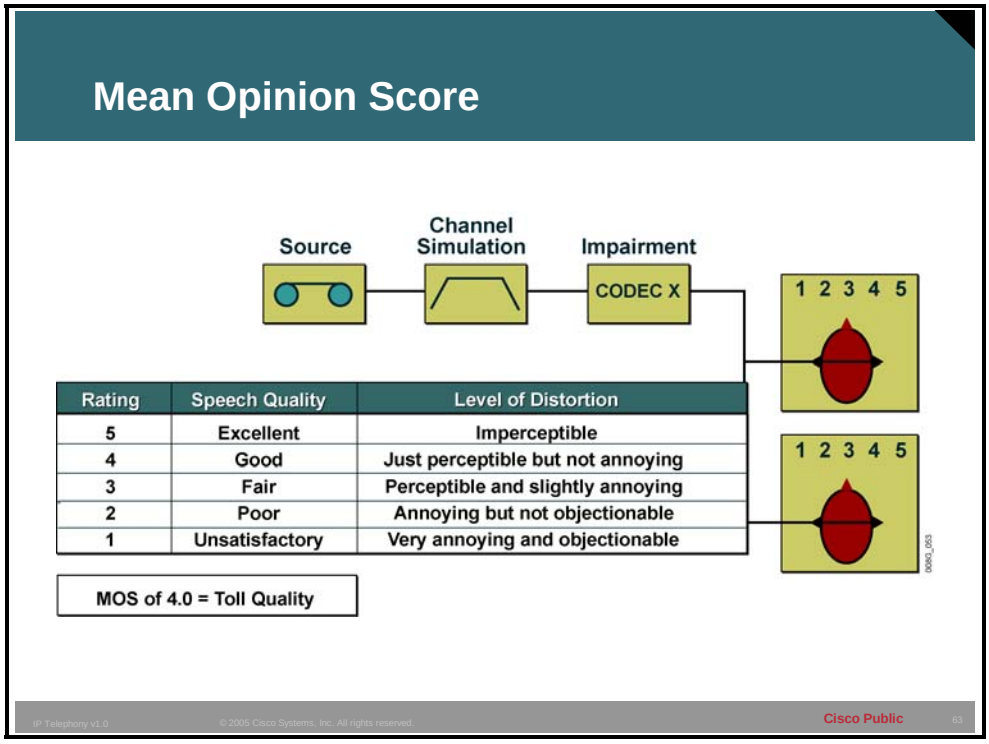
The table describes the codecs and compression standards:

Codecs and Compression Standards

Codec	Compression Technique	Bit Rate (kbps)
G.711	PCM	64
G.726	ADPCM	16, 24, 32
G.728	LDCELP	16
G.729	CS-ACELP	8
G.729A	CS-ACELP	8

Voice Quality Measurement

This topic describes two methods that are used to subjectively measure the quality of voice transported on a telephone line. Because different compression schemes produce different quality results, a method of comparing them is necessary.



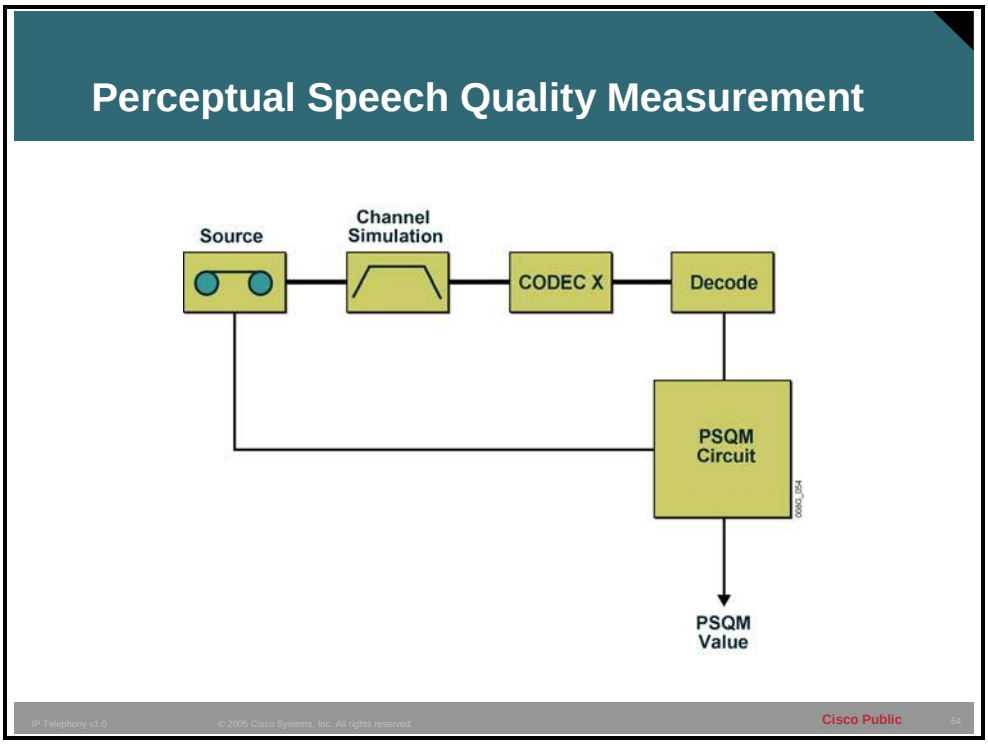
The figure depicts mean opinion score (MOS). MOS is a system of grading the voice quality of telephone connections. The MOS is a statistical measurement of voice quality derived from the judgments of several subscribers.

Graded by humans and very subjective, the range of MOS is 1 to 5, where 5 is direct conversation.

Voice Quality of Telephone Connections

Rating	Speech Quality	Level of Distortion
5	Excellent	Imperceptible
4	Good	Just perceptible but not annoying
3	Fair	Perceptible and slightly annoying
2	Poor	Annoying but not objectionable
1	Unsatisfactory	Very annoying and objectionable

 Copyright © 2005, Cisco Systems, Inc.



A newer, more objective measurement is available that is quickly overtaking MOS scores as the industry quality measurement of choice for coding algorithms. Perceptual Speech Quality Measurement (PSQM), as per ITU standard P.861, provides a rating on a scale of 0 to 6.5, where 0 is best and 6.5 is worst.

PSQM is implemented in test equipment and monitoring systems that are available from vendors other than Cisco. Some PSQM test equipment converts the 0-to-6.5 scale to a 0-to-5 scale to correlate to MOS. PSQM works by comparing the transmitted speech to the original input and yields a score. Various vendor test equipment is now capable of providing a PSQM score for a test voice call over a particular packet network.

In 1998, British Telecom developed a predictive voice quality measurement algorithm called Perceptual Analysis Measurement System (PAMS). PAMS can predict subjective speech quality measurement methods, such as MOS, when fidelity is affected by such things as waveform codecs, vocoders, and various speaker dependencies, such as language. PAMS, unlike PSQM, includes automatic normalization for levels.

ITU standard P.862 supercedes P.861 and describes a voice quality measurement technique that combines PSQM and PAMS. Originally developed by KPN Research, the Netherlands, and British Telecommunications (BT), Perceptual Evaluation of Speech Quality (PESQ) is an objective measuring tool that can “predict” results of subjective measuring tests, such as MOS. PESQ can be found in test equipment from a variety of vendors.

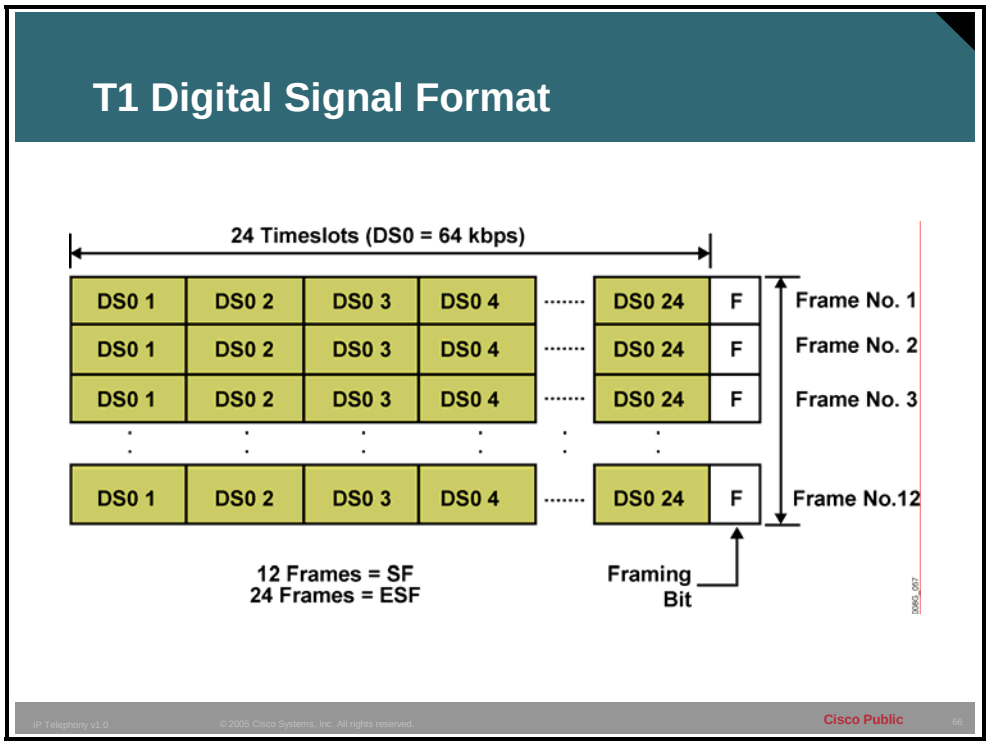
Example: Measuring Voice Quality

Cisco voice equipment does not perform voice quality measurements. There are a number of vendors who offer voice quality measurement products, some of which are designed to work with Cisco CallManager and CiscoWorks.

Signaling Systems

CAS Systems: T1

This topic describes channel associated signaling (CAS) and its uses with T1 transmission.



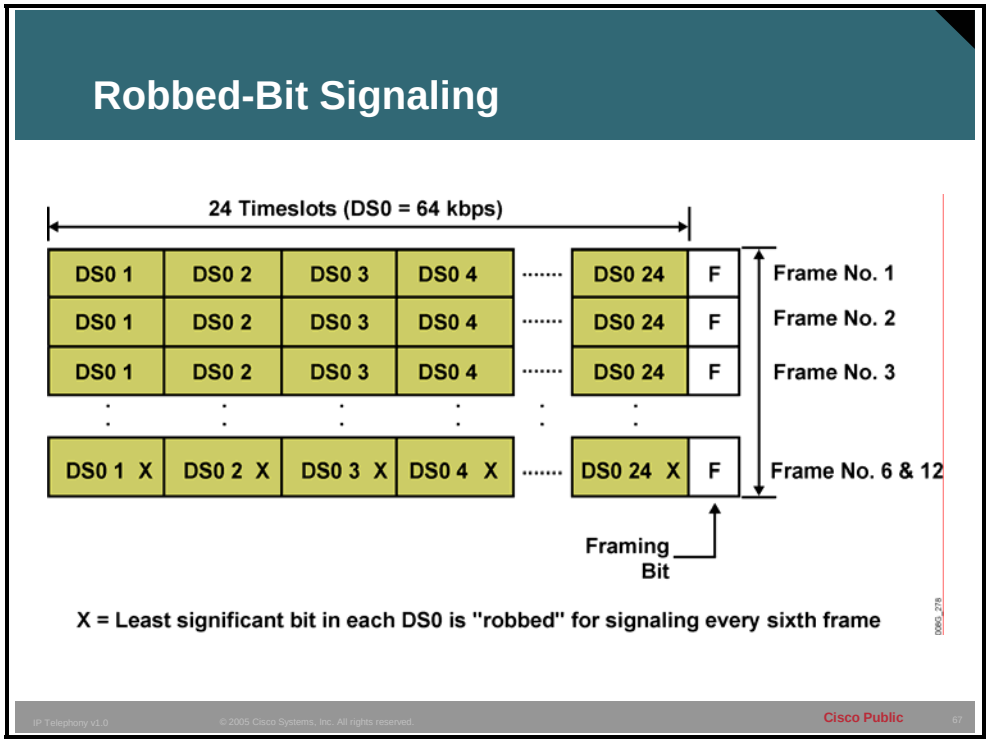
CAS is a signaling method commonly used between PBXs. Although this can manifest itself in many forms, some methods are more common than others. Signaling systems can also be implemented between a PBX and a Cisco voice device.

PBXs and Cisco devices use T1 and E1 to convey voice. Originally, this was the main purpose of T1, which carries signaling information using two methodologies, CAS and common channel signaling (CCS). The figure illustrates the format of the T1 digital signal.

 Copyright © 2005, Cisco Systems, Inc.

The characteristics of the T1 digital signal format are as follows:

- A T1 frame is 193 bits long—8 bits from each of the 24 timeslots (digital service zeros [DS0s]) plus 1 bit for framing. A T1 repeats every 125 microseconds, resulting in 8000 samples per second (8 bits * 24 timeslots + 1 framing bit * 8000 samples/second = 1.544 Mbps).
- T1 has two major framing and/or format standards:
  - Super Frame (SF), or D4, specifies 12 frames in sequence. The D4 framing pattern used in the F position in the figure is 100011011100 (a 1 goes with the first frame, a 0 goes with the second frame, a 0 goes with the third frame, and so on all the way through 12 frames). This unique framing pattern allows the receiving T1 equipment to synchronize within four frames, since any four consecutive frame bits are unique within the 12-bit pattern. Because there are 8000 T1 frames transmitted per second, 8000 F bits are produced and used for framing.
  - Extended Superframe (ESF) format was developed as an upgrade to SF and is now dominant in public and private networks. Both types of format retain the basic frame structure of one framing bit followed by 192 data bits. However, ESF repurposes the use of the F bit. In ESF, of the total 8000 F bits used in T1, 2000 are used for framing, 2000 are used for cyclic redundancy check (CRC) (for error checking only), and 4000 are used as an intelligent supervisory channel to control functions end to end (such as loopback and error reporting).

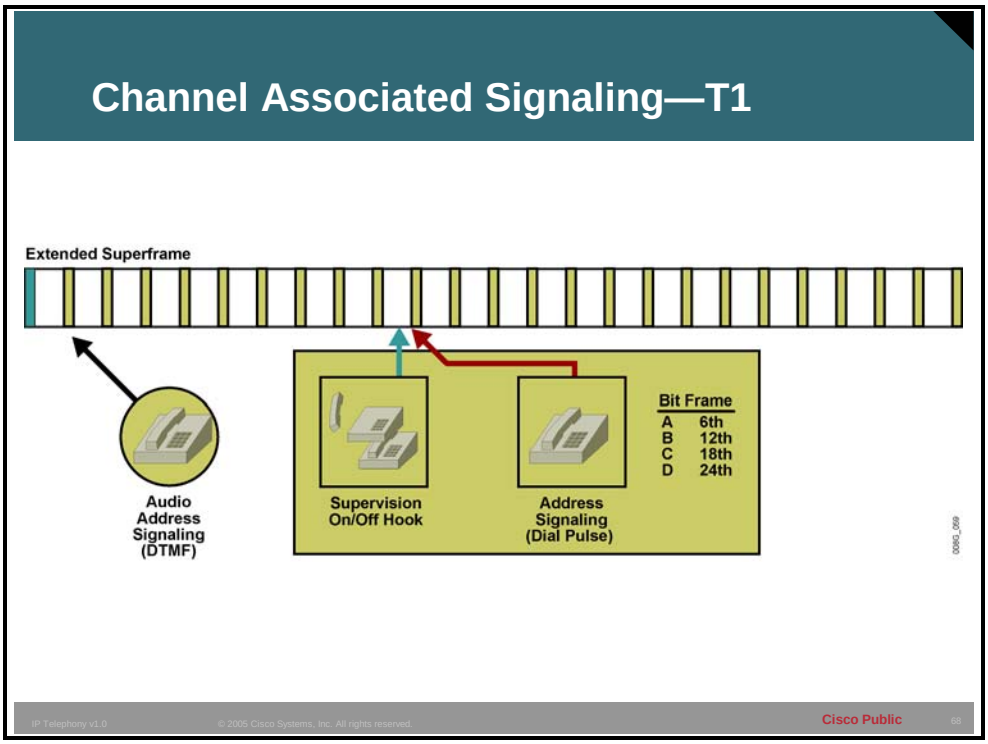


Because each DS0 channel carries 64 kbps, and G.711 is 64 kbps, there is no room to carry signaling. Implemented for voice, the T1 uses every sixth frame to convey signaling information. In every sixth frame, the least significant bit (LSB) for each of the voice channels is used to convey the signaling. Although this implementation detracts from the overall voice quality (because only seven bits represent a sample for that frame), the impact is not significant. This method is called robbed-bit signaling (RBS). When SF employs this method, the signaling bits are conveyed in both the 6th (called the “A” bit) and 12th (called the “B” bit) frames. For control signaling, A and B bits provide both near- and far-end off-hook indication.

The A and B bits can represent different signaling states or control features (on hook or off hook, idle, busy, ringing, and addressing). The robbed bit is the least significant bit from an 8-bit word.

ESF also uses RBS in frames 6, 12, 18, and 24, which yields ABCD signaling options, providing additional control and signaling information.

 Copyright © 2005, Cisco Systems, Inc.



Because the signaling occurs within each DS0, it is referred to as in band. Also, because the use of these bits is exclusively reserved for signaling each respective voice channel, it is referred to as CAS.

The robbed bits are used to convey E&M status or FXS/FXO status and provide call supervision for both on hook and off hook.

Example: Channel Associated Signaling

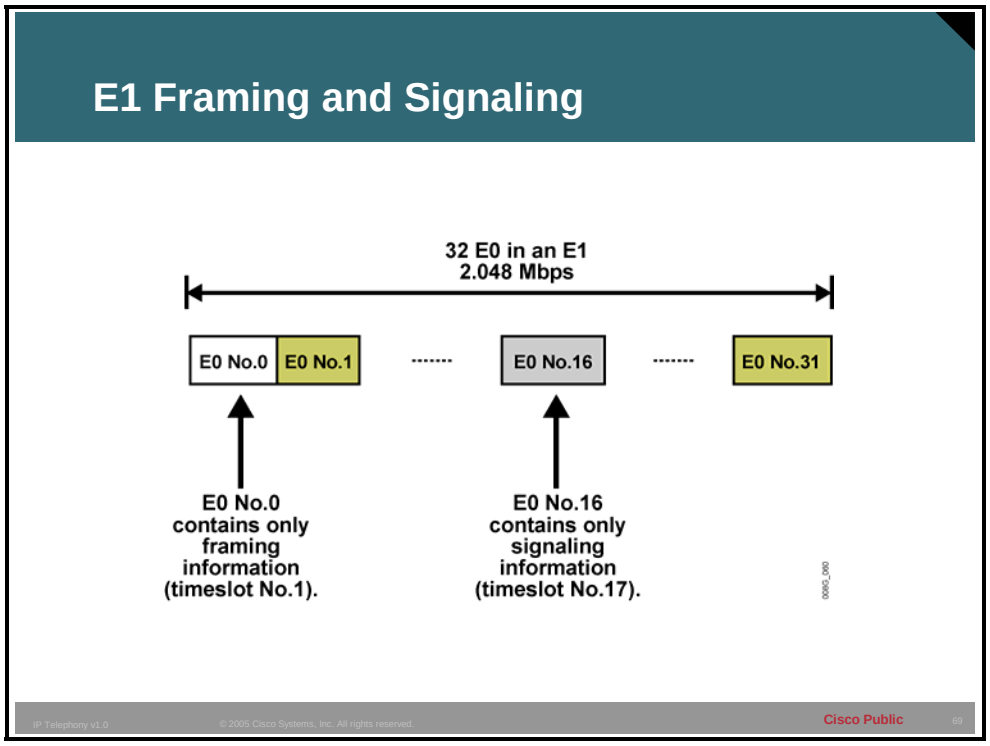
D4 has a 12-frame structure and provides AB bits for signaling.

ESF has a 24-frame structure and provides ABCD bits for signaling.

DTMF, or tone, can be carried in band in the audio path; however, other supervisory signals must still be carried via CAS.

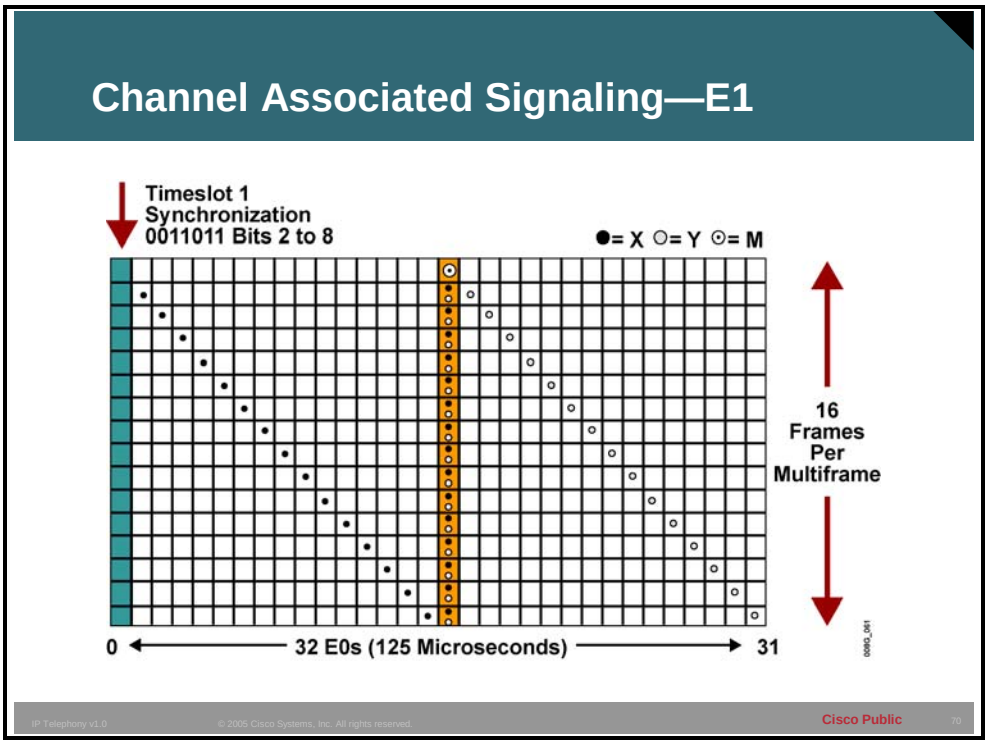
CAS Systems: E1

This topic describes CAS and its uses with E1 transmission.



In E1 framing and signaling, 30 of the 32 available channels, or timeslots, are used for voice and data. Framing information uses timeslot 1, while timeslot 17 (E0 16) is used for signaling by all the other timeslots. This signaling format is also known as CAS because the use of the bits in the 17th timeslot is exclusively reserved for the purpose of signaling each respective channel. However, this implementation of CAS is considered out of band because the signaling bits are not carried within the context of each respective voice channel, as is the case with T1.

 Copyright © 2005, Cisco Systems, Inc.



In the E1 frame format, 32 timeslots make up a frame. A multiframe consists of 16 E1 frames, as depicted in the figure.

The timeslots are numbered 1 though 32. Multiframe timeslots are configured as follows:

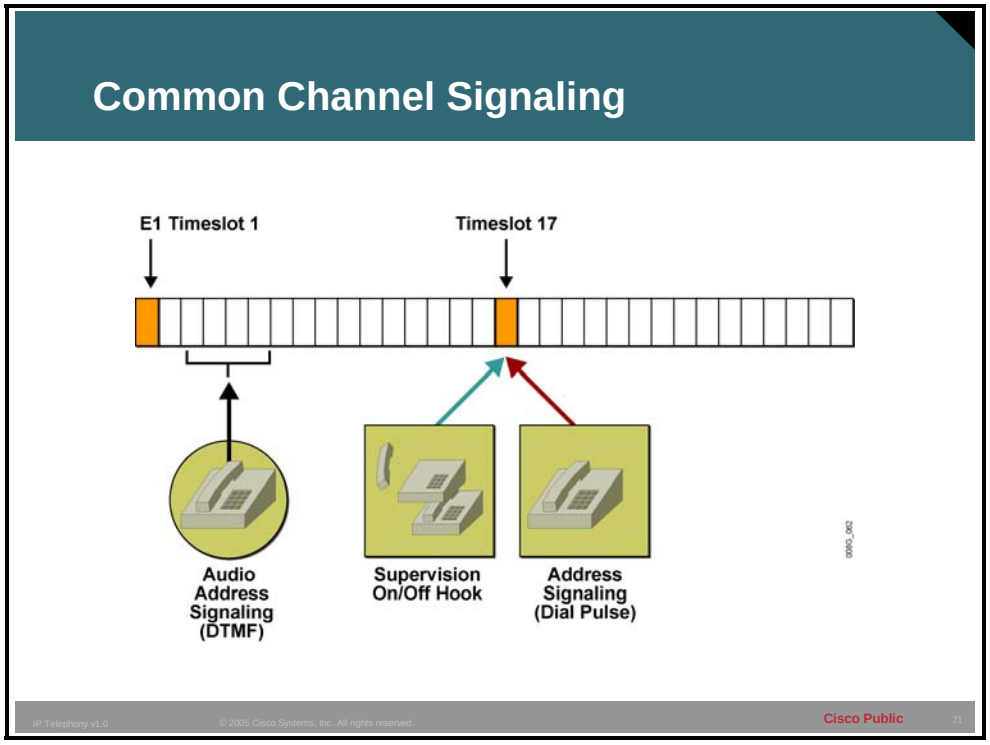
- Timeslot 1 carries only framing information.
- Timeslot 17, in the first frame of the 16-frame multiframe, declares the beginning of the multiframe, which is indicated by the M symbol in the figure.
- The remaining slot 17s carry signaling information for all the other timeslots:
  - Slot 17 of the first frame declares the beginning of a 16-frame multiframe (M).
  - Slot 17 of the second frame carries ABCD for voice slot 2 (X) and ABCD for voice slot 18 (Y).
  - Slot 17 of the third frame carries ABCD for voice slot 3 (X) and ABCD for voice slot 19 (Y).
  - This process continues for all of the remaining frames.

Example: E1 Channel Associated Signaling

E1 CAS is directly compatible with T1 CAS, because both methods use AB or ABCD bit signaling. Although the signaling for E1 CAS is carried in a single common timeslot, it is still referred to as CAS because each individual signaling timeslot represents a specific pair of voice channels.

CCS Systems

This topic describes common channel signaling (CCS) systems.



CCS differs from CAS in that all channels use a common channel and protocol for call setup. Using E1 as an example, a signaling protocol, such as the ISDN Q.931, would be deployed in timeslot 17 to exchange call-setup messages with its attached telephony equipment.

Example: CCS Signaling

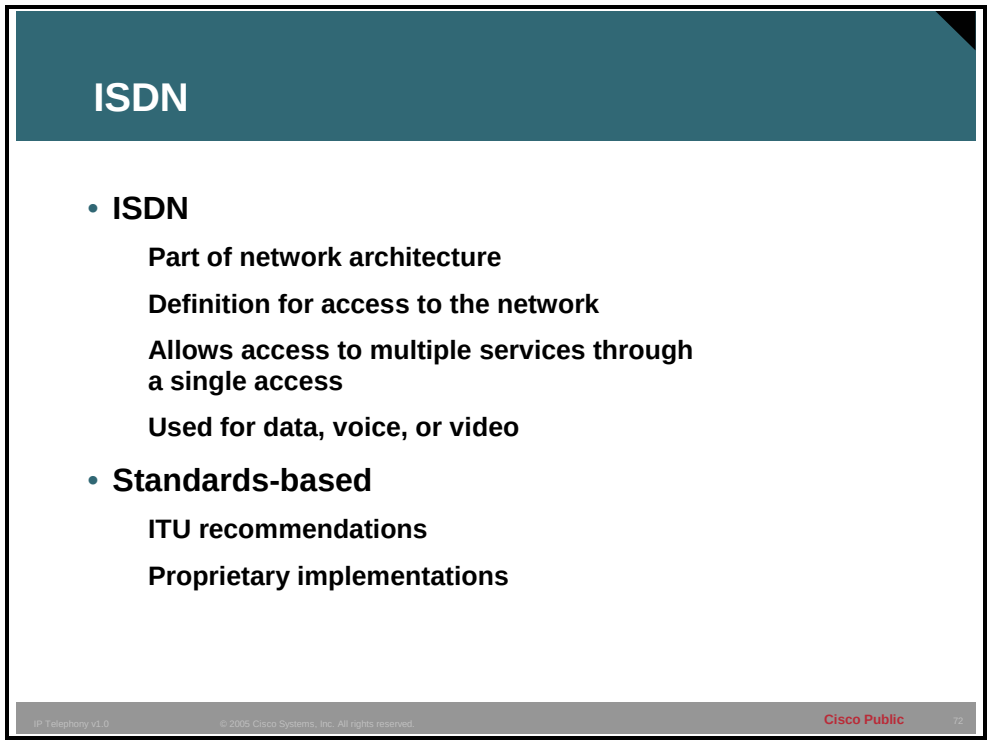
Examples of CCS signaling are as follows:

- **Proprietary implementations:** Some PBX vendors choose to use CCS for T1 and E1 and implement a proprietary CCS protocol between their PBXs. In this implementation, Cisco devices are configured for Transparent Common Channel Signaling (T-CCS) because they do not understand proprietary signaling information.
- **ISDN:** Uses Q.931 in a common channel to signal all other channels.
- **Digital Private Network Signaling System (DPNSS):** An open standard developed by British Telecom for implementation by any vendor who chooses to use it. DPNSS also uses a common channel to signal all other channels.
- **Q Signaling (QSIG):** Like ISDN, uses a common channel to signal all other channels.
- **Signaling System 7 (SS7):** An out-of-band network implemented and maintained by various telephone companies and used for signaling and other supplemental services.

 Copyright © 2005, Cisco Systems, Inc.

ISDN

This topic describes how to implement ISDN as a signaling system to support voice.



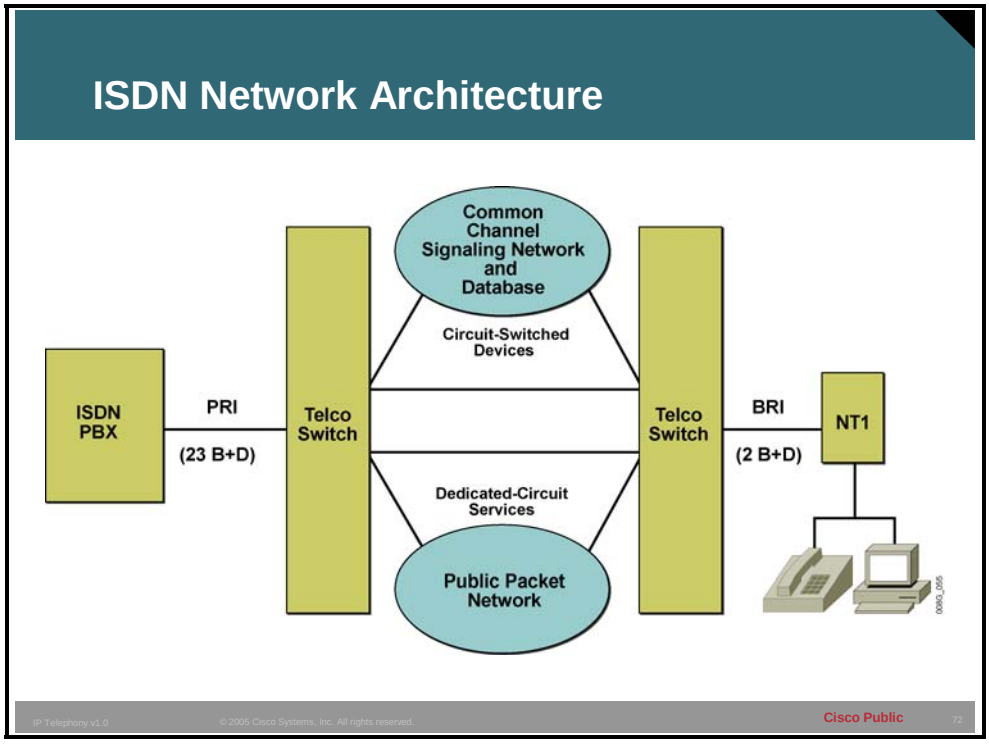
ISDN is an access specification to a network. You may have studied ISDN as an access method for dialup data systems. Because it is a digital system, ISDN makes connections rapidly.

ISDN can be implemented in two different ways: BRI and PRI. BRI features two bearer (B) channels, while PRI supports 23 (for T1) or 30 (for E1) B channels. Each implementation also supports a data (D) channel, used to carry signaling information (CCS).

The following are benefits of using ISDN to convey voice:

- Each B channel is 64 kbps, making it perfect for G.711 PCM.
- ISDN has a built-in call control protocol known as ITU-T Q.931.
- ISDN can convey standards-based voice features, such as call forwarding.
- ISDN supports standards-based enhanced dialup capabilities, such as Group 4 fax and audio channels.

Note ISDN BRI voice is commonly used in Europe; ISDN PRI voice is used worldwide.



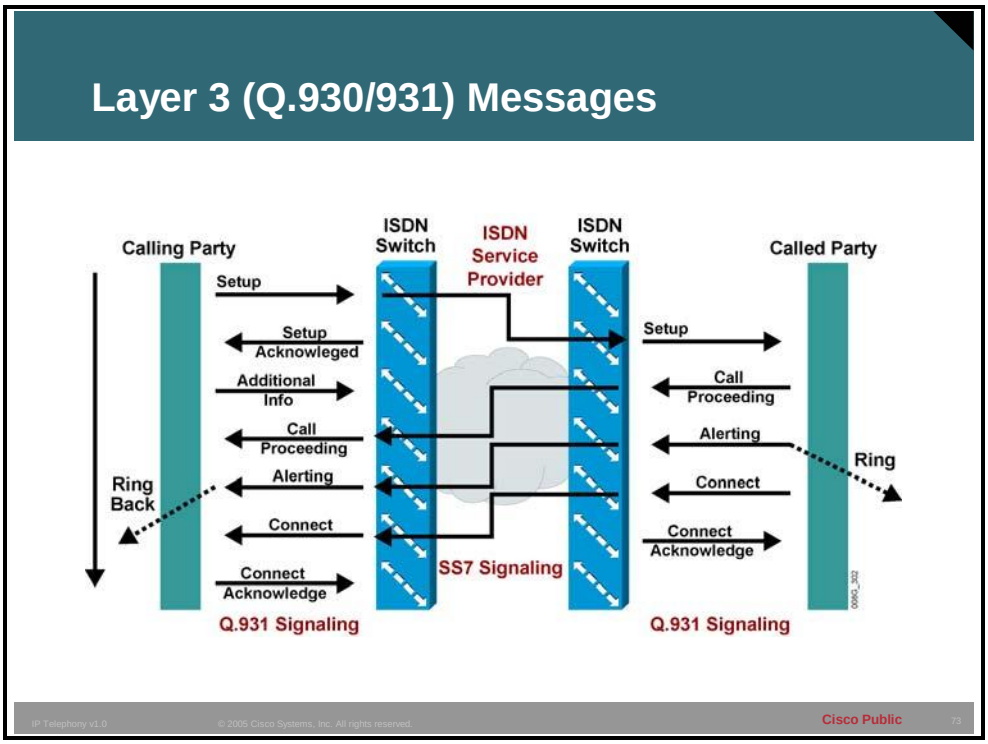
The figure here depicts the architecture of an ISDN network. The B channel carries information, such as voice, data, and video, at 64-kbps DS0.

The D channel carries call signaling between customer premises equipment (CPE) and the network, usually as the Q.931 protocol but sometimes as the QSIG protocol.

BRI operates using the average local copper pair. It uses two B channels and one signaling channel. It is represented as 2 B+D.

PRI implemented on T1 uses 23 B channels and one signaling channel. It is represented as 23 B+D. PRI implemented on E1 uses 30 B channels and one signaling channel. It is represented as 30 B+D.

 Copyright © 2005, Cisco Systems, Inc.



Layer 3, Q.931, uses a standard set of messages to communicate. These standard commands cover the following areas:

- **Call establishment:** Initially sets up a call. Messages travel between the user and the network. Call establishment events include alerting, call proceeding, connect, connect acknowledgment, progress, setup, and setup acknowledgment.
- **Call information phase:** Data sent between the user and the network after the call is established. This allows the user to, for example, suspend and then resume a call. Events in the call information phase include: hold, hold acknowledgment, hold reject, resume, resume acknowledgment, resume reject, retrieve, retrieve acknowledgment, retrieve reject, suspend, suspend acknowledgment, suspend reject, and user information.
- **Call clearing:** Terminates a call. The following events occur in the call-clearing phase: disconnect, release, release complete, restart, and restart acknowledgment.
- **Miscellaneous messages:** Negotiates network features (supplementary services). Miscellaneous services include congestion control, facility, information, notify, register, status, and status inquiry.

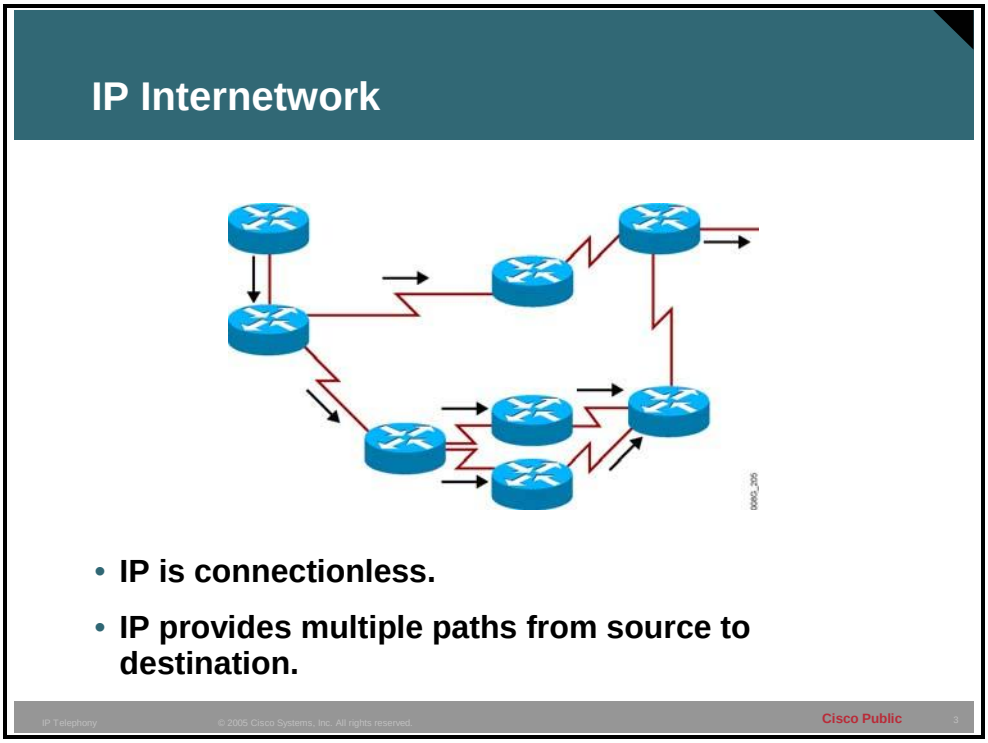
Example: ISDN Messages

ISDN Layer 3 messages, or Q.931, are carried within ISDN Layer 2 frames, called Q.921. Cisco ISDN equipment allows the administrator to monitor these messages as they occur using various **debug** commands.

Requirements of Voice in an IP Internetwork

Real-Time Voice in a Best-Effort IP Internetwork

This topic lists problems associated with implementation of real-time voice traffic in a best-effort IP internetwork.



The traditional telephony network was originally designed to carry voice. The design of circuit-switched calls provides a guaranteed path and a delay threshold between source and destination. The IP network was originally designed to carry data. Data networks were not designed to carry voice traffic. Although data traffic is best-effort traffic and can withstand some amount of delay, jitter, and loss, voice traffic is real-time traffic that requires a certain quality of service (QoS). In the absence of any special QoS parameters, a voice packet is treated as just another data packet.

The user must have a well-engineered network, end to end, when running delay-sensitive applications such as VoIP. Fine-tuning the network to adequately support VoIP involves a series of protocols and features geared toward QoS.

Example: Real-Time Voice Delivery Issues

In the IP network shown in the figure, voice packets that enter the network at a constant rate can reach the intended destination by a number of routes. Because each of these routes may have different delay characteristics, the arrival rate of the packets may vary. This condition is called jitter.

Another effect of multiple routes is that voice packets can arrive out of order. The far-end voice-enabled router or gateway has to re-sort the packets and adjust the interpacket interval for a proper-sounding voice playout.

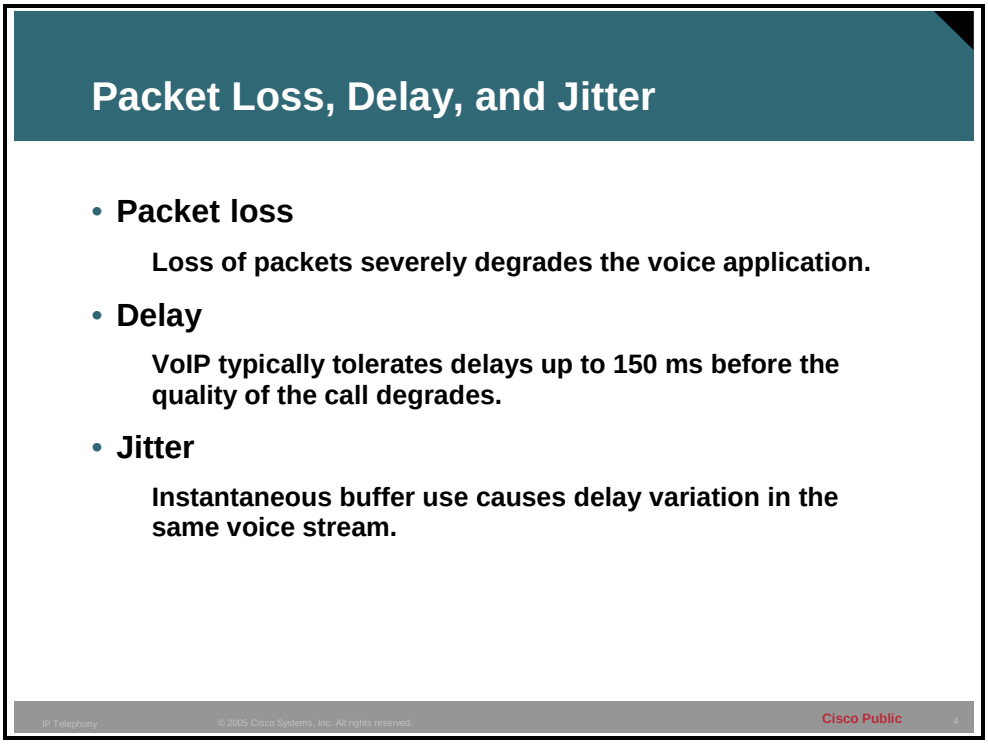
Network transmission adds corruptive effects like noise, delay, echo, jitter, and packet loss to the speech signal. VoIP is susceptible to these network behaviors, which can degrade the voice application.

If a VoIP network is to provide the same quality that users have come to expect from traditional telephony services, then the network must ensure that the delay in transmitting a voice packet across the network, and the associated jitter, does not exceed specific thresholds.

 Copyright © 2005, Cisco Systems, Inc.

Packet Loss, Delay, and Jitter

This topic discusses the causes of packet loss, end-to-end delay, and jitter delay in an IP internetwork.



In traditional telephony networks, voice has a guaranteed delay across the network by strict bandwidth association with each voice stream. Configuring voice in a data network environment requires network services with low delay, minimal jitter, and minimal packet loss. Over the long term, packet loss, delay, and jitter will all affect voice quality, as follows:

- **Packet loss:** The IP network may drop voice packets if the network quality is poor, if the network is congested, or if there is too much variable delay in the network. Codec algorithms can correct small amounts of loss, but too much loss can cause voice clipping and skips. The chief cause of packet loss is network congestion.
- **Delay:** End-to-end delay is the time that it takes the sending endpoint to send the packet to the receiving endpoint. End-to-end delay consists of the following two components:
  - **Fixed network delay:** You should examine fixed network delay during the initial design of the VoIP network. The International Telecommunication Union (ITU) standard G.114 states that a one-way delay budget of 150 ms is acceptable for high-quality voice. Research at Cisco Systems has shown that there is a negligible difference in voice quality scores using networks built with 200-ms delay budgets. Examples of fixed network delay include propagation delay of signals between the sending and receiving endpoints, voice encoding delay, and voice packetization time for various VoIP codecs.

- **Variable network delay:** Congested egress queues and serialization delays on network interfaces can cause variable packet delays. Serialization delay is a constant function of link speed and packet size. The larger the packet and the slower the link-clocking speed, the greater the serialization delay. Although this ratio is known, it can be considered variable because a larger data packet can enter the egress queue at any time before a voice packet. If the voice packet must wait for the data packet to serialize, the delay incurred by the voice packet is its own serialization delay, plus the serialization delay of the data packet in front of it.

- **Jitter:** Jitter is the variation between the expected arrival of a packet and when it is actually received. To compensate for these delay variations between voice packets in a conversation, VoIP endpoints use jitter buffers to turn the delay variations into a constant value so that voice can be played out smoothly. Buffers can fill instantaneously, however, because network congestion can be encountered at any time within a network. This instantaneous buffer use can lead to a difference in delay times between packets in the same voice stream.

Example: Packet Loss, Delay, and Jitter Problems

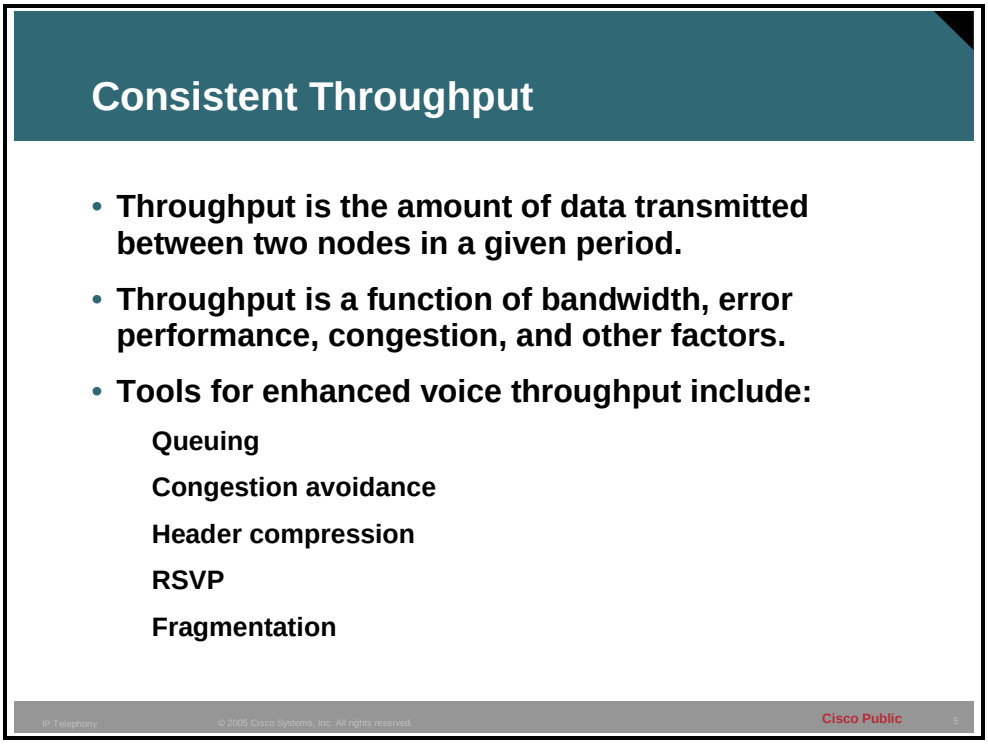
The effect of end-to-end packet loss, delay, and jitter can be heard as follows:

- The calling party says, “Good morning, how are you?”
- With end-to-end delay, the called party hears, “……Good morning, how are you?”
- With jitter, the called party hears, “Good……morning, how……are you?”
- With packet loss, the called party hears, “Good m..ning, w are you?”

 Copyright © 2005, Cisco Systems, Inc.

Consistent Throughput

This topic describes the methods that you can use to ensure consistent delivery and throughput of voice packets in an IP internetwork.



Throughput is the actual amount of useful data that is transmitted from a source to a destination. The amount of data that is placed in the pipe at the originating end is not necessarily the same amount of data that comes out at the destination. The data stream may be affected by error conditions in the network; for example, bits may be corrupted in transit, leaving the packet unusable. Packets may also be dropped during times of congestion, potentially forcing a retransmit, using twice the amount of bandwidth for that packet.

In the traditional telephony network, voice had guaranteed bandwidth associated with each voice stream. Cisco IOS software uses a number of techniques to reliably deliver real-time voice traffic across the modern data network. These techniques, which all work together to ensure consistent delivery and throughput of voice packets, include the following:

- **Queuing:** The act of holding packets so that they can be handled with a specific priority when leaving the router interface. Queuing enables routers and switches to handle bursts of traffic, measure network congestion, prioritize traffic, and allocate bandwidth. Cisco routers offer several different queuing mechanisms that can be implemented based on traffic requirements. Low Latency Queuing (LLQ) is one of the newest Cisco queuing mechanisms.
- **Congestion avoidance:** Congestion avoidance techniques monitor network traffic loads. The aim is to anticipate and avoid congestion at common network and internetwork bottlenecks before it becomes a problem. These techniques provide preferential treatment under congestion situations for premium (priority) class traffic, such as voice. At the same time, these techniques maximize network throughput and capacity use and minimize packet loss and delay. Weighted random early detection (WRED) is one of the QoS congestion avoidance mechanisms used in Cisco IOS software.

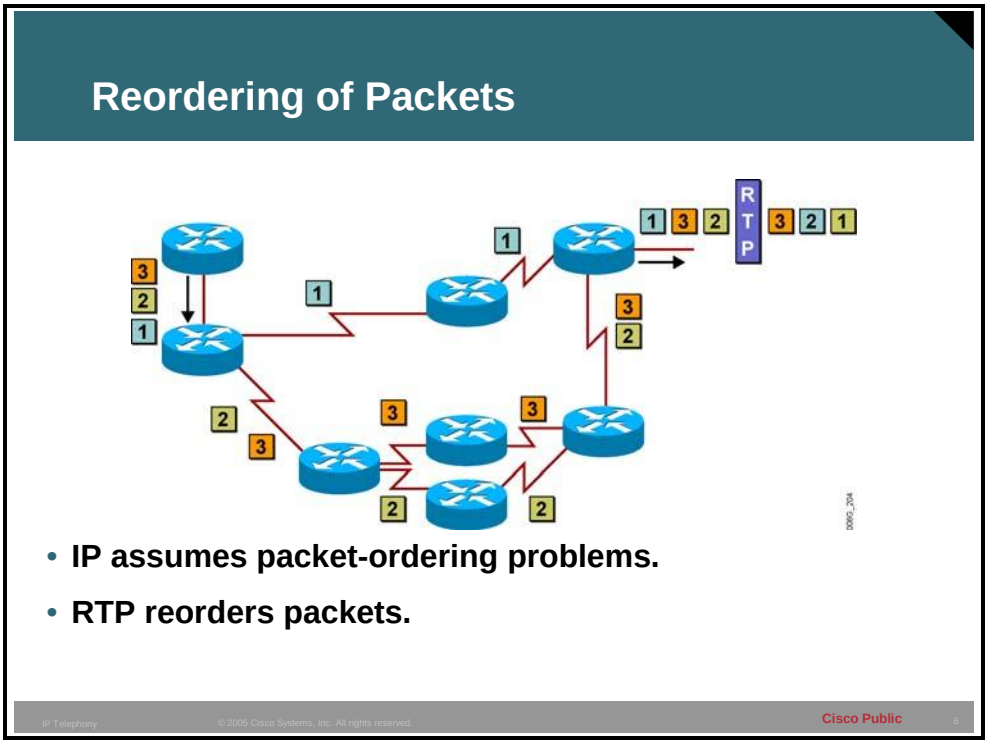
- **Header compression:** In the IP environment, voice is carried in Real-Time Transport Protocol (RTP), which is carried in User Datagram Protocol (UDP), which is then put inside an IP packet. This constitutes 40 bytes of RTP/UDP/IP header. This header size is large when compared to the typical voice payload of 20 bytes. Compressed RTP (CRTP) reduces the headers to 2 bytes in most cases, thus saving considerable bandwidth and providing for better throughput.
- **Resource Reservation Protocol:** Resource Reservation Protocol (RSVP) is a transport layer protocol that enables a network to provide differentiated levels of service to specific flows of data. Unlike routing protocols, RSVP is designed to manage flows of data rather than make decisions for each individual datagram. Data flows consist of discrete sessions between specific source and destination machines. Hosts use RSVP to request a QoS level from the network on behalf of an application data stream. Routers use RSVP to deliver QoS requests to other routers along the paths of the data stream. After an RSVP reservation is made, weighted fair queuing (WFQ) is the mechanism that actually delivers the queue space at each device. Voice calls in the IP environment can request RSVP service to provide guaranteed bandwidth for a voice call in a congested environment.
- **Fragmentation:** Fragmentation defines the maximum size for a data packet and is used in the voice environment to prevent excessive serialization delays. Serialization delay is the time that it takes to actually place the bits onto an interface; for example, a 1500-byte packet takes 187 ms to leave the router over a 64-kbps link. If a best-effort data packet of 1500 bytes is sent, real-time voice packets are queued until the large data packet is transmitted. This delay is unacceptable for voice traffic. However, if best-effort data packets are fragmented into smaller pieces, they can be interleaved with real-time (voice) packets. In this way, both voice and data packets can be carried together on low-speed links without causing excessive delay to the real-time voice traffic.

There are many QoS tools that can be used to ensure consistent throughput. When these mechanisms are employed, voice traffic on the network is assured priority and its delivery is more consistent.

 Copyright © 2005, Cisco Systems, Inc.

Reordering of Voice Packets

This topic describes how RTP ensures consistent delivery order of voice packets in an IP internetwork.



In traditional telephony networks, voice samples are carried in an orderly manner through the use of time-division multiplexing (TDM). Because the path is circuit-switched, the path between the source and destination is reserved for the duration of the call. All of the voice samples stay in order as they are transmitted across the wire. Because IP provides connectionless transport with the possibility of multiple paths between sites, voice packets cannot arrive out of order at the destination. Because voice rides in UDP/IP packets, there is no automatic reordering of packets.

RTP provides end-to-end delivery services for data that require real-time support, such as interactive voice and video. According to RFC 1889, the services provided by RTP include payload-type identification, sequence numbering, time stamping, and delivery monitoring.

Example: Reordering Voice Packets

In the figure, RTP reorders the voice packets through the use of sequence numbers before playing them out to the user.

The table illustrates the various stages of packet reordering by RTP.

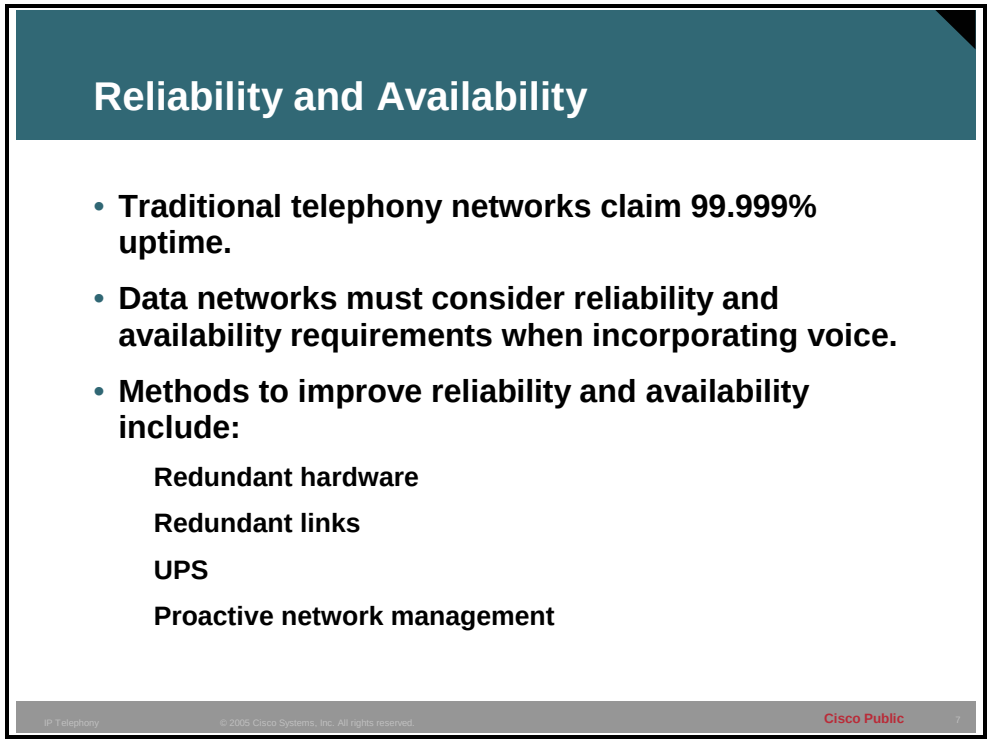
Sequencing of Packets by RTP

Stage	What Happens
Voice packets enter the network.	IP assumes packet-ordering problems.
RTP reorders the voice packets.	The voice packets are put in order through the use of sequence numbers.
RTP retimes the voice packets.	The voice packets are spaced according to the time stamp contained in each RTP header.
	The user hears the voice packets in order and with the same timing as when the voice stream left the source.
RTCP (Real-Time Transport Control Protocol) sends occasional report packet for delivery monitoring.	Both the sender and receiver send occasional report packets containing information, such as number of packets sent or received, the octet count, and the number of lost packets.

 Copyright © 2005, Cisco Systems, Inc.

Reliability and Availability

The traditional telephony network strives to provide 99.999 percent uptime to the user. This corresponds to 5.25 minutes per year of downtime. Many data networks cannot make the same claim. This topic describes methods that you can use to improve reliability and availability in data networks.



To provide telephony users the same—or close to the same—level of service as they experience with traditional telephony, the reliability and availability of the data network takes on new importance.

Reliability is a measure of how resilient a network can be. Efforts to ensure reliability may include choosing hardware and software with a low mean time between failure, or installing redundant hardware and links. Availability is a measure of how accessible the network is to the users. When a user wants to make a call, for example, the network should be accessible to that user at any time a call is required. Efforts to ensure availability may include installing proactive network management to predict failures before they happen, and taking steps to correct problems in design of the network as it grows.

When the data network goes down, it may not come back up for minutes or even hours. This delay is unacceptable for telephony users. Local users with network equipment, such as voice-enabled routers, gateways, or switches for IP Phones, now find that their connectivity is terminated. Administrators must, therefore, provide an uninterruptible power supply (UPS) to these devices in addition to providing network availability. Previously, depending on the type of connection the user had, they received their power directly from the telephone company central office (CO) or through a UPS that was connected to their keyswitch or PBX in the event of a power outage. Now the network devices must have protected power to continue to function and provide power to the end devices.

Network reliability comes from incorporating redundancy into the network design. In traditional telephony, switches have multiple redundant connections to other switches. If either

a link or a switch becomes unavailable, the telephone company can route the call in different ways. This is why telephone companies can claim a high availability rate.

High availability encompasses many areas of the network. In a fully redundant network, the following components need to be duplicated:

- Servers and call managers
- Access layer devices, such as LAN switches
- Distribution layer devices, such as routers or multilayer switches
- Core layer devices, such as multilayer switches
- Interconnections, such as WAN links and public switched telephone network (PSTN) gateways, even through different providers
- Power supplies and UPSs

Example: Cisco Reliability and Availability

In some data networks, a high level of availability and reliability is not critical enough to warrant financing the hardware and links required to provide complete redundancy. If voice is layered onto the network, these requirements need to be revisited.

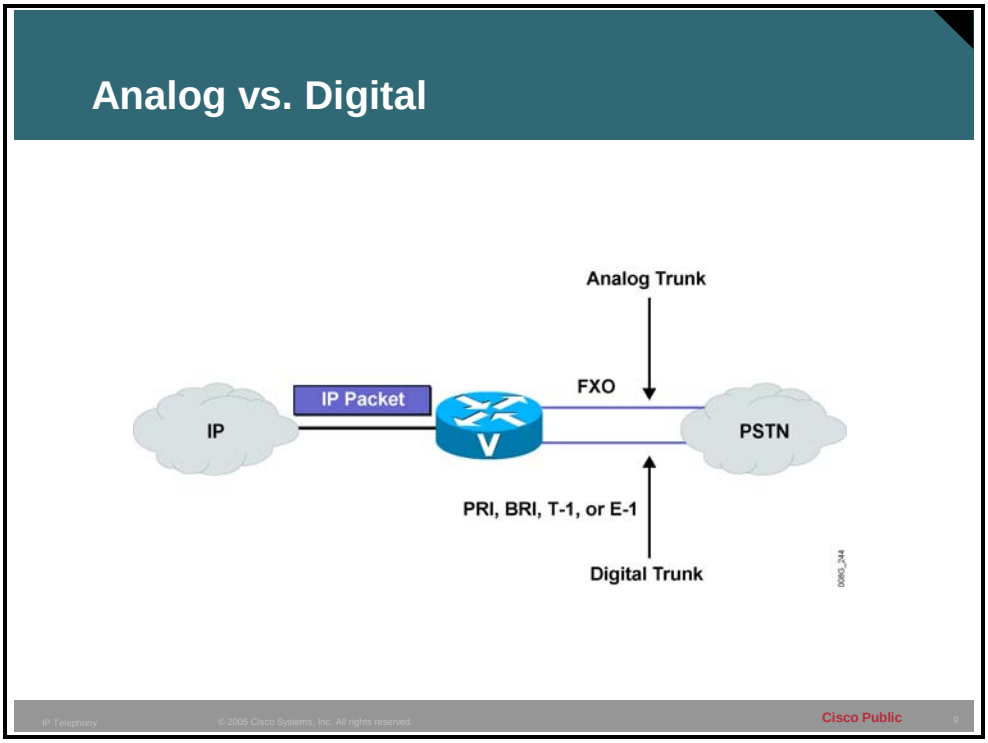
With Cisco Architecture for Voice, Video and Integrated Data (AVVID) technology, the use of Cisco CallManager clusters provides a way to design redundant hardware in the event of Cisco CallManager failure. When using gatekeepers, you can configure backup devices as secondary gatekeepers in case the primary gatekeeper fails. You must also revisit the network infrastructure. Redundant devices and Cisco IOS services, like Hot Standby Router Protocol (HSRP), can provide high availability. For proactive network monitoring and trouble reporting, a network management platform such as CiscoWorks2000 provides a high degree of responsiveness to network issues.

 Copyright © 2005, Cisco Systems, Inc.

Gateways and Their Roles

Understanding Gateways

This topic describes the role of voice gateways and their application when connecting VoIP to traditional PSTN and telephony equipment.



A gateway is a device that translates one type of signal to a different type of signal. There are different types of gateways, including the voice gateway.

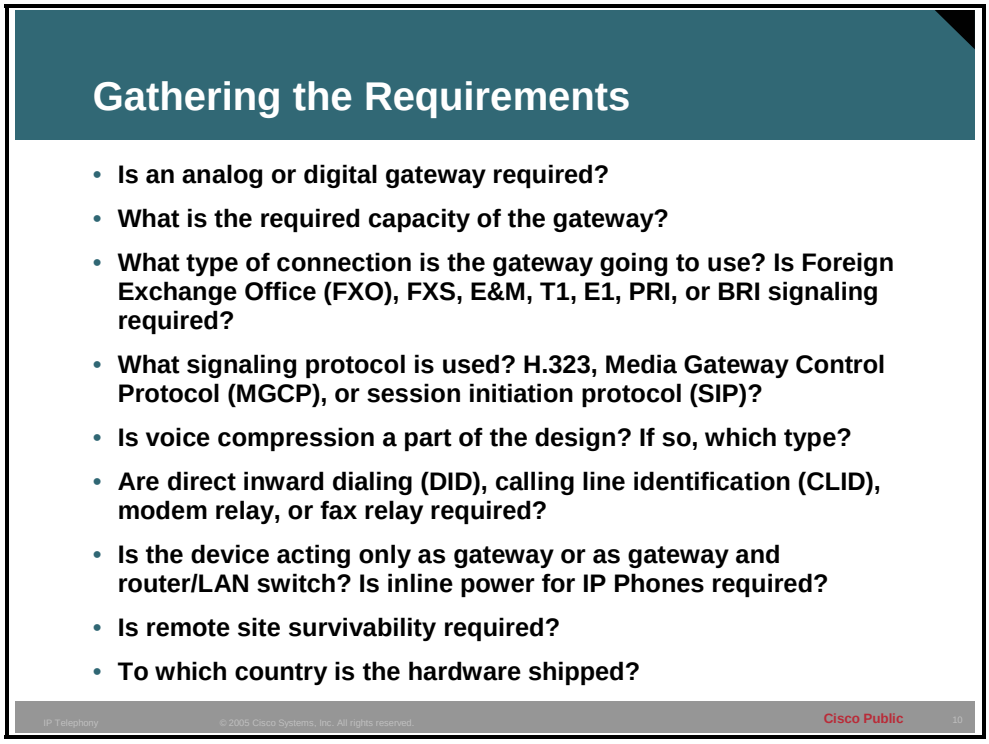
A voice gateway is a router or switch that converts IP voice packets to analog or digital signals that are understood by TDM trunks or stations. Gateways are used in several situations; for example, to connect the PSTN, a PBX, or a key system to a VoIP network.

Example: Analog and Digital Gateways

In the figure, the voice-enabled router examines the incoming IP packet to determine if it is a voice packet and where it is heading. Based on information inside the voice packet, the router translates the digitized signal or voice into the appropriate analog or digital signal to be sent to the PSTN. For a call coming from the PSTN, the gateway interprets the dialed digits and determines the IP destination for this call.

Guidelines for Selecting the Correct Gateway

This topic describes the guidelines for selecting the correct gateway.



Understanding gateways and being able to select the correct gateway out of numerous gateway options is challenging. Factors to consider include the protocols that are supported, the density and types of interfaces on the gateway, and the features that are required. Knowing the requirements will guide you to the correct solution.

One criterion involves defining the type of site that the gateway supports. Is it a small office/home office (SOHO), branch office, enterprise campus environment, or service provider? Each type of site has its own set of requirements.

The figure lists the questions that you should be asking before selecting a gateway. The answers will help to define the gateway functions and determine if the proposed design meets current requirements and encompasses future growth.

A key step is identifying the number and type of voice interfaces that are necessary and verifying the protocol support. Are supplementary services supported? Which codecs must be supported? Is fax relay necessary? Many of these functions are features of specific Cisco IOS software releases. Identification of the proper IOS software release that is necessary to support the features is critical.

Another key question is whether the gateway is acting as a gateway only or needs to combine the functions of gateway and router within one device. This, too, points to a specific set of hardware and software.

When planning gateways for location in other countries, verify that the device meets the government standards for PSTN connection in that country. Also, if the device supports encryption capabilities, verify the legality of export to the destination country.

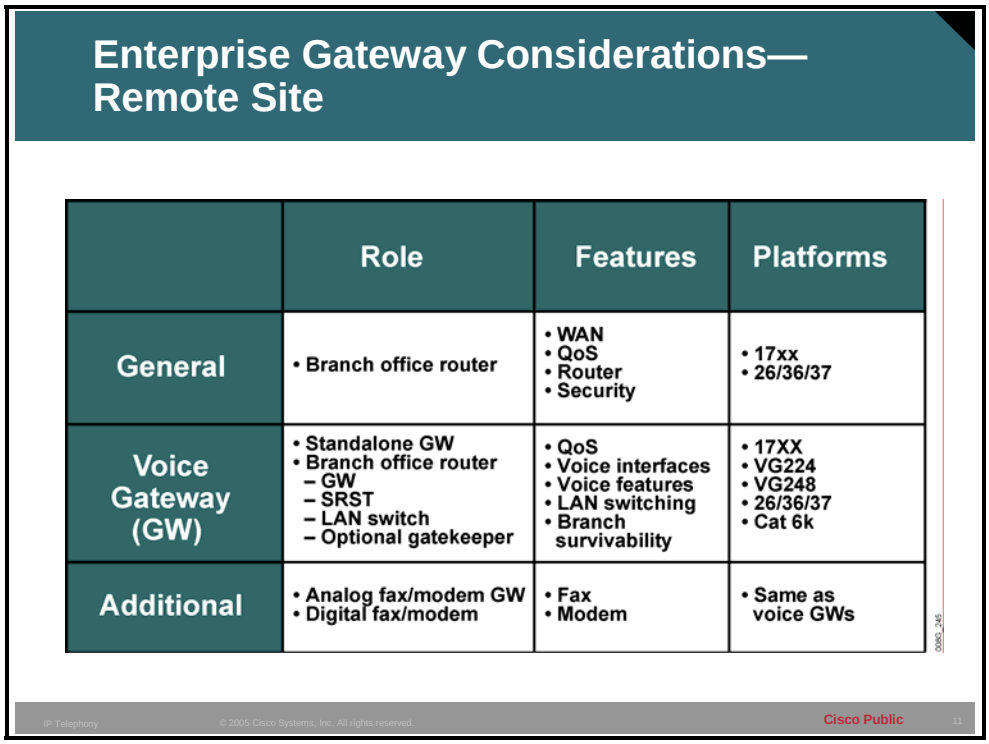
 Copyright © 2005, Cisco Systems, Inc.

Example: Selecting a Gateway

For example, if the requirements are to support Foreign Exchange Station (FXS) and recEive and transMit (E&M) connections, as well as T1 PRI from the PBX, then a suitable choice would be a Cisco 3745 Multiservice Access Router with a two-slot voice network module (VNM), 1 FXS voice interface card (VIC), 1 E&M VIC, and a High Density Voice (HDV) module.

Determining Gateway Interconnection Requirements in an Enterprise Environment, Central and Remote Site

This topic describes the guidelines for determining gateway interconnection requirements in an enterprise environment for both central and remote sites.



As IP telephony services become a standard in the corporate environment, a broad mix of requirements surface in the enterprise environment. The IP telephony deployment typically begins by connecting to the PSTN to manage off-net calls and using a Cisco CallManager infrastructure to manage on-net calls.

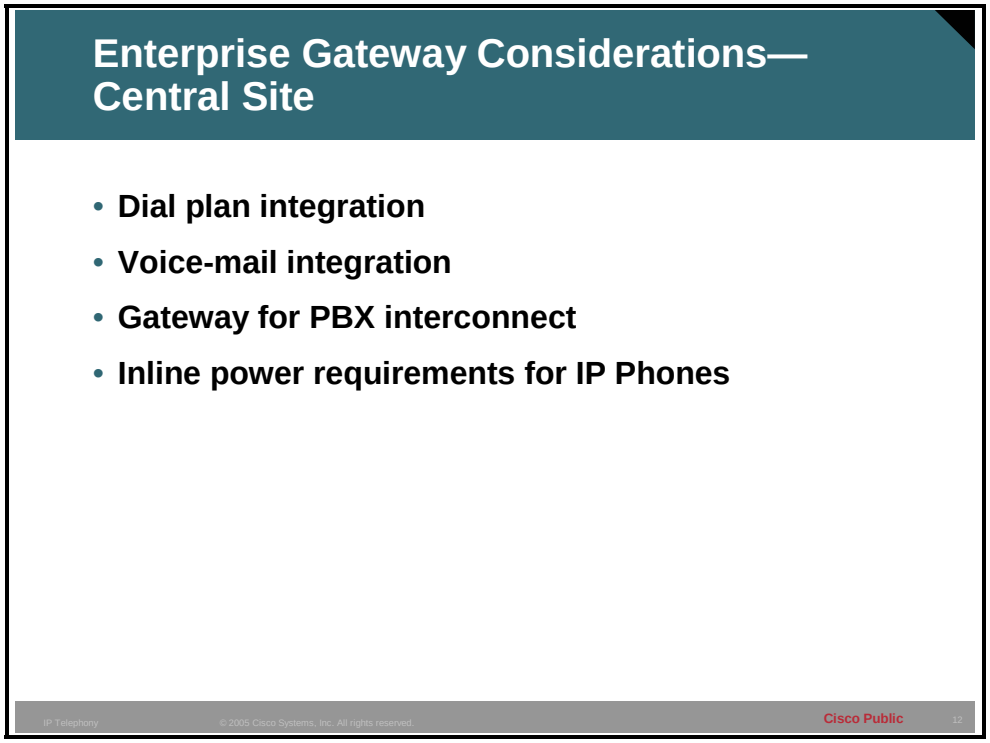
Example: Gateway Interconnect Considerations

The table shows examples of questions that you must ask to determine the requirements for gateway interconnections.

 Copyright © 2005, Cisco Systems, Inc.

Determining Gateway Interconnection Requirements

Question	Reasoning
How do you control the gateways?	You must ensure support for proper call processing, such as Media Gateway Control Protocol (MGCP), session initiation protocol (SIP), or H.323.
Is cost an issue?	Distributed call processing is easier to implement, but costs are higher when deploying intelligent devices at each site.
Is remote site survivability an issue?	Remote site survivability is not an issue with a distributed model unless there is a need for redundancy. This is an issue for a centralized model that must be addressed by providing Survivable Remote Site Telephony (SRST). This means ensuring that the version of Cisco IOS software supports the feature.
Are gatekeepers in the design, and if so, how are the zones structured?	Gatekeepers are normally used in enterprise sites for scalability and manageability. The design must include proper planning for zone configurations.
Are the gateways switches or routers?	This question determines how other features, such as QoS, are implemented. Numerous switches and routers are available that have voice gateway functionality along with other core services. These services include Layer 2 and Layer 3 QoS implementations, inline power, and security features.
Is fax or modem support required?	This requirement means the gateway must be capable of fax and modem relay functions. Another option for the enterprise customer may be to purchase IP telephony services from a service provider. In that case, a decision must be made regarding who manages the gateway and what type of connection is required; for example, SIP, H.323, or MGCP.



At the central site, the specific issues that need to be addressed include the following:

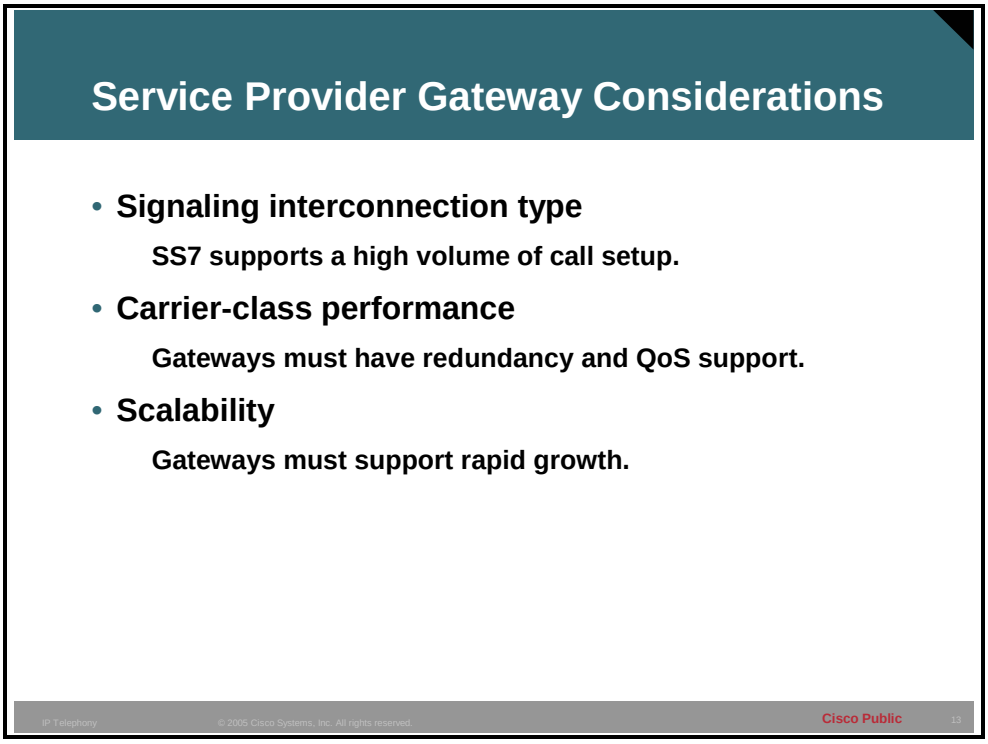
- **Dial plan integration:** For consistent reachability, the new dial plan for the IP voice network must integrate with the existing dial plan. It is essential that you have a thorough understanding of how the dial plans interact.
- **Voice-mail integration:** After a voice-mail application is selected, the designer must ensure that all users can seamlessly reach the voice-mail server and that all incoming calls are properly forwarded when the recipient does not answer the telephone. This may mean dedicating gateway connections for an existing voice mail server, or dedicating an entire gateway for the express purpose of voice mail server integration.
- **Gateway for PBX interconnect:** When the IP voice network interconnects PBXs, the designer must determine what type of connection is supported by the PBX and which gateway will support that connection.
- **Inline power requirements for IP Phones:** Beyond the gateway, when the design includes IP Phones, the power requirements must be considered. In many cases, it is desirable to provide inline power to the telephones. A number of devices provide inline power. The decision about inline power requirements is based on capacity and the current power options.

Note	The network administrator should evaluate the need for inline power depending on the network design.

 Copyright © 2005, Cisco Systems, Inc.

Determining Gateway Interconnection Requirements in a Service Provider Environment

This topic provides the gateway interconnection requirements in service provider environments.



Service providers must provide a level of service that meets or exceeds PSTN standards. The gateways that service providers implement must provide for reliable, high-volume voice traffic with acceptable levels of latency and jitter. The following functions address those requirements:

- **Signaling interconnection type:** Signaling System 7 (SS7) interconnect supports a high volume of call setup and benefits from redundant interconnect capabilities directly into the PSTN switch network.
- **Carrier-class performance:** Carrier-class performance can be provided through the proper redundant design for high availability in addition to the proper implementation of QoS features to ensure acceptable delay and jitter.
- **Scalability:** Scalability is a critical factor in the service provider arena. Customers who need access should be serviced promptly. Choosing a gateway with capacity for rapid growth is an important design decision. Gateways can scale upward to T3 capabilities for large-scale environments.

Example: Service Provider Requirements

An IP telephony service provider needs to upgrade their existing gateway platforms because of business growth. The service provider sells a managed IP telephony service to small and medium businesses and provides connections to many different low-cost, long-distance carriers for their customers. Their issues are call quality over the IP network, so delay and jitter need to be controlled. Service providers also must consider scalability and the ability to provide differentiated levels of service through QoS. They also need connectivity to SS7 networks of long-distance carriers to reduce costs, and, finally, they need to consider the overall cost of

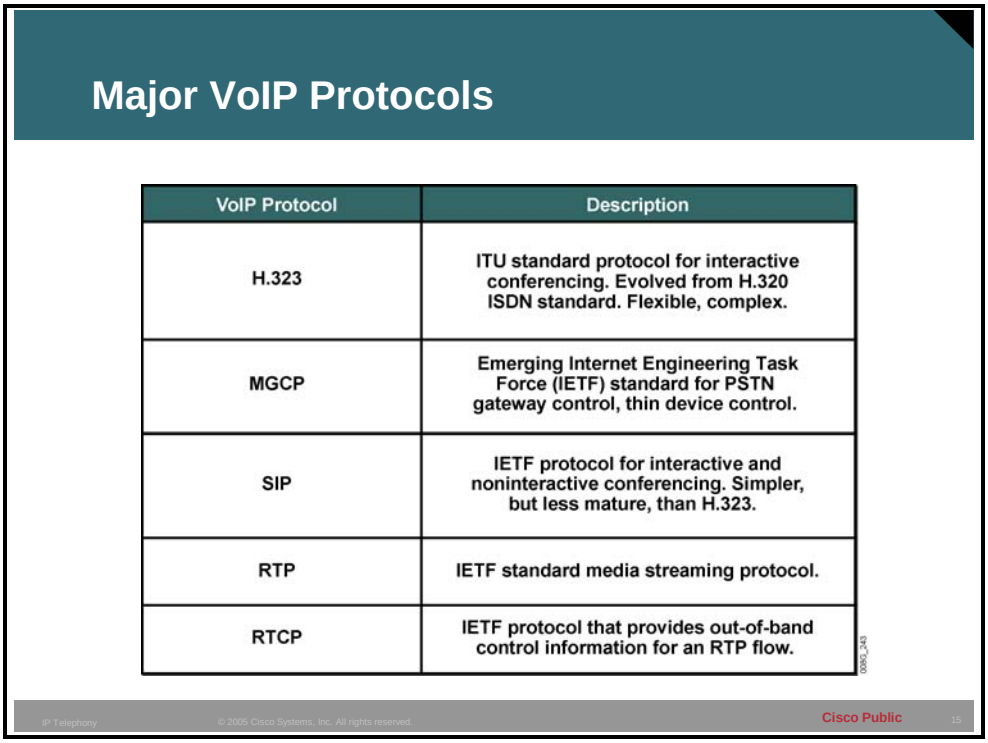
implementation. SS7 capabilities and a redundant design enable the service provider to deliver a reliable level of service.

 Copyright © 2005, Cisco Systems, Inc.

Encapsulating Voice in IP Packets

Major VoIP Protocols

This topic defines the major VoIP protocols and matches them with the seven layers of the OSI model.



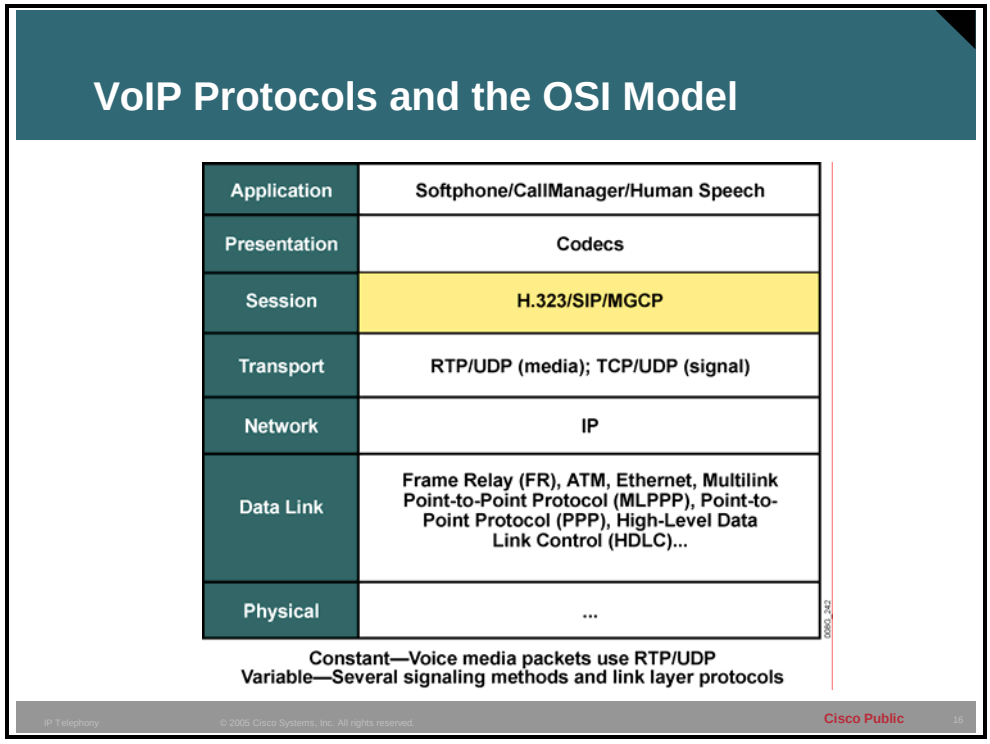
The major VoIP protocols include the following:

- **H.323:** An ITU standard protocol for interactive conferencing. The ITU standard protocol was originally designed for multimedia in a connectionless environment, such as a LAN. The H.323 is an umbrella of standards that defines all aspects of synchronized voice, video, and data transmission. H.323 defines end-to-end call signaling.
- **MGCP:** An emerging standard for PSTN gateway control or thin device control. Specified in RFC 2705, MGCP defines a protocol to control VoIP gateways connected to external call-control devices, referred to as call agents. MGCP provides the signaling capability for less expensive edge devices, such as gateways, that may not contain a full voice-signaling stack, such as H.323. In essence, any time an event such as off hook occurs at the voice port of a gateway, the voice port reports that event to the call agent. The call agent then signals that device to provide a service, such as dial-tone signaling.
- **SIP:** A detailed protocol that specifies the commands and responses to set up and tear down calls. It also details features such as security, proxy, and transport (TCP or UDP) services. SIP and its partner protocols, Session Announcement Protocol (SAP) and Session Description Protocol (SDP), provide announcements and information about multicast sessions to users on a network. SIP defines end-to-end call signaling between devices. SIP is a text-based protocol that borrows many elements of HTTP, using the same transaction request and response model, and similar header and response codes. It also adopts a

modified form of the URL-addressing scheme used within e-mail that is based on Simple Mail Transfer Protocol (SMTP).

- **RTP:** An Internet Engineering Task Force (IETF) standard media-streaming protocol. RTP carries the voice payload across the network. RTP provides sequence numbers and time stamps for the orderly processing of voice packets.
- **RTCP:** Provides out-of-band control information for an RTP flow. Every RTP flow has a corresponding RTCP flow that reports statistics on the call. RTCP is used for QoS reporting.

 Copyright © 2005, Cisco Systems, Inc.



Example: VoIP and the OSI Model

Successfully integrating connection-oriented voice traffic in a connectionless-oriented IP network requires enhancements to the signaling stack. In some ways, the user must make the connectionless network appear more connection-oriented.

Applications such as Cisco IP Softphone and Cisco CallManager provide the interface for users to originate voice at their PCs or laptops and convert and compress it before passing it to the network. If a gateway is used, a standard telephone becomes the interface to users, so human speech is the application.

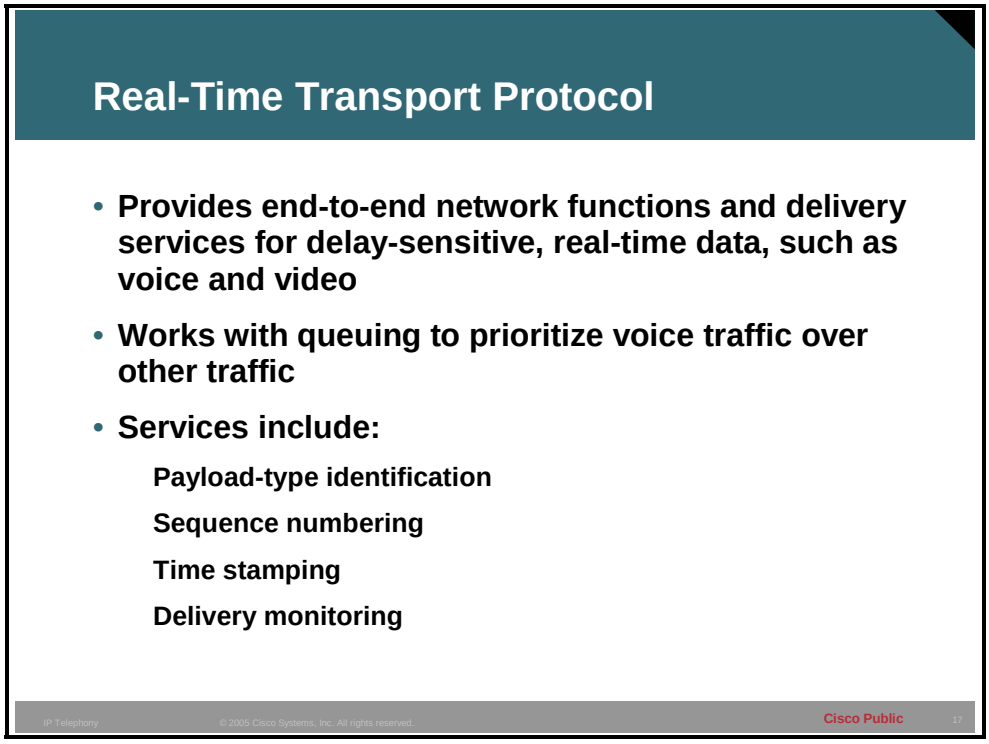
Codecs define how the voice is compressed. The user can configure which codec to use or a codec is negotiated according to what is available.

One of the constants in VoIP implementation is that voice uses RTP inside of UDP to carry the payload across the network. Because IP voice packets can reach the destination out of order and unsynchronized, the packets must be reordered and resynchronized before playing them out to the user. Since UDP does not provide services such as sequence numbers or time stamps, RTP provides sequencing functionality.

The variables in VoIP are the signaling methods used. H.323 and SIP define end-to-end call-signaling methods. MGCP defines a method to separate the signaling function from the voice call function. MGCP uses a call agent to control signaling on behalf of the endpoint devices, such as gateways. The central control device participates in the call setup only. Voice traffic still flows directly from endpoint to endpoint.

RTP and RTCP

This topic describes the functions of RTP and RTCP as they relate to the VoIP network.



RTP provides end-to-end network transport functions intended for applications transmitting real-time requirements, such as audio and video. Those functions include payload-type identification, sequence numbering, time stamping, and delivery monitoring.

RTP typically runs on top of UDP to use the multiplexing and checksum services of that protocol. Although RTP is often used for unicast sessions, it is primarily designed for multicast sessions. In addition to the roles of sender and receiver, RTP also defines the roles of translator and mixer to support the multicast requirements.

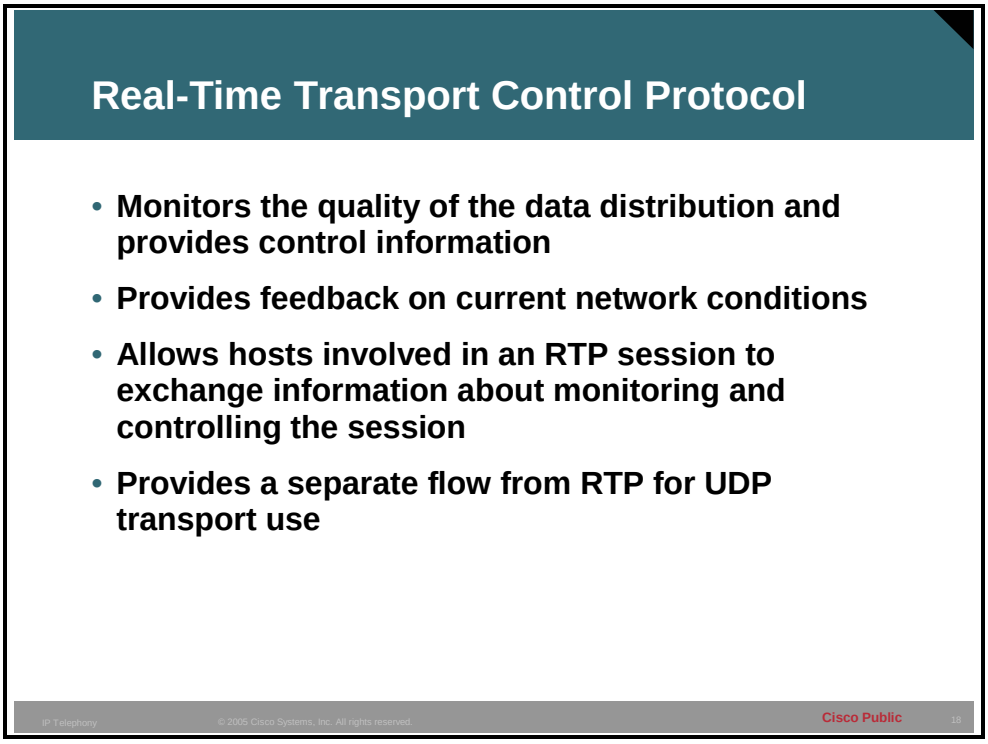
RTP is a critical component of VoIP because it enables the destination device to reorder and retime the voice packets before they are played out to the user. An RTP header contains a time stamp and sequence number, which allows the receiving device to buffer and remove jitter and latency by synchronizing the packets to play back a continuous stream of sound. RTP uses sequence numbers to order the packets only. RTP does not request retransmission if a packet is lost.

Example: RTP Application

As voice packets are placed on the network to reach a destination, they may take one or more paths to reach their destination. Each path may have a different length and transmission speed, resulting in the packets being out of order when they arrive at their destination. As the packets were placed on the wire at the source of the call, RTP tagged the packets with a time stamp and sequence number. At the destination, RTP can reorder the packets and send them to the digital signal processor (DSP) at the same pace as they were placed on the wire at the source.

Note For more information on RTP, refer to RFC 1889.

 Copyright © 2005, Cisco Systems, Inc.



RTCP monitors the quality of the data distribution and provides control information. RTCP provides the following feedback on current network conditions:

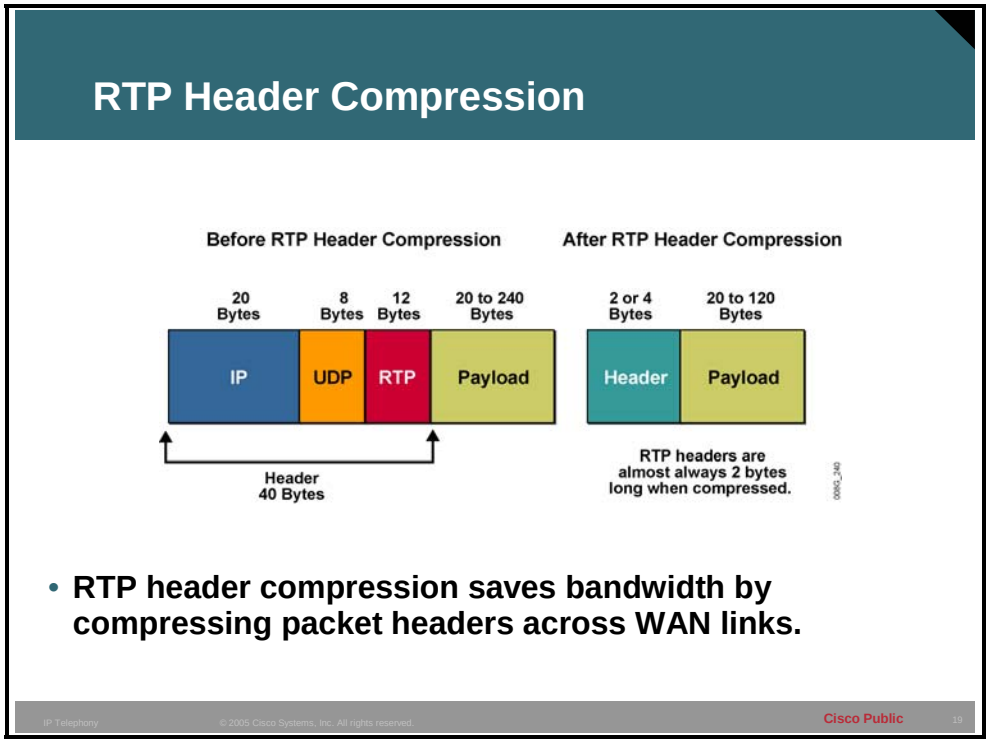
- RTCP provides a mechanism for hosts involved in an RTP session to exchange information about monitoring and controlling the session. RTCP monitors the quality of elements such as packet count, packet loss, delay, and interarrival jitter. RTCP transmits packets as a percentage of session bandwidth, but at a specific rate of at least every 5 seconds.
- The RTP standard states that the Network Time Protocol (NTP) time stamp is based on synchronized clocks. The corresponding RTP time stamp is randomly generated and based on data-packet sampling. Both NTP and RTP are included in RTCP packets by the sender of the data.
- RTCP provides a separate flow from RTP for transport use by UDP. When a voice stream is assigned UDP port numbers, RTP is typically assigned an even-numbered port and RTCP is assigned the next odd-numbered port. Each voice call has four ports assigned: RTP plus RTCP in the transmit direction and RTP plus RTCP in the receive direction.

Example: RTCP Application

Throughout the duration of each RTP call, the RTCP report packets are generated at least every 5 seconds. In the event of poor network conditions, a call may be disconnected due to high packet loss. When viewing packets using a packet analyzer, a network administrator could check information in the RTCP header that includes packet count, octet count, number of packets lost, and jitter. The RTCP header information would shed light on why the calls were disconnected.

Reducing Header Overhead with CRTP

This topic describes how IP voice headers are compressed using CRTP.



Given the number of protocols that are necessary to transport voice over an IP network, the packet header can be large. You can use CRTP headers on a link-by-link basis to save bandwidth.

Using CRTP compresses the IP/UDP/RTP header from 40 bytes to 2 bytes without UDP checksums and from 40 bytes to 4 bytes with UDP checksums. RTP header compression is especially beneficial when the RTP payload size is small; for example, with compressed audio payloads between 20 and 50 bytes.

In addition, CRTP works on the premise that most of the fields in the IP/UDP/RTP header do not change, or that the change is predictable. Static fields include source and destination IP address, source and destination UDP port numbers, as well as many other fields in all three headers. For those fields where the change is predictable, the CRTP process is illustrated in the following table:

CRTP

Stage	What Happens
The change is predictable.	The sending side tracks the predicted change.
The predicted change is tracked.	The sending side sends a hash of the header.
The receiving side predicts what the constant change is.	The receiving side substitutes the original stored header and calculates the changed fields.
There is an unexpected change.	The sending side sends the entire header without compression.

 Copyright © 2005, Cisco Systems, Inc.

CRTP Packet Components

In a packet voice environment when speech samples are framed every 20 ms, a payload of 20 bytes is generated. Without CRTP, the total packet size includes the following components:

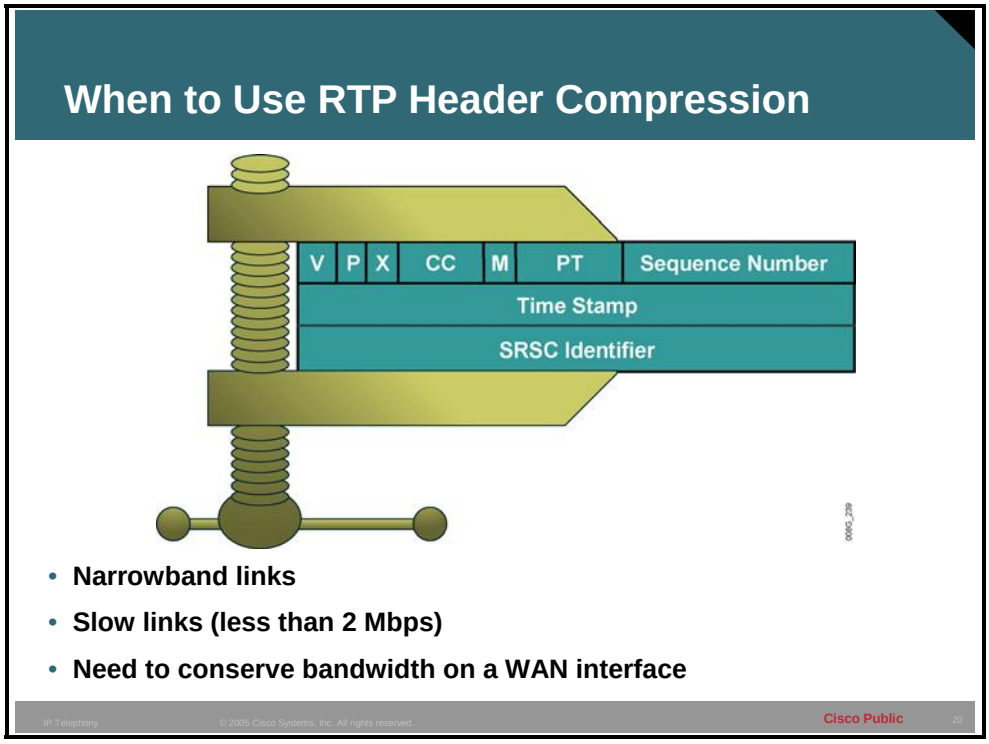
- IP header (20 bytes)
- UDP header (8 bytes)
- RTP header (12 bytes)
- Payload (20 bytes)

The header is twice the size of the payload: IP/UDP/RTP (20 + 8 + 12 = 40 bytes) versus payload (20 bytes). When generating packets every 20 ms on a slow link, the header consumes a large portion of bandwidth.

In the figure, RTP header compression reduces the header to 2 bytes. The compressed header is one tenth of the payload size.

When to Use RTP Header Compression

This topic describes when to use CRTP.



You must configure CRTP on a specific serial interface or subinterface if you have any of these conditions:

- Narrowband links
- Slow links (less than 2 Mbps)
- Need to conserve bandwidth on a WAN interface

Compression works on a link-by-link basis and must be enabled for each link that fits these requirements. You must enable compression on both sides of the link for proper results. Enabling compression on both ends of a low-bandwidth serial link can greatly reduce the network overhead if there is a significant volume of RTP traffic on that slow link.

Note	Compression adds to processing overhead. You must check resource availability on each device prior to turning on RTP header compression.

Example: Applying CRTP

If you want the router to compress RTP packets, use the **ip rtp header-compression** command. The **ip rtp header-compression** command defaults to active mode when it is configured. However, this command provides a passive mode setting in instances where you want the router to compress RTP packets *only* if it has received compressed RTP on that interface. When applying to a Frame Relay interface, use the **frame-relay ip rtp header-compression** command.

 Copyright © 2005, Cisco Systems, Inc.

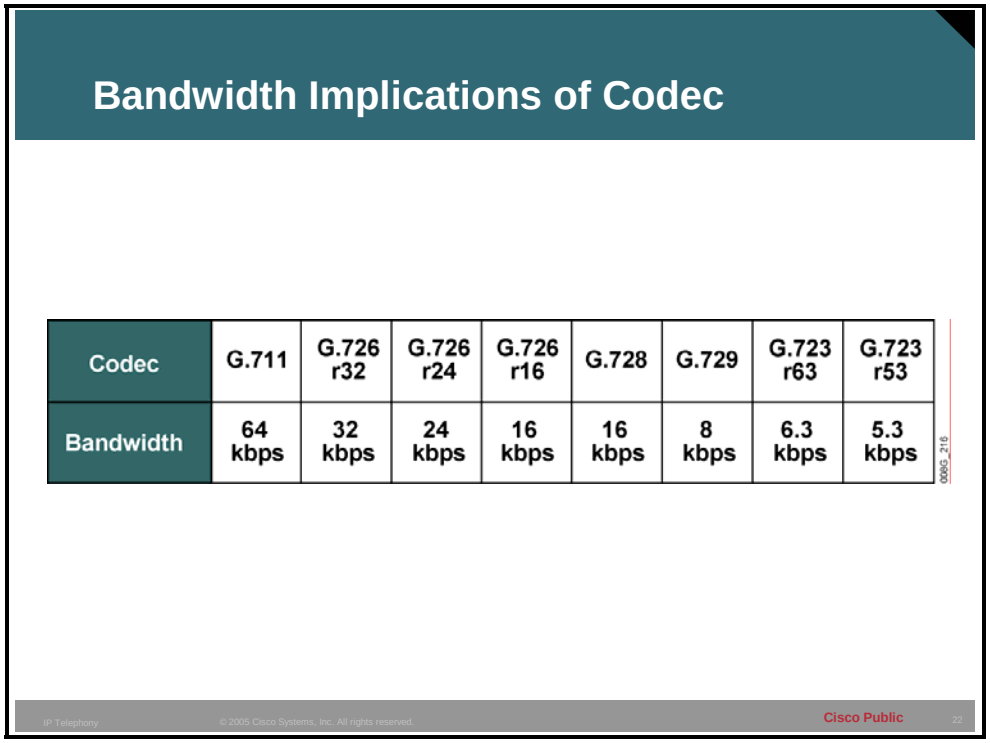
By default, the software supports a total of 16 RTP header compression connections on an interface. Depending on the traffic on the interface, you can change the number of header compression connections with the **ip rtp compression-connections** *number* command.

Note	Do not use CRTP if you have high-speed interfaces or links faster than 2 Mbps.

Calculating Bandwidth Requirements

Codec Bandwidths

This topic describes the bandwidth that each codec uses and illustrates its impact on total bandwidth.



One of the most important factors for the network administrator to consider while building voice networks is proper capacity planning. Network administrators must understand how much bandwidth is used for each VoIP call. With a thorough understanding of VoIP bandwidth, the network administrator can apply capacity-planning tools.

Following is a list of codecs and their associated bandwidth:

- **G.711:** The G.711 pulse code modulation (PCM) coding scheme uses the most bandwidth. It takes samples 8000 times per second, each of which is 8 bits in length, for a total of 64,000 bps.
- **G.726:** The G.726 adaptive differential pulse code modulation (ADPCM) coding schemes use somewhat less bandwidth. While each coding scheme takes samples 8000 times per second like PCM, it uses 4, 3, or 2 bits for each sample, thereby resulting in total bandwidths of 32,000, 24,000, or 16,000 bps.
- **G.728:** The G.728 low-delay code excited linear prediction (LDCELP) coding scheme compresses PCM samples using codebook technology. It uses a total bandwidth of 16,000 bps.
- **G.729:** The G.729 and G.729A Conjugate Structure Algebraic Code Excited Linear Prediction (CS-ACELP) coding scheme also compresses PCM using advanced codebook technology. It uses 8000 bps total bandwidth.

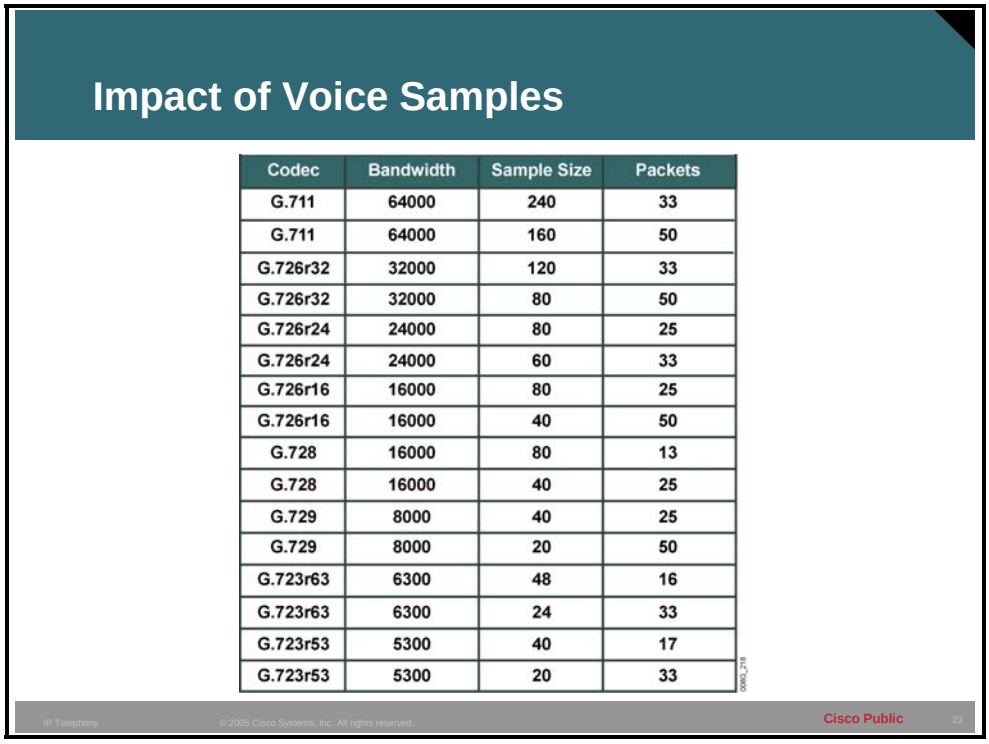
 Copyright © 2005, Cisco Systems, Inc.

- **G.723:** The G.723 and G.723A multipulse maximum likelihood quantization (MPMLQ) coding schemes use a look-ahead algorithm. These compression schemes result in 6300 or 5300 bps.

The network administrator should balance the need for voice quality against the cost of bandwidth in the network when choosing codecs. The higher the codec bandwidth, the higher the cost of each call across the network.

Impact of Voice Samples and Packet Size on Bandwidth

This topic illustrates the effect of voice sample size on bandwidth.



Voice sample size is a variable that can affect total bandwidth used. A voice sample is defined as the digital output from a codec DSP that is encapsulated into a protocol data unit (PDU). Cisco uses DSPs that output samples based on digitization of 10 ms-worth of audio. Cisco voice equipment encapsulates 20 ms of audio in each PDU by default, regardless of the codec used. You can apply an optional configuration command to the dial peer to vary the number of samples encapsulated. When you encapsulate more samples per PDU, total bandwidth is reduced. However, encapsulating more samples per PDU comes at the risk of larger PDUs, which can cause variable delay and severe gaps if PDUs are dropped.

Example: Encapsulated Bytes Calculation

Using a simple formula, it is possible for you to determine the number of bytes encapsulated in a PDU based on the codec bandwidth and the sample size (20 ms is default):

Bytes_per_Sample = (*Sample_Size* * *Codec_Bandwidth*) / 8

If you apply G.711 numbers, the formula reveals the following:

Bytes_per_Sample = (.020 * 64000) / 8

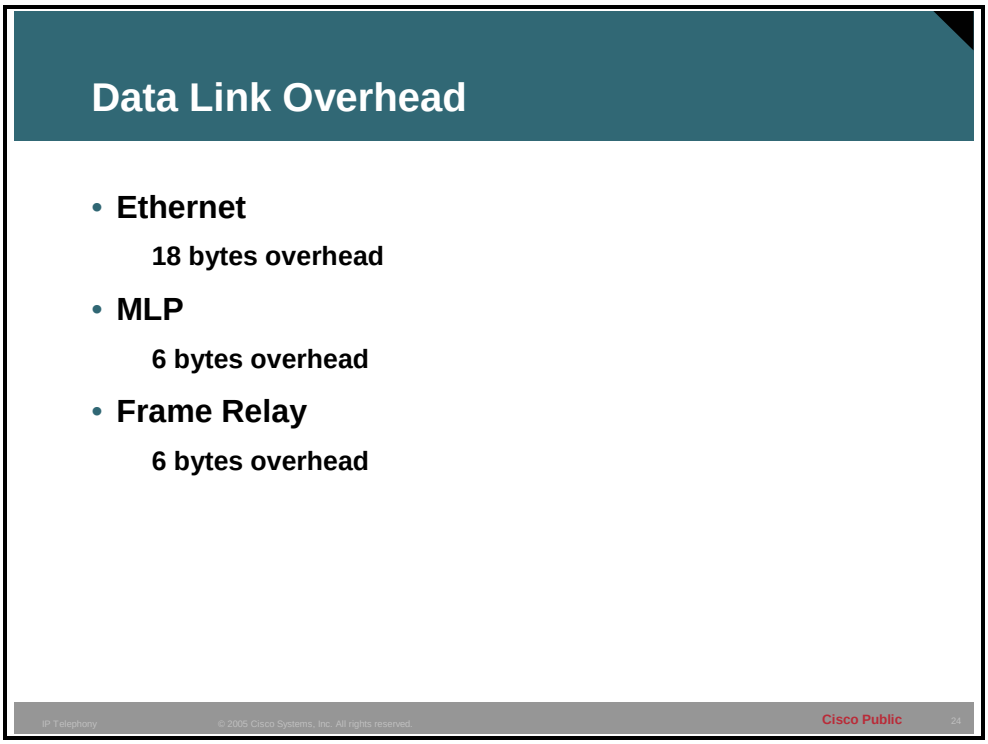
Bytes_per_Sample = 160

The figure illustrates various codecs and sample sizes and the number of packets that are required for VoIP to transmit one second of audio. The larger the sample size, the larger the packet, and the fewer the encapsulated samples that have to be sent (which reduces bandwidth).

 Copyright © 2005, Cisco Systems, Inc.

Data Link Overhead

This topic lists overhead sizes for various Layer 2 protocols.

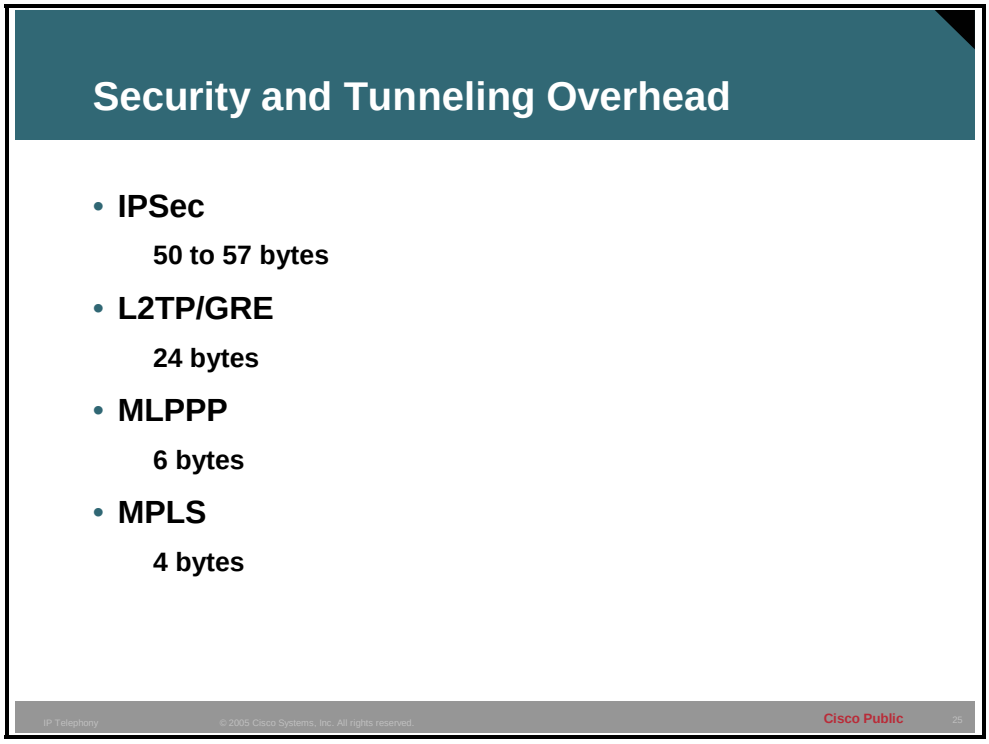


Another contributing factor to bandwidth is the Layer 2 protocol used to transport VoIP. VoIP alone carries a 40-byte IP/UDP/RTP header, assuming uncompressed RTP. Depending on the Layer 2 protocol used, the overhead could grow substantially. The larger the Layer 2 overhead, the more bandwidth required to transport VoIP. The following points illustrate the Layer 2 overhead for various protocols:

- **Ethernet II:** Carries 18 bytes of overhead; 6 bytes for source MAC, 6 bytes for destination MAC, 2 bytes for type, and 4 bytes for cyclic redundancy check (CRC)
- **Multilink Point-to-Point Protocol (MLP):** Carries 6 bytes of overhead; 1 byte for flag, 1 byte for address, 2 bytes for control (or type), and 2 bytes for CRC
- **FRF.12:** Carries 6 bytes of overhead; 2 bytes for data-link connection identifier (DLCI) header, 2 bytes for FRF.12, and 2 bytes for CRC

Security and Tunneling Overhead

This topic describes overhead associated with various security and tunneling protocols.



Certain security and tunneling encapsulations will also add overhead to voice packets and should be considered when calculating bandwidth requirements. When using a Virtual Private Network (VPN), IP Security (IPSec) will add 50 to 57 bytes of overhead, a significant amount when considering small voice packets. Layer 2 Tunneling Protocol/generic routing encapsulation (L2TP/GRE) adds 24 bytes. When using MLP, 6 bytes will be added to each packet. Multiprotocol Label Switching (MPLS) adds a 4-byte label to every packet. All of these specialized tunneling and security protocols must be considered when planning for bandwidth demands.

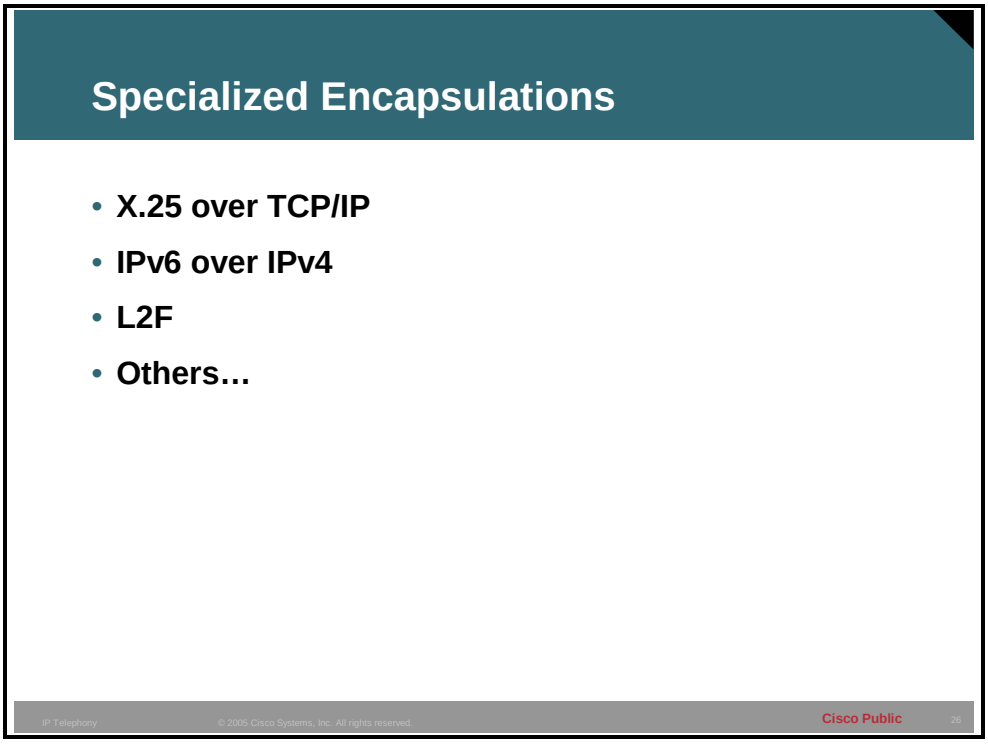
Example: VPN Overhead

Many companies have their employees telecommute from home. These employees initiate a VPN connection into their enterprise for secure Internet transmission. When deploying a remote telephone at the employee's home using a router and a PBX Off-Premises eXtension (OPX), the voice packets will experience additional overhead associated with the VPN.

 Copyright © 2005, Cisco Systems, Inc.

Specialized Encapsulations

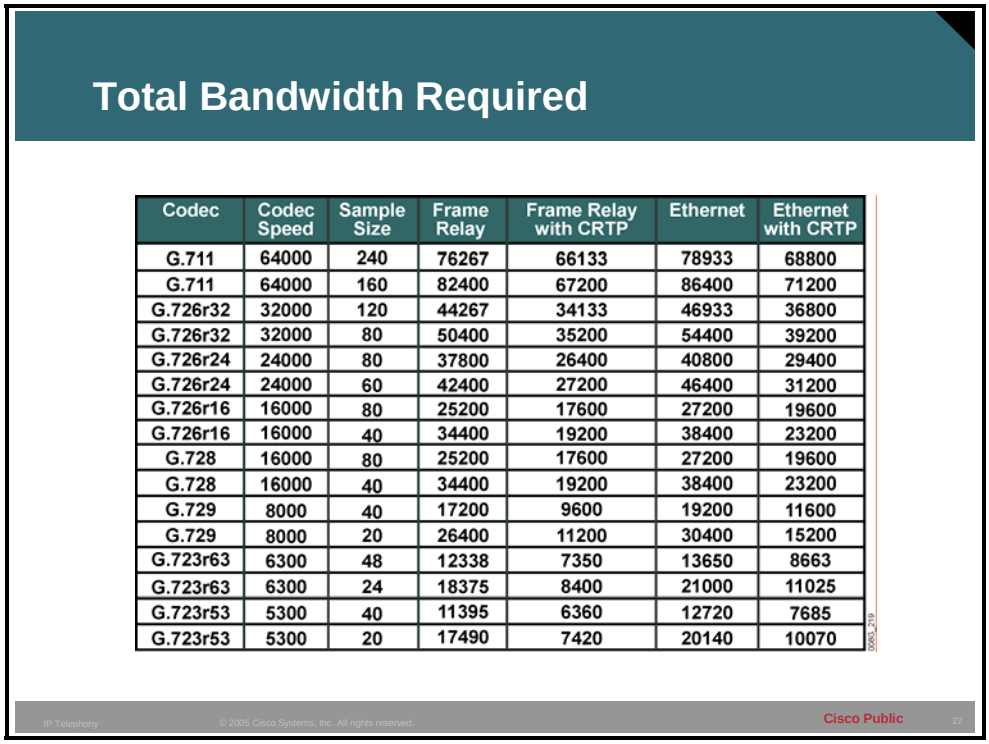
This topic describes considerations for specialized encapsulations for VoIP.



There exist many other encapsulations to consider when transporting VoIP. Specialized encapsulations include protocol-specific encapsulation such as X.25, experimental encapsulations such as IPv6 over IPv4, Layer 2 Forwarding (L2F) Protocol, and other vendor-specific encapsulations. Each must be considered when calculating total bandwidth.

Calculating the Total Bandwidth for a VoIP Call

This topic calculates the total bandwidth required for a VoIP call using codec, data link, and sample size.



Codec	Codec Speed	Sample Size	Frame Relay	Frame Relay with CRTP	Ethernet	Ethernet with CRTP
G.711	64000	240	76267	66133	78933	68800
G.711	64000	160	82400	67200	86400	71200
G.726r32	32000	120	44267	34133	46933	36800
G.726r32	32000	80	50400	35200	54400	39200
G.726r24	24000	80	37800	26400	40800	29400
G.726r24	24000	60	42400	27200	46400	31200
G.726r16	16000	80	25200	17600	27200	19600
G.726r16	16000	40	34400	19200	38400	23200
G.728	16000	80	25200	17600	27200	19600
G.728	16000	40	34400	19200	38400	23200
G.729	8000	40	17200	9600	19200	11600
G.729	8000	20	26400	11200	30400	15200
G.723r63	6300	48	12338	7350	13650	8663
G.723r63	6300	24	18375	8400	21000	11025
G.723r53	5300	40	11395	6360	12720	7685
G.723r53	5300	20	17490	7420	20140	10070

Codec choice, data-link overhead, sample size, and compressed RTP have positive and negative impacts on total bandwidth. To perform the calculations, you must consider these contributing factors as part of the equation:

- More bandwidth required for the codec = more total bandwidth required
- More overhead associated with the data link = more total bandwidth required
- Larger sample size = less total bandwidth required
- Compressed RTP = significantly reduced total bandwidth required

Example: Total Bandwidth Calculation

The following calculation was used to produce the figure:

Total_Bandwidth = ([Layer_2_Overhead + IP_UDP_RTP Overhead + Sample_Size] / Sample_Size) * Codec_Speed

For example, assume a G.729 codec, 20-byte sample size, using Frame Relay without CRTP:

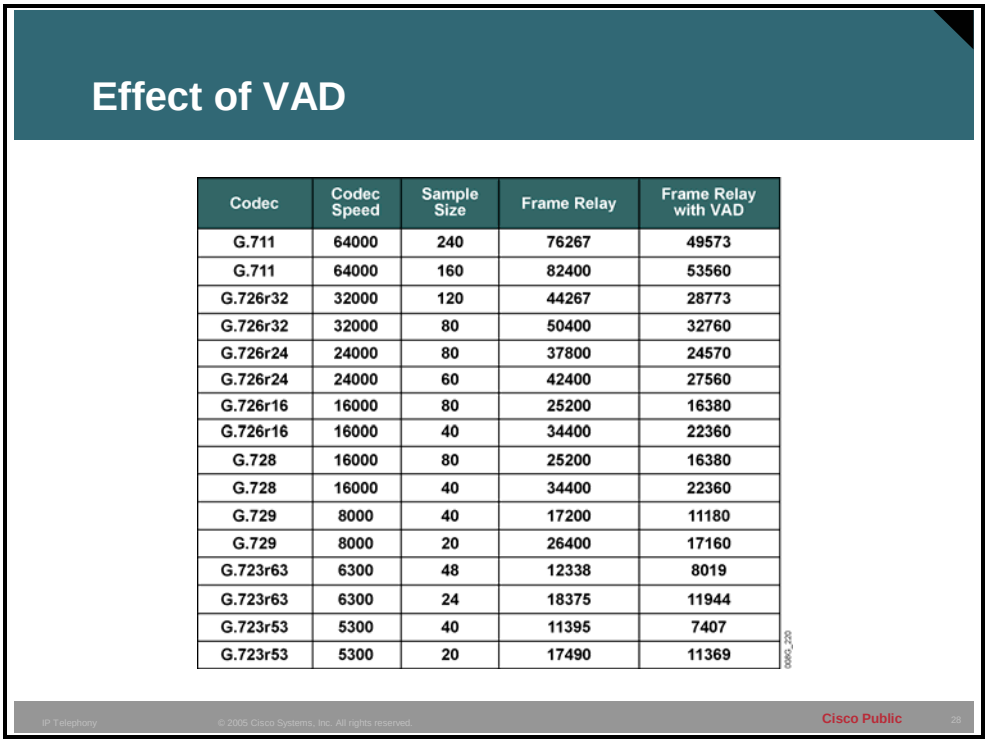
Total_Bandwidth = ([6 + 40 +20]/20) * 8000

Total_Bandwidth = 26,400 bps

 Copyright © 2005, Cisco Systems, Inc.

Effects of VAD on Bandwidth

This topic describes the effect of voice activity detection (VAD) on total bandwidth.



Codec	Codec Speed	Sample Size	Frame Relay	Frame Relay with VAD
G.711	64000	240	76267	49573
G.711	64000	160	82400	53560
G.726r32	32000	120	44267	28773
G.726r32	32000	80	50400	32760
G.726r24	24000	80	37800	24570
G.726r24	24000	60	42400	27560
G.726r16	16000	80	25200	16380
G.726r16	16000	40	34400	22360
G.728	16000	80	25200	16380
G.728	16000	40	34400	22360
G.729	8000	40	17200	11180
G.729	8000	20	26400	17160
G.723r63	6300	48	12338	8019
G.723r63	6300	24	18375	11944
G.723r53	5300	40	11395	7407
G.723r53	5300	20	17490	11369

0085_229

On average, an aggregate of 24 calls or more may contain 35 percent silence. With traditional telephony voice networks, all voice calls use 64-kbps fixed-bandwidth links regardless of how much of the conversation is speech and how much is silence. In Cisco VoIP networks, all conversations and silences are packetized. VAD suppresses packets of silence. Instead of sending VoIP packets of silence, VoIP gateways interleave data traffic with VoIP conversations to more effectively use network bandwidth.

VAD provides a maximum of 35 percent bandwidth savings based on an average volume of more than 24 calls.

Note Bandwidth savings of 35 percent is an average figure and does not take into account loud background sounds, differences in languages, and other factors.

The savings are not realized on every individual voice call, or on any specific point measurement.

Note For the purposes of network design and bandwidth engineering, VAD should *not* be taken into account, especially on links that will carry fewer than 24 voice calls simultaneously.

Various features, such as music on hold (MOH) and fax, render VAD ineffective. When the network is engineered for the full voice call bandwidth, all savings provided by VAD are available to data applications.

VAD is enabled by default for all VoIP calls. VAD reduces the silence in VoIP conversations but it also provides comfort noise generation (CNG). Because you can mistake silence for a disconnected call, CNG provides locally generated *white noise* to make the call appear normally connected to both parties.

Example: VAD Bandwidth Savings

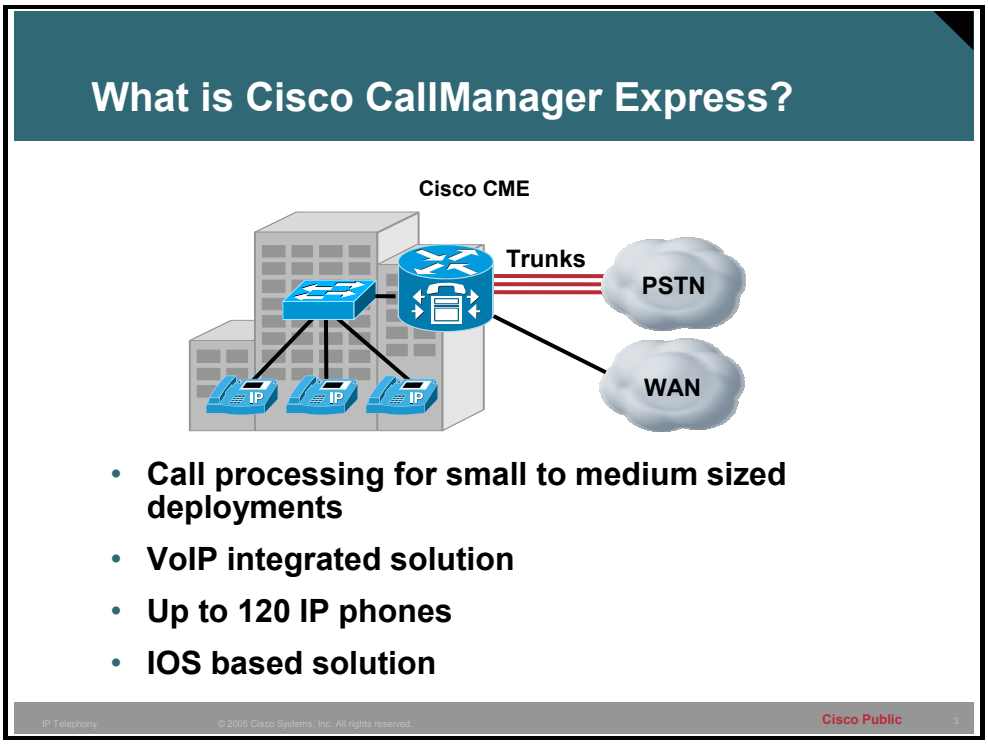
The figure shows examples of the VAD effect in a Frame Relay VoIP environment. In the example using G.711 with a 160-byte payload, the bandwidth required is 82,400 bps. By turning VAD on, you can reduce the bandwidth utilization to 53,560 bps. This is a bandwidth savings of 35 percent.

 Copyright © 2005, Cisco Systems, Inc.

Overview of Cisco CME

What is Cisco CallManager Express?

This topic describes the Cisco CME system.



Cisco CallManager Express (CME) is an integrated call-processing solution, based on Cisco midrange access routers using Cisco IOS software, that delivers telephony services for 10 to 100 users in small offices. Cisco CME is part of Cisco IP Communication Solution and works in conjunction with the extended Cisco Systems® product portfolio, including routers, data switches, public telephone switched network (PSTN) gateways, gatekeepers, Cisco Unity voice mail, and analog terminal adapters.

Cisco CME delivers a robust set of telephony features similar to those commonly used by business users. Cisco CME is an optional feature of Cisco IOS Software and is available on a wide range of Cisco access routers supporting as many as 120 phones. This allows customers to take advantage of the benefits of IP communications without the higher costs and complexity of deploying a server-based solution. Because the solution is based on the Cisco access router and Cisco IOS software, it is simple to deploy and manage, especially for customers who already use Cisco IOS software products. Cisco CME allows customers to scale IP telephony to a small or branch office site with a solution that is easy to deploy, administer, and maintain.

What is Cisco CallManager Express? (Cont.)

- **Select IOS based platform**
- **Multiservice access routers**



2600XM



3700



1700

IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 4

Cisco CME enables Cisco's large portfolio of multiservice access routers to deliver low-end PBX and Key System type features, creating a cost-effective, highly reliable, feature-rich IP communications solution for the small office.

Cisco CME supports a new generation of intelligent IP Phones with robust display capabilities. End users can easily customize these phones based on their changing needs.

 Copyright © 2005, Cisco Systems, Inc.

How Does Cisco CallManager Express Work?

This topic describes how Cisco CME system works.

The Cisco CME system provides the PBX-like features and functions for the IP phones. These features are a result of the concept of a centralized point of control and intelligence. The Cisco CME router provides all of the call control and intelligence needed for the IP phones to place and receive calls. In a Cisco CME deployment, the IP phones are not capable of setting up a call by themselves. In fact, the IP phones are totally under the control of the Cisco CME system and are instructed how to place or receive a call.

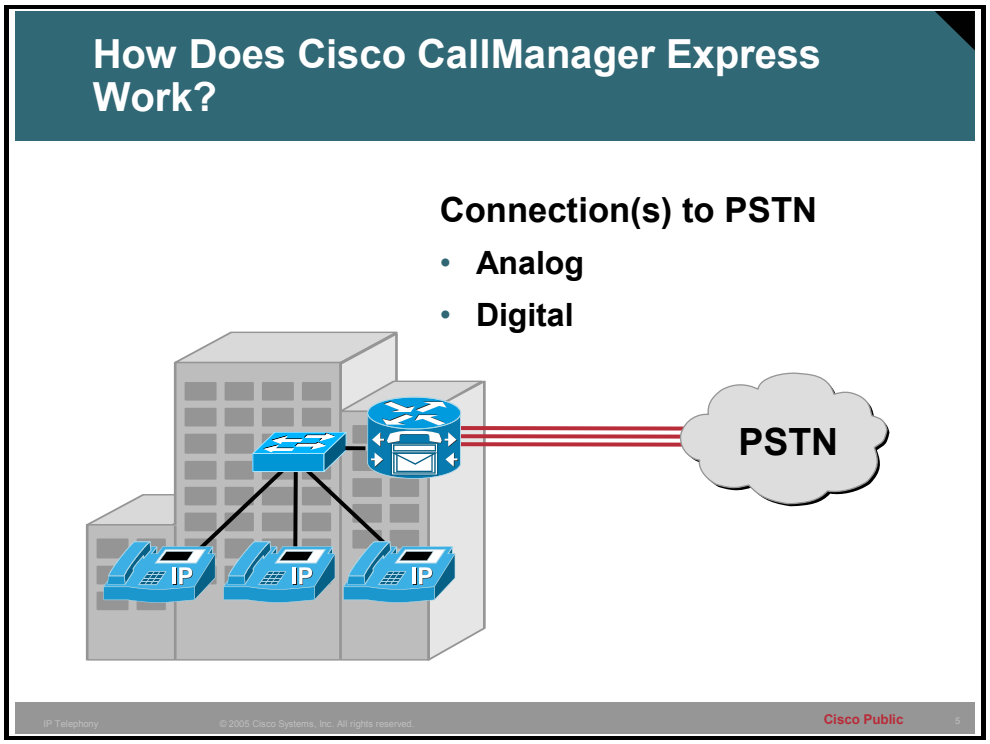
The IP phones will boot up and register with the Cisco CME. If configured, the Cisco CME is then able to set up or tear down calls to or from the IP phones. The IP phones and the CME router use a protocol called Skinny Client Control Protocol (SCCP) to communicate.

When a call is placed between two IP phones under the control of Cisco CME, the SCCP protocol is used to set the call up. SCCP is also commonly known as the "skinny" protocol. The SCCP protocol will not go between the two IP phones, only between the IP phone and the Cisco CME system. Once the call is set up, the Realtime Transport Protocol (RTP) will be used to carry the audio stream. RTP is used to carry voice inside of IP packets. RTP is a common protocol that is used to carry time-sensitive traffic like voice and real-time video. RTP is carried inside of a UDP segment, which is then carried inside of an IP packet.

The sequence of events to for a phone call follows:

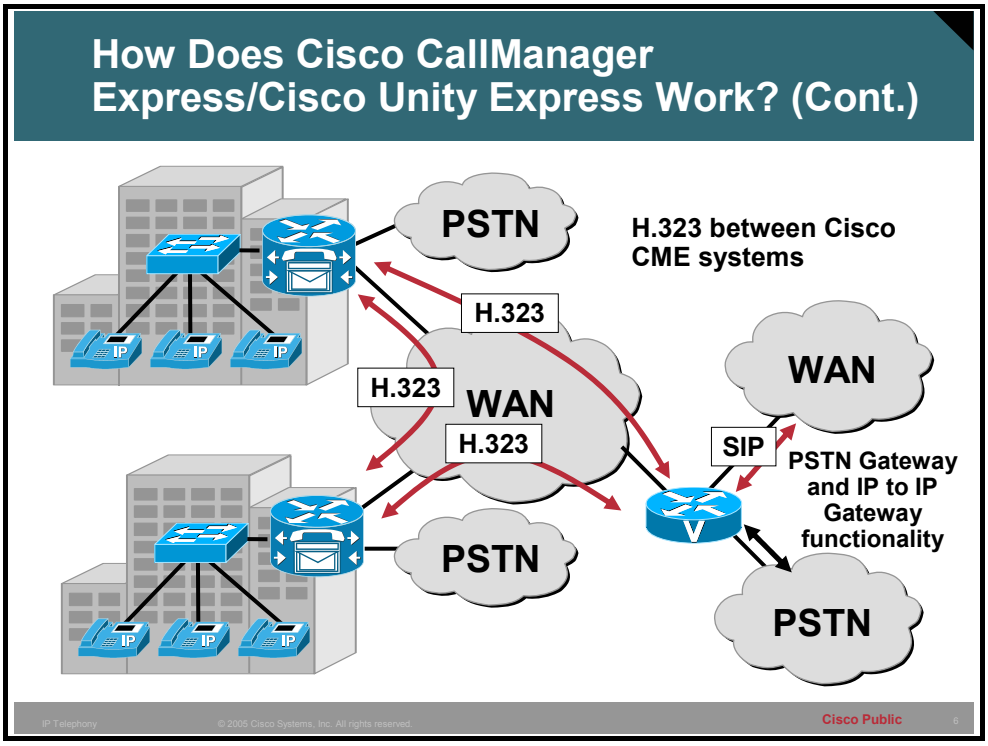
- **Step 1 -** Phone A picks up the handset and dials the number of phone B
- **Step 2 -** The digits dialed are set through the skinny protocol to the CME
- **Step 3 -** CME knows where the phone B is due to the registration and the phones status (busy, on-hook, off-hook)
- **Step 4 -** Assuming that Phone B is on-hook (available), the CME will send skinny messages to tell the phone B about the incoming call and to tell phone B to ring
- **Step 5 -** Phone B answers the call by picking up the handset
- **Step 6 -** Cisco CME informs both IP phones about the settings on the other and instructs them to construct RTP connections
- **Step 7 -** The IP phones construct two one-way RTP connections for the voice to travel across, one for phone A's voice to travel across to B and one for phone B's voice to travel to A
- **Step 8** – The call takes place
- **Step 9** – Phone B hangs up and skinny messages are sent to the Cisco CME system
- **Step 10** – Cisco CME sends skinny messages to phone A instructing it that the call has been disconnected.

Copyright © 2005, Cisco Systems, Inc.



The Cisco CME system can act as the PSTN gateway as well as managing the IP phones. There are different types of connections to the PSTN including both digital and analog connections. The type of connection used will be dependant on the density of connections needed, technology available in the region, cost of the connections and the interfaces present on the router.

 Copyright © 2005, Cisco Systems, Inc.



If the Cisco CME system needs to set a call up to an IP phone under the control of another CME system, then the H.323 protocol will need to be used between the Cisco CME systems. This allows for many different deployments of Cisco CME to be integrated together through an IP-based WAN link.

The PSTN gateway function can be performed on the Cisco CME router or on a separate standalone gateway. If a separate PSTN gateway is used, the additional functionality of an IP to IP gateway functions may also be run on the router. This would enable the ability to translate between H.323 and SIP.

Note	Local PSTN will be needed for each site for at least 911 Emergency purposes

Licensing

This topic describes the licensing of Cisco CME system.

There are four CUE license levels available on the network module (NM-CUE). There are three CUE license levels available with the advanced integration module (AIM-CUE). The fifty-mailbox option, while available, is discouraged due to the 4-port limitation of the AIM module. The preferred configuration when using the AIM module is to have the 12 or 25 mailbox license installed.

The hardware associated with CUE (NM-CUE, AIM-CUE) must be purchased with an accompanying license. Hardware and software are packaged. Mailbox licenses are purchased separately with the exception of the 12-mailbox license level that is included in the price of the hardware/software bundle. Because of this, a minimum license level of 12 mailboxes must be ordered with each CUE purchase.

CUE license files, like Cisco IOS software, can be downloaded from http://cisco.com and installed on any number of systems for which a license was purchased without change to the file itself. When a license is purchased or software from Cisco is used, a contractual obligation is created. The subscriber must abide by the terms spelled out in the license agreement including prohibitions regarding unauthorized replication of the software or modification to the licensed mailbox level.

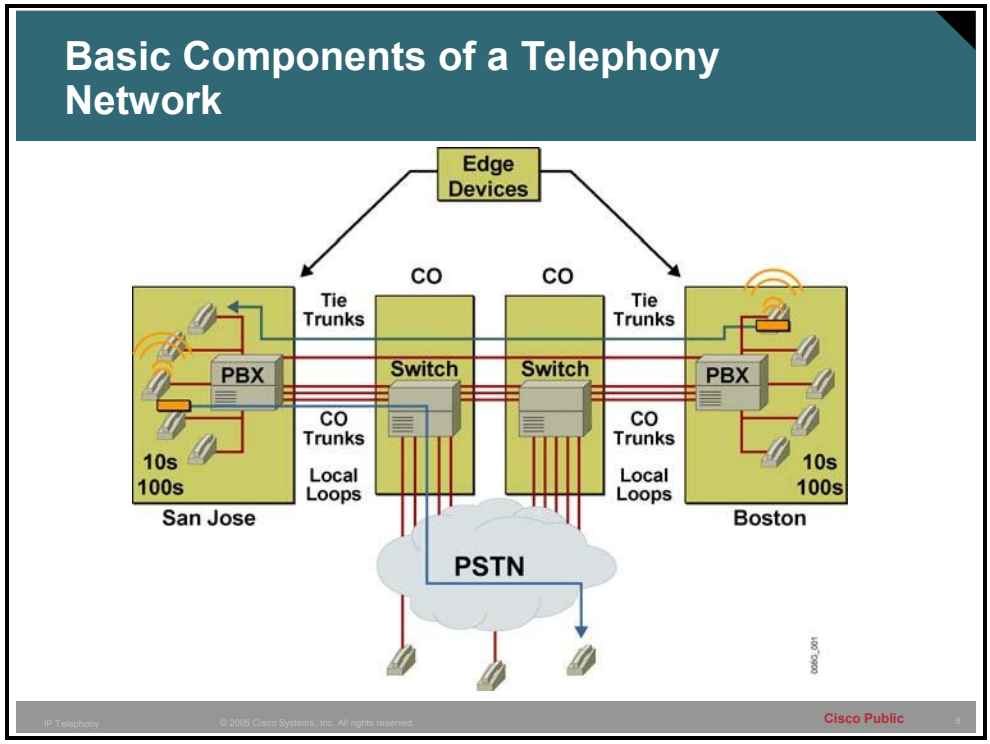
The capacity limitations on ports, subscribers, and mailboxes depend on whether CUE is running on a network module or advanced integration module and is controlled by the license installed on the CUE application.

 Copyright © 2005, Cisco Systems, Inc.

Differences between Traditional Telephony and VoIP

Traditional Telephony

This topic introduces the components of traditional telephony networks.



A number of components must be in place for an end-to-end call to succeed. These components are shown in the figure and include the following:

- Edge devices
- Local loops
- Private or central office (CO) switches
- Trunks

Edge Devices

The two types of edge devices that are used in a telephony network include:

- **Analog telephones:** Analog telephones are most common in home, small office/home office (SOHO), and small business environments. Direct connection to the public switched

telephone network (PSTN) is usually made by using analog telephones. Proprietary analog telephones are occasionally used in conjunction with a PBX. These phones provide additional functions such as speakerphone, volume control, PBX message-waiting indicator, call on hold, and personalized ringing.

- **Digital telephones:** Digital telephones contain hardware to convert analog voice into a digitized stream. Larger corporate environments with PBXs generally use digital telephones. Digital telephones are typically proprietary, meaning that they work with the PBX or key system of that vendor only.

Local Loops

A local loop is the interface to the telephone company network. Typically, it is a single pair of wires that carry a single conversation. A home or small business may have multiple local loops.

Private or CO Switches

The CO switch terminates the local loop and handles signaling, digit collection, call routing, call setup, and call teardown.

A PBX switch is a privately owned switch located at the customer site. A PBX typically interfaces with other components to provide additional services; for example, voice mail.

Trunks

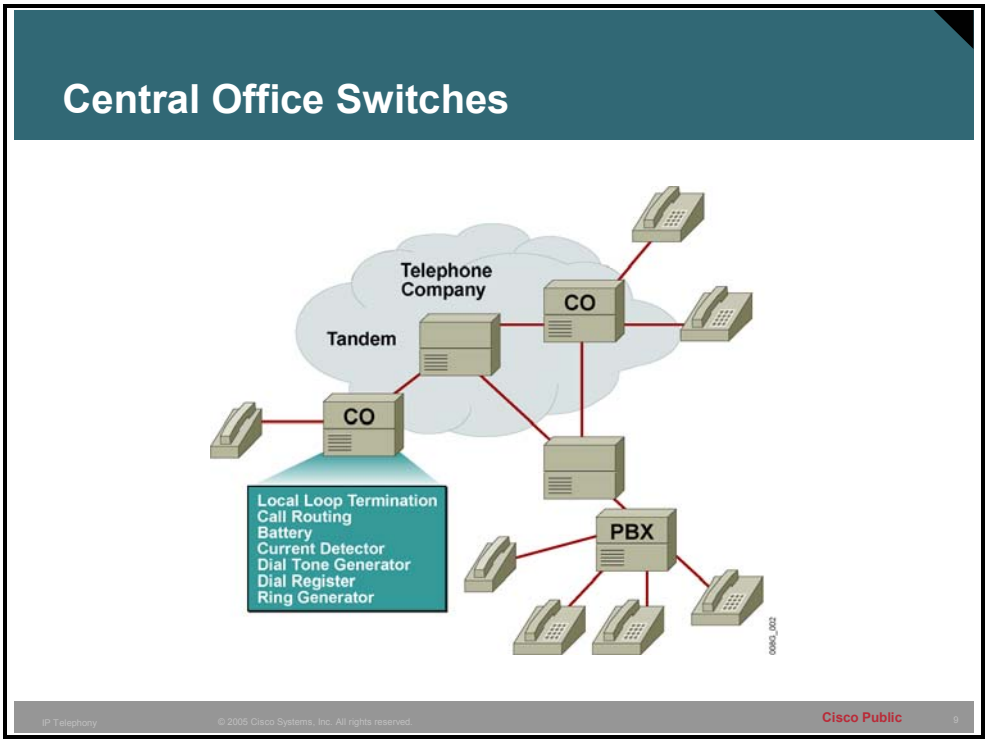
The primary function of a trunk is to provide the path between two switches. There are several common trunk types including:

- **Tie trunk:** A dedicated circuit that connects PBXs directly
- **CO trunk:** A direct connection between a local CO and a PBX
- **Interoffice trunk:** A circuit that connects two local telephone company COs.

 Copyright © 2005, Cisco Systems, Inc.

Traditional Telephony: Central Office Switches

This topic describes how CO switches function and make switching decisions.



The figure shows a typical CO switch environment. The CO switch terminates the local loop and makes the initial call-routing decision.

The call-routing function forwards the call to one of the following:

- Another end-user telephone if it is connected to the same CO
- Another CO switch
- A tandem switch

The CO switch makes the telephone work with the following components:

- **Battery:** The battery is the source of power to both the circuit and the telephone—it determines the status of the circuit. When the handset is lifted to let current flow, the telephone company provides the source that powers the circuit and the telephone. Because the telephone company powers the telephone from the CO, electrical power outages should not affect the basic telephone.

Note	Some telephones on the market offer additional features that require a supplementary power source that the subscriber supplies; for example, cordless telephones. Some cordless telephones may lose function during a power outage.

- **Current detector:** The current detector monitors the status of a circuit by detecting whether it is open or closed. The table here describes current flow in a typical telephone.

Table 1: Current Flow in a Typical Telephone

Handset	Circuit	Current Flow
On cradle	On hook/open circuit	No
Off cradle	Off hook/closed circuit	Yes

- **Dial tone generator:** When the digit register is ready, the dial-tone generator produces a dial tone to acknowledge the request for service.

- **Digit register:** The digit register receives the dialed digits.

- **Ring generator:** When the switch detects a call for a specific subscriber, the ring generator alerts the called party by sending a ring signal to that subscriber.

You must configure a PBX connection to a CO switch that matches the signaling of the CO switch. This configuration ensures that the switch and the PBX can detect on hook, off hook, and dialed digits coming from either direction.

CO Switching Systems

Switching systems provide three primary functions:

- Call setup, routing, and teardown

- Call supervision

- Customer ID and telephone numbers

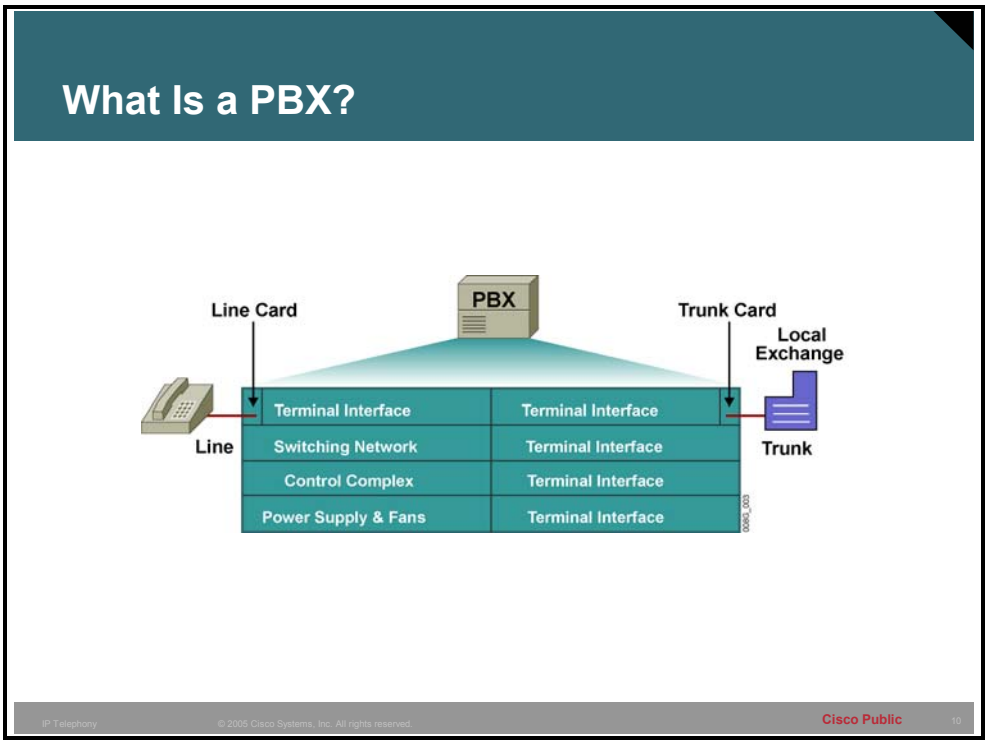
CO switches switch calls between locally terminated telephones. If a call recipient is not locally connected, the CO switch decides where to send the call based on its call-routing table. The call then travels over a trunk to another CO or to an intermediate switch that may belong to an inter-exchange carrier (IXC). Although intermediate switches do not provide dial tone, they act as hubs to connect other switches and provide interswitch call routing.

PSTN calls are traditionally circuit-switched, which guarantees end-to-end path and resources. Therefore, as the PSTN sends a call from one switch to another, the same resource is associated with the call until the call is terminated.

 Copyright © 2005, Cisco Systems, Inc.

Traditional Telephony: PBX and Key Telephone System Functionality

In a corporate environment, where large numbers of staff need access to each other and the outside, individual telephone lines are not economically viable. This topic explores PBX and key telephone system functionality in environments today.



A PBX is a smaller, privately-owned version of the CO switches used by telephone companies.

Most businesses have a PBX telephone system, a key telephone system, or Centrex service. Large offices with more than 50 telephones or handsets choose a PBX to connect users, both in-house and to the PSTN.

PBXs come in a variety of sizes, typically from 20 to 20,000 stations. The selection of a PBX is important to most companies because a PBX has a typical life span of 7 to 10 years.

All PBXs offer a standard, basic set of calling features. Optional software provides additional capabilities.

The figure illustrates the internal components of a PBX: it connects to telephone handsets using line cards and to the local exchange using trunk cards.

A PBX has three major components:

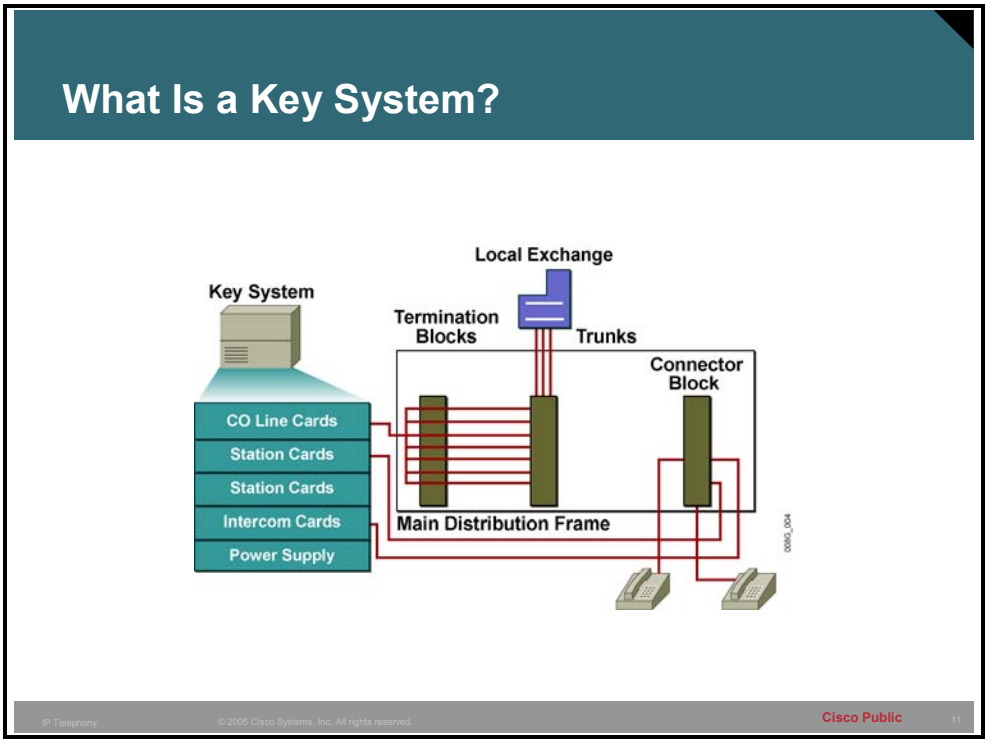
- **Terminal interface:** The terminal interface provides the connection between terminals and PBX features that reside in the control complex. Terminals can include telephone handsets, trunks, and lines. Common PBX features include dial tone and ringing.

- **Switching network:** The switching network provides the transmission path between two or more terminals in a conversation; for example, two telephones within an office communicate over the switching network.

- **Control complex:** The control complex provides the logic, memory, and processing for call setup, call supervision, and call disconnection.

 Copyright © 2005, Cisco Systems, Inc.

Traditional Telephony: What Is a Key System



Small organizations and branch offices often use a key telephone system because a PBX offers functionality and extra features that they may not require. For example, a key system offers small businesses distributed answering from any telephone, unlike the central answering position required for a PBX.

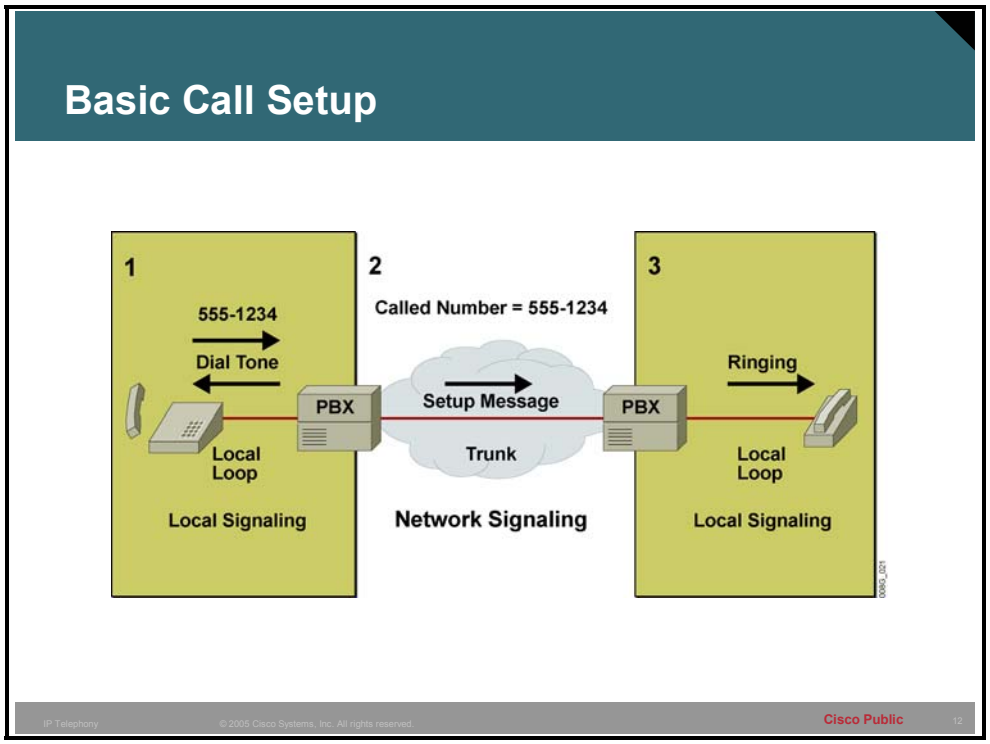
Today, key telephone systems are either analog or digital and are microprocessor-based. Key systems are typically used in offices with 30 to 40 users, but can be scaled to support over 100 users.

A key system has three major components:

- **Key service unit:** A key service unit (KSU) holds the system switching components, power, intercom, line and station cards, and the system logic.
- **System software:** System software provides the operating system and calling-feature software.
- **Telephones (instruments or handsets):** Telephones allow the user to choose a free line and dial out, usually by pressing a button on the telephone.

Traditional Telephony: Basic Call Setup

Call signaling, in its most basic form, is the capacity of a user to communicate a need for service to a network. The call-signaling process requires the ability to detect a request for and termination of service, send addressing information, and provide progress reports to the initiating party. This functionality corresponds to the three call-signaling types discussed in this topic: supervisory, address, and informational signaling.



The figure shows the three major steps in an end-to-end call. These steps include:

Step 1 Local signaling—originating side

The user signals the switch by going off hook and sending dialed digits through the local loop.

Step 2 Network signaling

The switch makes a routing decision and signals the next, or terminating, switch through the use of setup messages sent across a trunk.

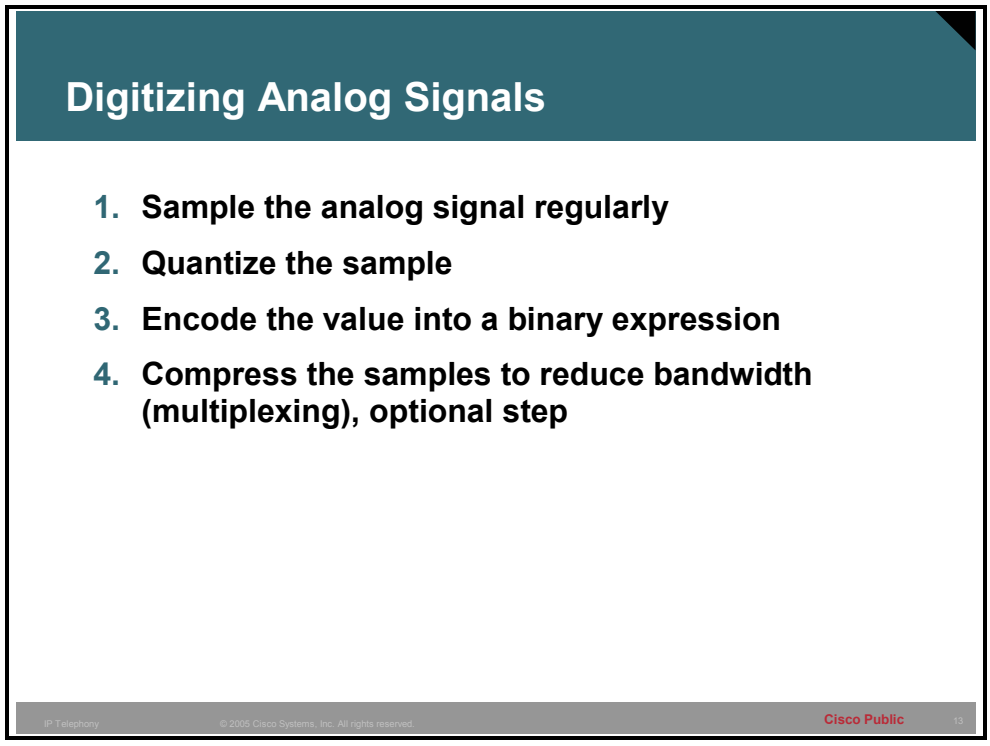
Step 3 Local signaling—terminating side

The terminating switch signals the call recipient by sending ringing voltage through the local loop to the recipient telephone.

 Copyright © 2005, Cisco Systems, Inc.

PCM Theory

This topic describes the process of converting analog signals to digital signals.



Digitizing speech was a project first undertaken by the Bell System in the 1950s. The original purpose of digitizing speech was to deploy more voice circuits with a smaller number of wires. This evolved into the T1 and E1 transmission methods of today.

To convert an analog signal to a digital signal, you must perform these steps:

Note	The last step is optional.

Table 1: Analog to Digital Signal Conversion

Step	Procedure	Description
1.	Sample the analog signal regularly.	The sampling rate must be two times the highest frequency to produce playback that appears neither choppy nor too smooth.
2.	Quantize the sample.	Quantization consists of a scale made up of 8 major divisions or chords. Each chord is subdivided into 16 equally spaced steps. The chords are not equally spaced but are actually finest near the origin. Steps are equal within the chords but different when they are compared between the chords. Finer graduations at the origin result in less distortion for low-level tones.
3.	Encode the value into 8-bit digital form.	PBX output is a continuous analog voice waveform. T1 digital voice is a snapshot of the wave encoded in ones and zeros.
4.	(Optional) Compress the samples to reduce bandwidth.	Although not essential to convert analog signals to digital, signal compression is widely used to reduce bandwidth.

Three components in the analog-to-digital conversion process include:

- **Sampling:** Sample the analog signal at periodic intervals. The output of sampling is a pulse amplitude modulation (PAM) signal.

- **Quantization:** Match the PAM signal to a segmented scale. This scale measures the amplitude (height) of the PAM signal and assigns an integer number to define that amplitude.

- **Encoding:** Convert the integer base-10 number to a binary number. The output of encoding is a binary expression in which each bit is either a 1 (pulse) or a 0 (no pulse).

This three-step process is repeated 8000 times per second for telephone voice channel service. Use the fourth optional step—compression—to save bandwidth. This optional step allows a single channel to carry more voice calls.

Note The most commonly used method of converting analog to digital is pulse code modulation (PCM).

 Copyright © 2005, Cisco Systems, Inc.

Basic Voice Encoding: Converting Digital to Analog

This topic describes the process of converting digital signals back to analog signals.

After the receiving terminal at the far end receives the digital PCM signal, it must convert the PCM signal back into an analog signal.

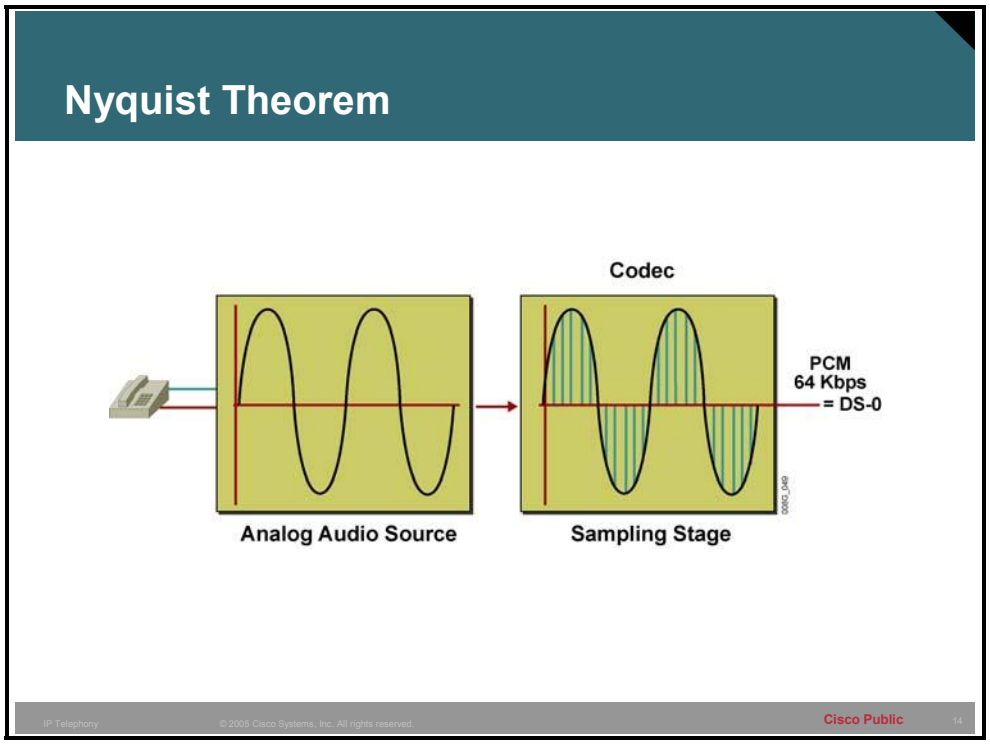
The process of converting digital signals back into analog signals includes the following two parts:

- **Decoding:** The received eight-bit word is decoded to recover the number that defines the amplitude of that sample. This information is used to rebuild a PAM signal of the original amplitude. This process is simply the reverse of the analog-to-digital conversion.

- **Filtering:** The PAM signal is passed through a properly designed filter that reconstructs the original analog wave form from its digitally coded counterpart.

PCM Theory

This topic describes the Nyquist Theorem that is the basis for digital signal technology.



Nyquist Theorem

Digital signal technology is based on the premise stated in the Nyquist Theorem: when a signal is instantaneously sampled at the transmitter in regular intervals and has a rate of at least twice the highest channel frequency, then the samples will contain sufficient information to allow an accurate reconstruction of the signal at the receiver.

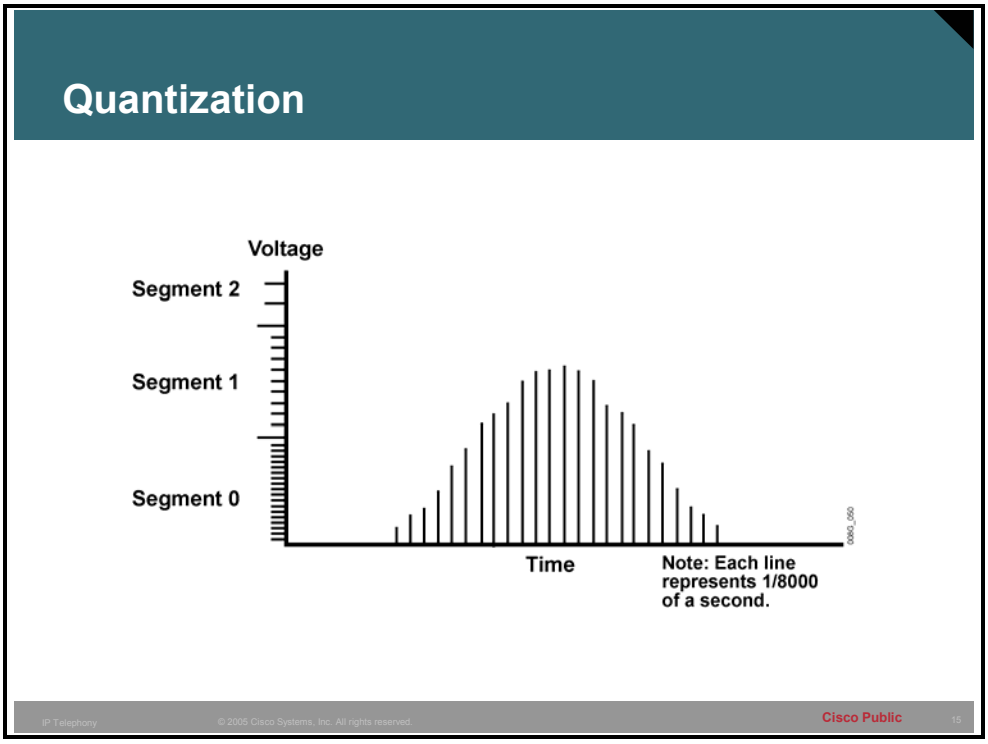
Example

While the human ear can sense sounds from 20 to 20,000 Hz, and speech encompasses sounds from about 200 to 9000 Hz, the telephone channel was designed to operate at about 300 to 3400 Hz. This economical range carries enough fidelity to allow callers to identify the party at the far end and sense their mood. Nyquist decided to extend the digitization to 4000 Hz, to capture higher-frequency sounds that the telephone channel may deliver. Therefore, the highest frequency for voice is 4000 Hz, or 8000 samples per second; that is, one sample every 125 microseconds.

 Copyright © 2005, Cisco Systems, Inc.

PCM Theory: Quantization

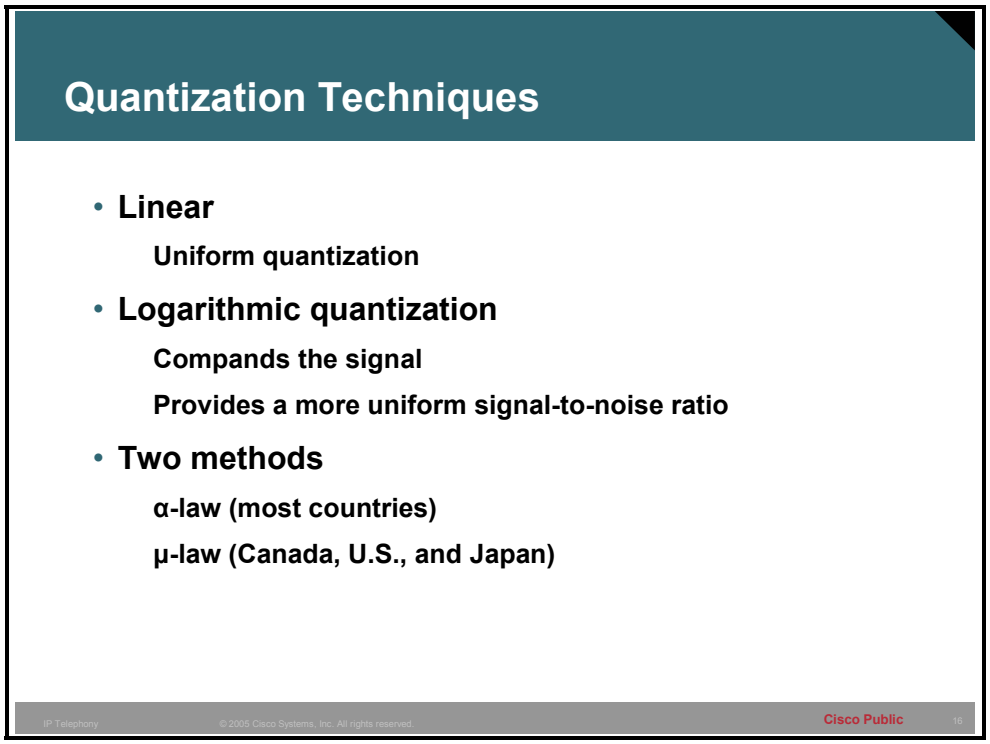
This topic explains quantization and its techniques.



Quantization involves dividing the range of amplitude values that are present in an analog signal sample into a set of discrete steps that are closest in value to the original analog signal. Each step is assigned a unique digital code word.

The figure here depicts quantization. In this example, the x-axis is time and the y-axis is the voltage value (PAM).

The voltage range is divided into 16 segments (0 to 7 positive, and 0 to 7 negative). Starting with segment 0, each segment has fewer steps than the previous segment, which reduces the noise-to-signal ratio and makes it uniform. This segmentation also corresponds closely to the logarithmic behavior of the human ear. If there is a noise-to-signal ratio problem, it is resolved by using a logarithmic scale to convert PAM to PCM.



Linear sampling of analog signals causes small-amplitude signals to have a higher noise-to-signal ratio, and therefore poorer quality than larger amplitude signals. The Bell System developed the *μ-law* method of quantization, which is widely used in North America. The International Telecommunication Union (ITU) modified the original μ-law method and created *α-law*, which is used in countries outside of North America.

By allowing smaller step functions at lower amplitudes—rather than higher amplitudes—μ-law and α-law provide a method of reducing this problem. Both μ-law and α-law compand the signal; for example, they both compress the signal for transmission and then expand the signal back to its original form at the other end.

The result of using μ-law and α-law is a more accurate value for smaller amplitude and uniform signal-to-noise quantization ratio (SQR) across the input range

Both μ-law and α-law are linear approximations of a logarithmic input/output relationship. They both generate 64-kbps bit streams using 8-bit code words to segment and quantize levels within segments.

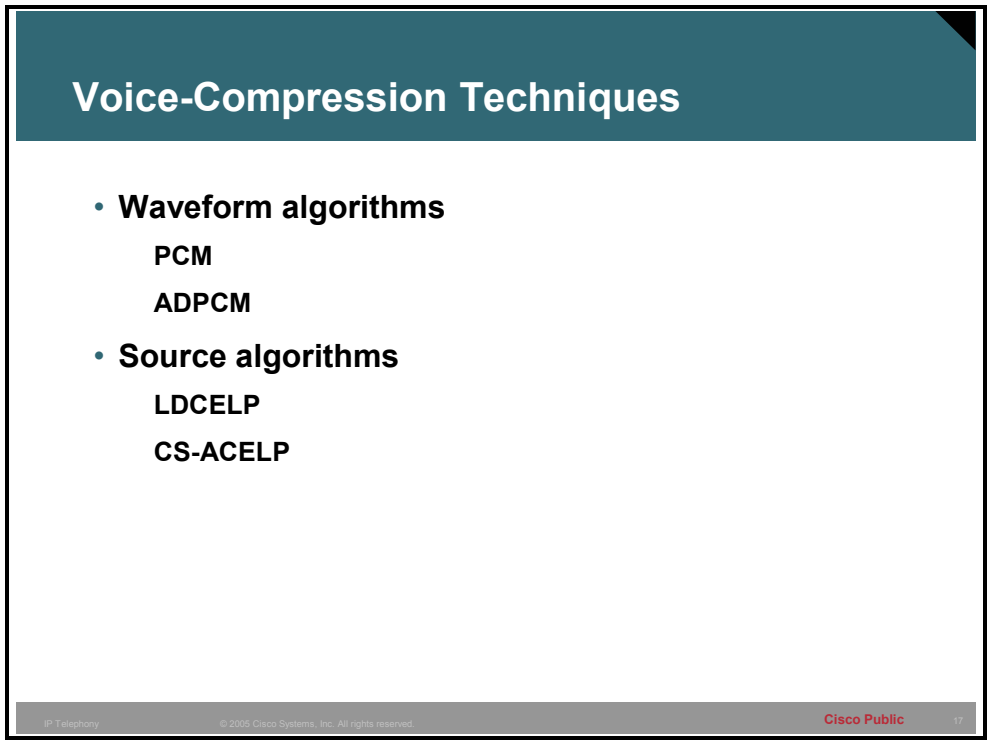
The difference between the original analog signal and the quantization level assigned is called quantization error, which is the source of distortion in digital transmission systems. Quantization error is any random disturbance or signal that interferes with the quality of the transmission or the signal itself.

Note	For communication between a μ-law country and an α-law country, the μ-law country must change its signaling to accommodate the α-law country.

 Copyright © 2005, Cisco Systems, Inc.

Coder-Decoder

This topic describes two types of speech-coding schemes: waveform and source coding.



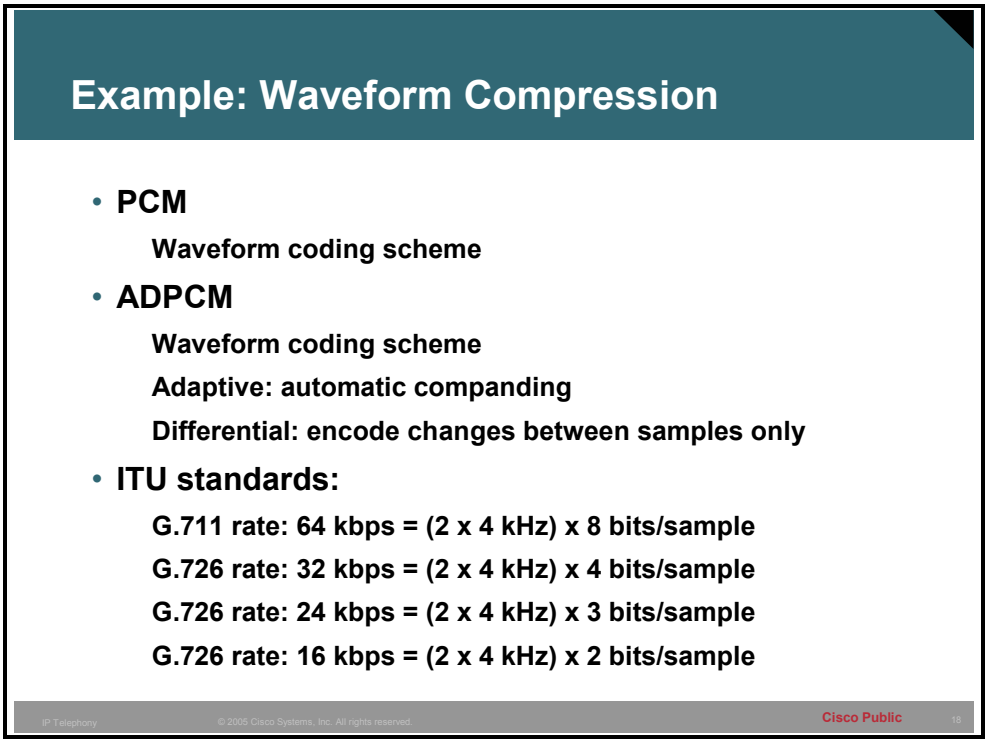
There are two voice compression techniques:

- Waveform algorithms (coders) function as follows:
  - Sample analog signals at 8000 times per second
  - Use predictive differential methods to reduce bandwidth
  - Bandwidth reduction highly impacts voice quality
  - Do not take advantage of speech characteristics
- Source algorithms function as follows:
  - Source algorithm coders are called vocoders. Vocoder is a term that describes ‘Voice Coding’, which is a device that converts analog speech into digital speech, using a specific compression scheme that is optimized for coding human speech.
  - Vocoders take advantage of speech characteristics.

— Codebooks store specific predictive waveshapes of human speech. They match the speech, encode the phrases, decode the waveshapes at the receiver by looking up the coded phrase, and match it to the stored waveshape in the receiver codebook.

 Copyright © 2005, Cisco Systems, Inc.

Coder-Decoder: Waveform Compression



Standard PCM is known as ITU standard G.711.

Adaptive differential pulse code modulation (ADPCM) coders, like other waveform coders, encode analog voice signals into digital signals to adaptively predict future encodings by looking at the immediate past. The adaptive feature of ADCPM reduces the number of bits per second that the PCM method requires to encode voice signals.

ADCPM does this by taking 8000 samples per second of the analog voice signal and turning them into a linear PCM sample. ADCPM then calculates the predicted value of the next sample, based on the immediate past sample, and encodes the difference. The ADPCM process generates 4-bit words, therefore generating 16 specific bit patterns.

The ADPCM algorithm from the Consultative Committee for International Telegraph and Telephone (CCITT) transmits all 16 possible bit patterns. The ADPCM algorithm from the American National Standards Institute (ANSI) uses 15 of the 16 possible bit patterns. The ANSI ADPCM algorithm does not generate a 0000 pattern.

The ITU standards for compression are as follows:

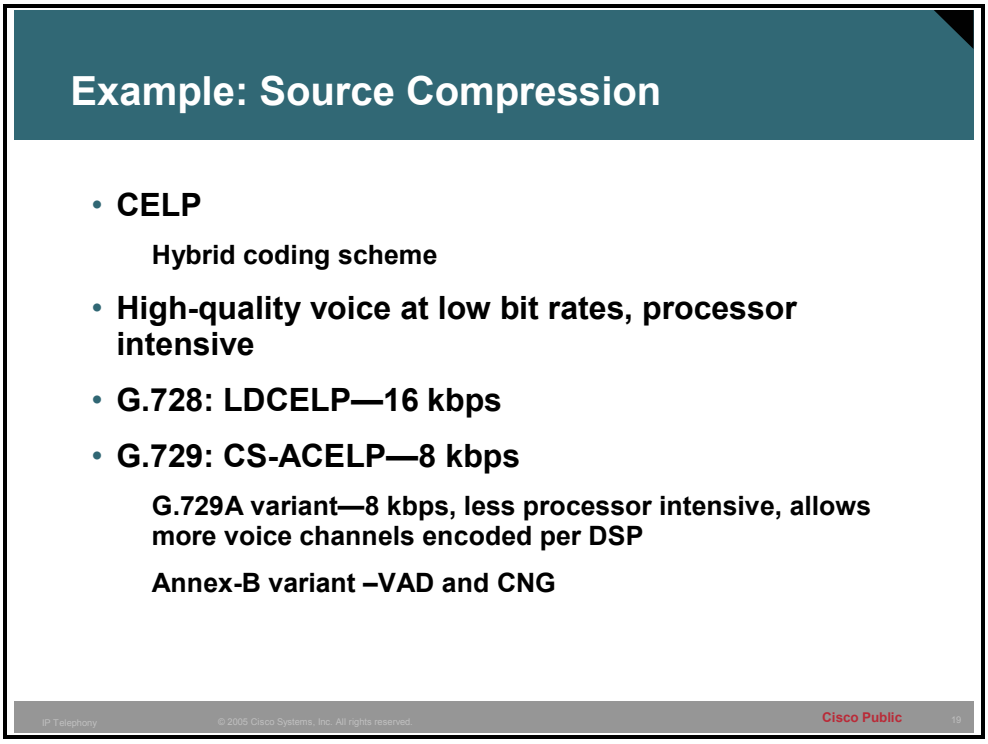
- **G.711 rate:** 64 kbps = (2 x 4 kHz) x 8 bits/sample
- **G.726 rate:** 32 kbps = (2 x 4 kHz) x 4 bits/sample
- **G.726 rate:** 24 kbps = (2 x 4 kHz) x 3 bits/sample

- **G.726 rate:** 16 kbps = (2 x 4 kHz) x 2 bits/sample

Note	CCITT is now called ITU-T.

 Copyright © 2005, Cisco Systems, Inc.

Coder-Decoder: Source Compression



Code excited linear prediction (CELP) compression transforms analog voice signals as follows:

- The input to the coder is converted from an 8-bit PCM to a 16-bit linear PCM sample.
- A codebook uses feedback to continuously learn and predict the voice waveform.
- A white noise generator excites the coder.
- The mathematical result (recipe) is sent to the far-end decoder for synthesis and generation of the voice waveform.

Low-delay CELP (LDCELP) is similar to Conjugate Structure Algebraic Code Excited Linear Prediction (CS-ACELP), except:

- LDCELP uses a smaller codebook and operates at 16 kbps to minimize delay—or look-ahead—to 2 to 5 ms.
- The 10-bit codeword is produced from every five speech samples from the 8-kHz input.
- Four of these 10-bit codewords are called a subframe; they take approximately 2.5 ms to encode.

Two of these subframes are combined into a 5-ms block for transmission. CS-ACELP is a variation of CELP that performs these functions:

- Codes on 80-byte frames, which take approximately 10 ms to buffer and process
- Adds a look-ahead of 5 ms. A look-ahead is a coding mechanism that continuously analyzes, learns, and predicts the next waveshape.
- Adds noise reduction and pitch-synthesis filtering to processing requirements

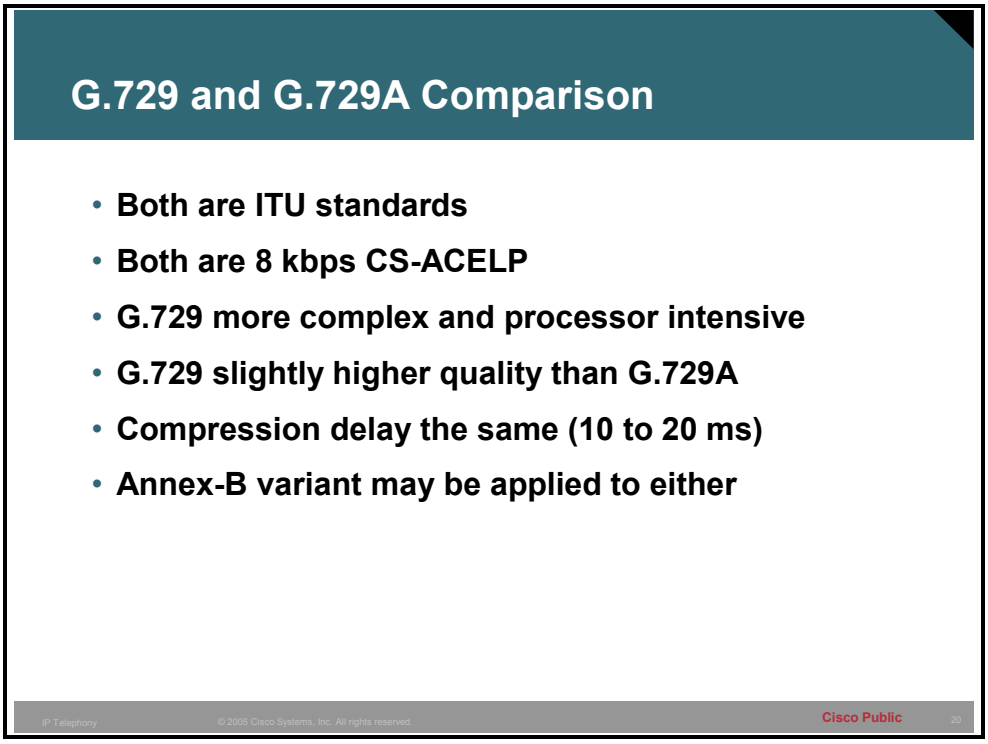
Example

The Annex-B variant adds voice activity detection (VAD) in strict compliance with G.729B standards. When this coder-decoder (codec) variant is used, VAD is not tunable for music threshold. However, when Cisco VAD is configured, music threshold is tunable.

 Copyright © 2005, Cisco Systems, Inc.

Coder-Decoder: G 729 and G 729A Compression

This topic compares G.729 and G.729A compression.



G.729, G.729 Annex-A (G.729A), G.729 Annex-B (G.729B), and G.729A Annex-B (G.729AB) are variations of CS-ACELP.

There is little difference between the ITU recommendations for G.729 and G.729A. All of the platforms that support G.729 also support G.729A.

G.729 is the compression algorithm that Cisco uses for high-quality 8-kbps voice. When properly implemented, G.729 sounds as good as the 32-kbps ADPCM. G.729 is a high-complexity, processor-intensive, compression algorithm that monopolizes processing resources.

Although G.729A is also an 8-kbps compression, it is not as processor-intensive as G.729. It is a medium-complexity variant of G.729 with slightly lower voice quality. The quality of G.729A is not as high as G.729 and is more susceptible to network irregularities such as delay, variation, and tandeming. Tandeming causes distortion that occurs when speech is coded, decoded, and then coded and decoded again, much like the distortion that occurs when a videotape is repeatedly copied.

Example

On Cisco IOS® gateways, you must use the variant (G.729 or G.729A) that is related to the codec complexity configuration on the voice card. This variant does not show up explicitly in the Cisco IOS command-line interface (CLI) codec choice. For example, the CLI does not display **g729r8** (alpha code) as a codec option. However, if the voice card is defined as medium-complexity, then the **g729r8** option is the G.729A codec.

G.729B is a high-complexity algorithm and G.729AB is a medium-complexity variant of G.729B with slightly lower voice quality. The difference between the G.729 and G.729B codec is that the G.729B codec provides built-in Internet Engineering Task Force (IETF) VAD and comfort noise generation (CNG).

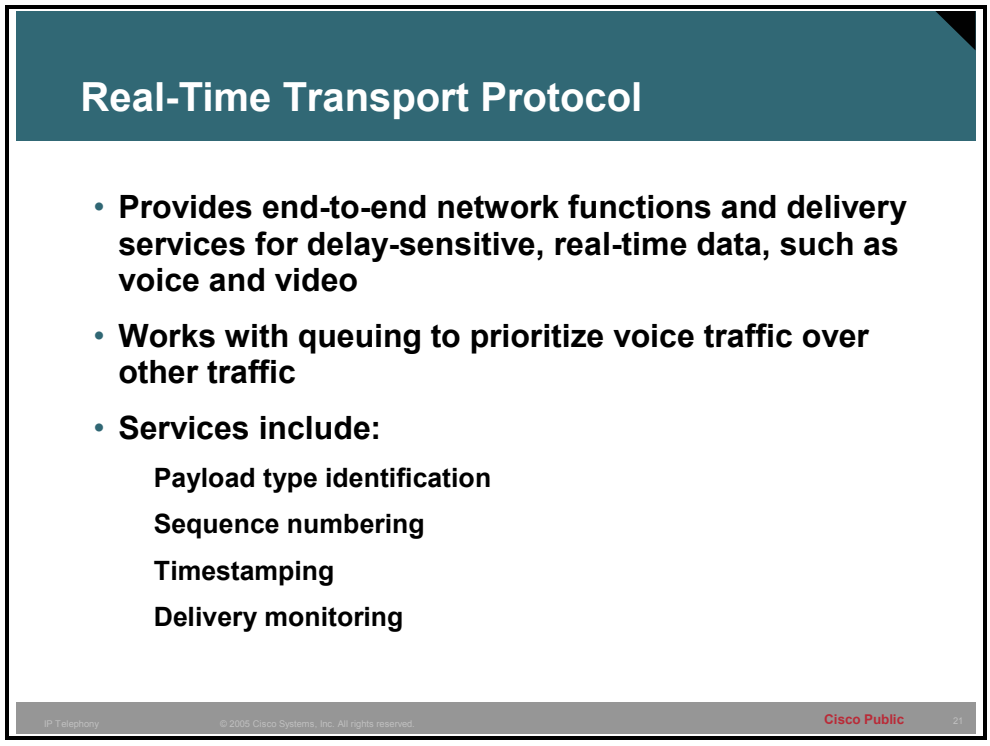
The following G.729 codec combinations interoperate:

- G.729 and G.729A
- G.729 and G.729
- G.729A and G.729A
- G.729B and G.729AB
- G.729B and G.729B
- G.729AB and G.729AB

 Copyright © 2005, Cisco Systems, Inc.

Encapsulating Voice in IP Packets

This topic describes the functions of RTP and RTCP as they relate to the VoIP network.



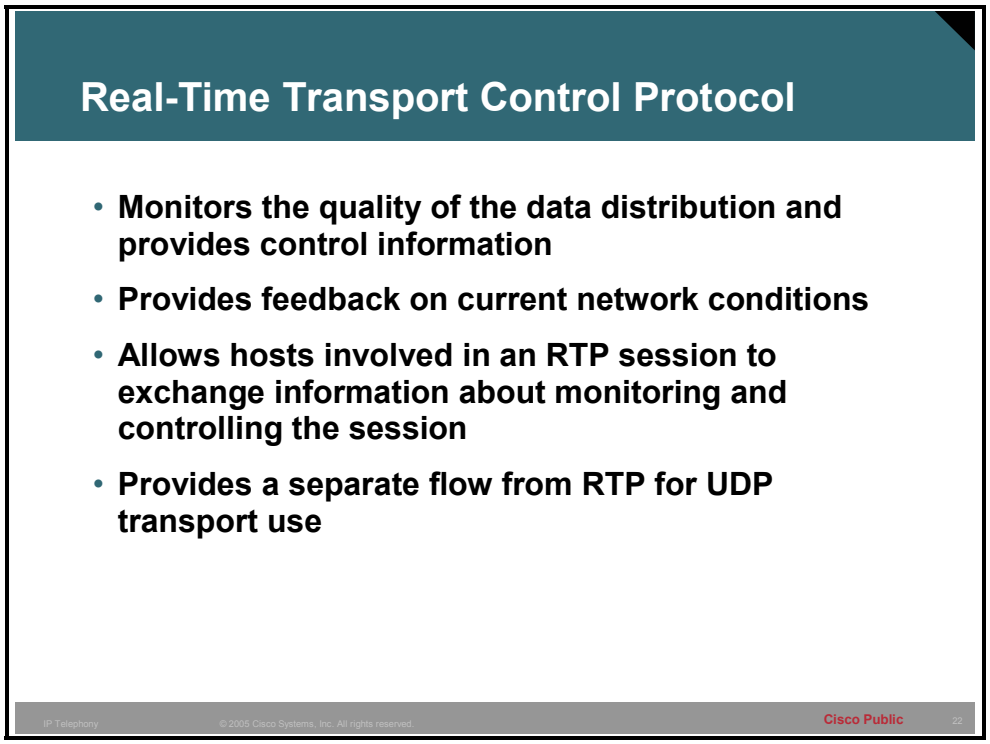
RTP provides end-to-end network transport functions intended for applications transmitting real-time requirements, such as audio and video. Those functions include payload type identification, sequence numbering, time stamping, and delivery monitoring.

RTP typically runs on top of UDP to utilize the multiplexing and checksum services of that protocol. Although RTP is often used for unicast sessions, it is primarily designed for multicast sessions. In addition to the roles of sender and receiver, RTP also defines the roles of translator and mixer to support the multicast requirements.

Example

RTP is a critical component of VoIP because it enables the destination device to reorder and retime the voice packets before they are played out to the user. An RTP header contains a time stamp and sequence number, which allows the receiving device to buffer and remove jitter and latency by synchronizing the packets to play back a continuous stream of sound. RTP uses sequence numbers to order the packets only. RTP does not request retransmission if a packet is lost.

For more information on RTP, refer to RFC 1889.



RTCP monitors the quality of the data distribution and provides control information. RTCP provides the following feedback on current network conditions:

- RTCP provides a mechanism for hosts involved in an RTP session to exchange information about monitoring and controlling the session. RTCP monitors the quality of elements such as packet count, packet loss, delay, and inter-arrival jitter. RTCP transmits packets as a percentage of session bandwidth, but at a specific rate of at least every 5 seconds.

- The RTP standard states that the Network Time Protocol (NTP) time stamp is based on synchronized clocks. The corresponding RTP time stamp is randomly generated and based on data-packet sampling. Both NTP and RTP are included in RTCP packets by the sender of the data.

- RTCP provides a separate flow from RTP for transport use by UDP. When a voice stream is assigned UDP port numbers, RTP is typically assigned an even-numbered port and RTCP is assigned the next odd-numbered port. Each voice call has four ports assigned: RTP plus RTCP in the transmit directions and RTP plus RTCP in the receive direction.

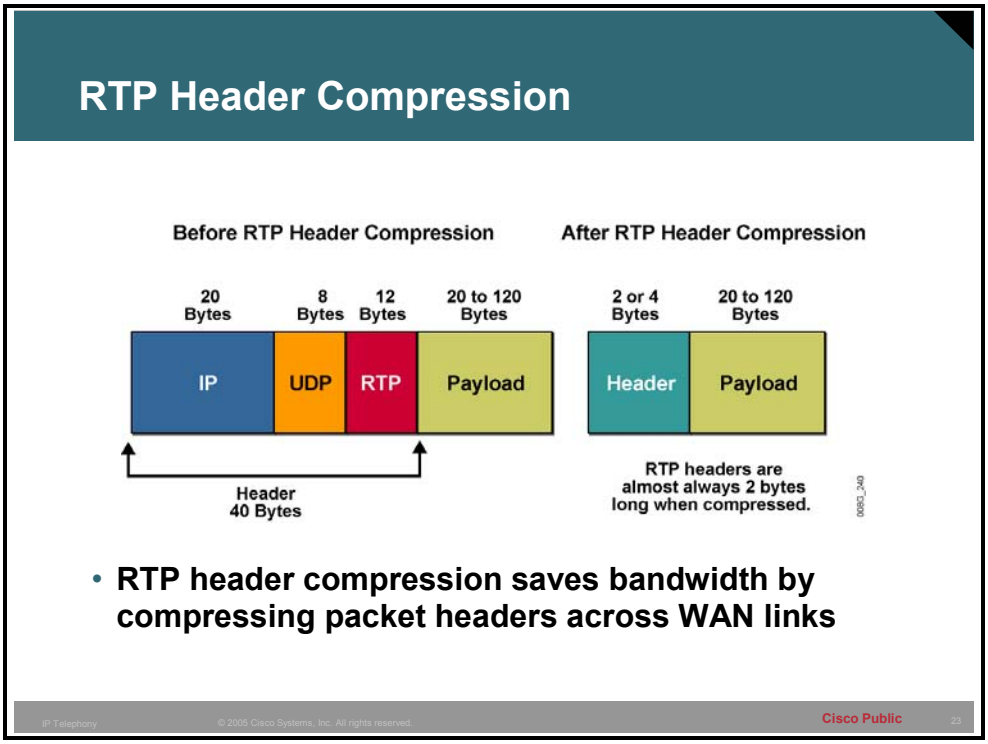
Example

Throughout the duration of each RTP call, the RTCP report packets are generated at least every 5 seconds. In the event of poor network conditions, a call may be disconnected due to high packet loss. When viewing packets using a packet analyzer, a network administrator could check information in the RTCP header that includes packet count, octet count, number of packets lost, and jitter. The RTCP header information would shed light on why the calls were disconnected.

 Copyright © 2005, Cisco Systems, Inc.

Encapsulating Voice in IP Packets: Compressed Real-Time Transport Protocol (CRTP)

This topic describes how IP voice headers are compressed using CRTP.



Given the number of multiple protocols that are necessary to transport voice over an IP network, the packet header can be large. You can use cRTP headers on a link-by-link basis to save bandwidth.

Using CRTP compresses the IP/UDP/RTP header from 40 bytes to 2 bytes without UDP checksums and from 40 bytes to 4 bytes with UDP checksums. RTP header compression is especially beneficial when the RTP payload size is small; for example, with compressed audio payloads are 20 and 50 bytes.

In addition, CRTP works on the premise that most of the fields in the IP/UDP/RTP header do not change, or that the change is predictable. Static fields include source and destination IP address, source and destination UDP port numbers, as well as many other fields in all three headers. For those fields where the change is predictable, the CRTP process is illustrated in the following table:

Table 1: CRTP

Stage	What Happens
The change is predictable.	The sending side tracks the predicted change.
The predicted change is tracked.	The sending side sends a hash of the header.
The receiving side predicts what the constant change is.	The receiving side substitutes the original stored header and calculates the changed fields.
There is an unexpected change.	The sending side sends the entire header without compression.

RTP Packet Components

In a packet voice environment using G.729 and when speech samples are framed every 20 ms, a payload of 20 bytes is generated. Without CRTP, the total packet size includes the following components:

- IP header (20 bytes)
- UDP header (8 bytes)
- RTP header (12 bytes)
- Payload (20 bytes)

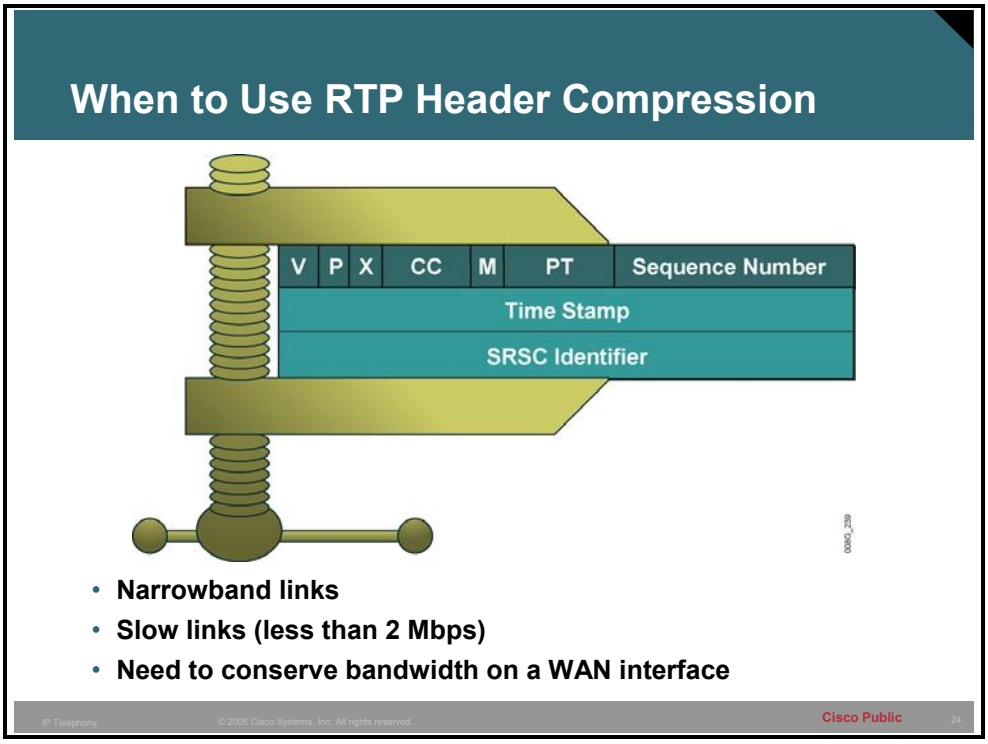
The header is twice the size of the payload; IP/UDP/RTP (20 + 8 + 12 = 40 bytes) vs. payload (20 bytes). When generating packets every 20 ms on a slow link, the header consumes a large portion of bandwidth.

In the figure, RTP header compression reduces the header to 2 bytes. The compressed header is $1/10^{th}$ the payload size.

 Copyright © 2005, Cisco Systems, Inc.

Encapsulating Voice in IP Packets: Using CRTP

This topic describes when to use CRTP.



You must configure CRTP on a specific serial interface or subinterface if you have any of these conditions:

- Congested WAN links
- Slow links (less than 2 Mbps)
- Need to conserve bandwidth on a WAN interface

Compression works on a link-by-link basis and must be enabled for each link that fits these requirements. You must enable compression on both sides of the link for proper results. Enabling compression on both ends of a low-bandwidth serial link can greatly reduce the network overhead if there is a significant volume of RTP traffic on that slow link.

Note	Compression adds to processing overhead. You must check resource availability on each device prior to turning on RTP header compression.

Example

If you want the router to compress RTP packets, use the **ip rtp header-compression** command. The **ip rtp header-compression** command defaults to active mode when it is configured. However, this command provides a passive mode setting in instances where you want the router to compress RTP packets *only* if it has received compressed RTP on that interface. When

applying to a Frame Relay interface, use the **frame-relay ip rtp header-compression** command.

By default, the software supports a total of 16 RTP header compression connections on an interface. Depending on the traffic on the interface, you can change the number of header compression connections with the **ip rtp compression-connections *number*** command.

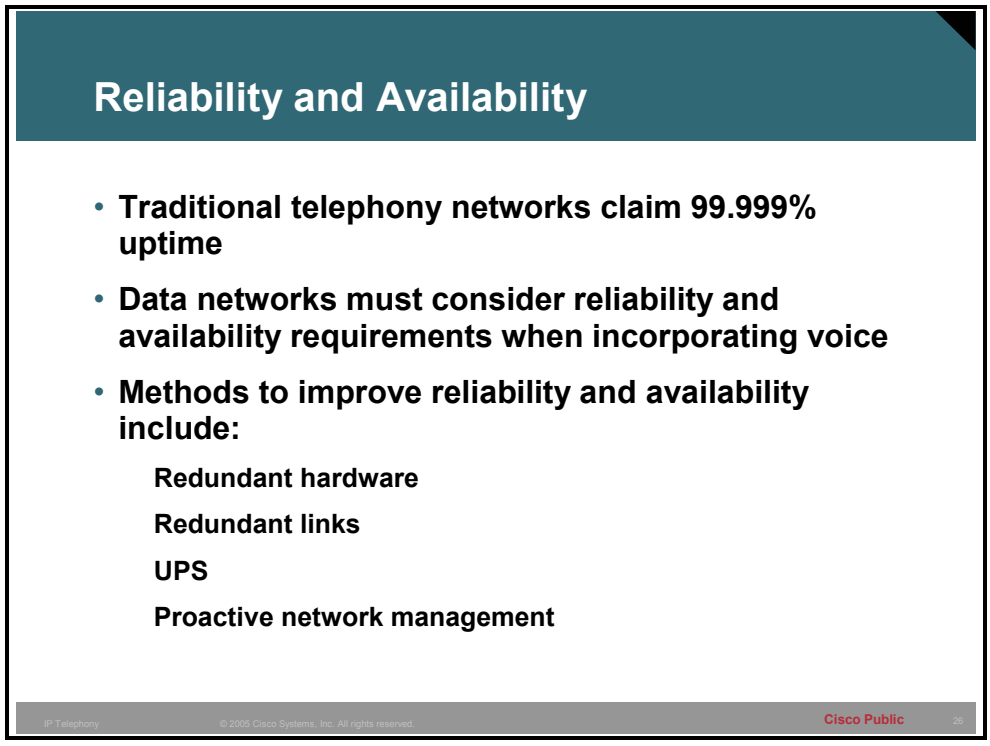
Note	Do not use CRTP if the link is faster than 2 Mbps.

 Copyright © 2005, Cisco Systems, Inc.

Challenges and Solutions in VoIP

Challenges in VoIP

The traditional telephony network strives to provide 99.99 percent uptime to the user. This corresponds to 5.25 minutes per year of down time. Many data networks cannot make the same claim. This topic describes methods that you can use to improve reliability and availability in data networks.



To provide telephony users the same—or close to the same—level of service as they experience with traditional telephony, the reliability and availability of the data network takes on new importance.

When the data network goes down, it may not come back up for minutes or even hours. This delay is unacceptable for telephony users. Local users, with network equipment such as voice-enabled routers, gateways, or switches for IP Phones, now find that their connectivity is terminated. Administrators must, therefore, provide an uninterruptible power supply (UPS) to these devices *in addition* to providing network availability. Previously, depending on the type of connection the user had, they received their power directly from the telephone company central office (CO) or through a UPS that was connected to their keyswitch or PBX in the event of a power outage. Now the network devices must have protected power to continue to function and provide power to the end devices.

Network reliability comes from incorporating redundancy into the network design. In traditional telephony, switches have multiple redundant connections to other switches. If either a link or a switch becomes unavailable, the telephone company can route the call in different ways. This is why telephone companies can claim a high availability rate.

High availability encompasses many areas of the network. In a fully redundant network, the following components need to be duplicated:

- Servers and call managers
- Access layer devices, such as LAN switches
- Distribution layer devices, such as routers or multilayer switches
- Core layer devices, such as multilayer switches
- Interconnections, such as WAN links, even through different providers
- Power supplies and UPSs

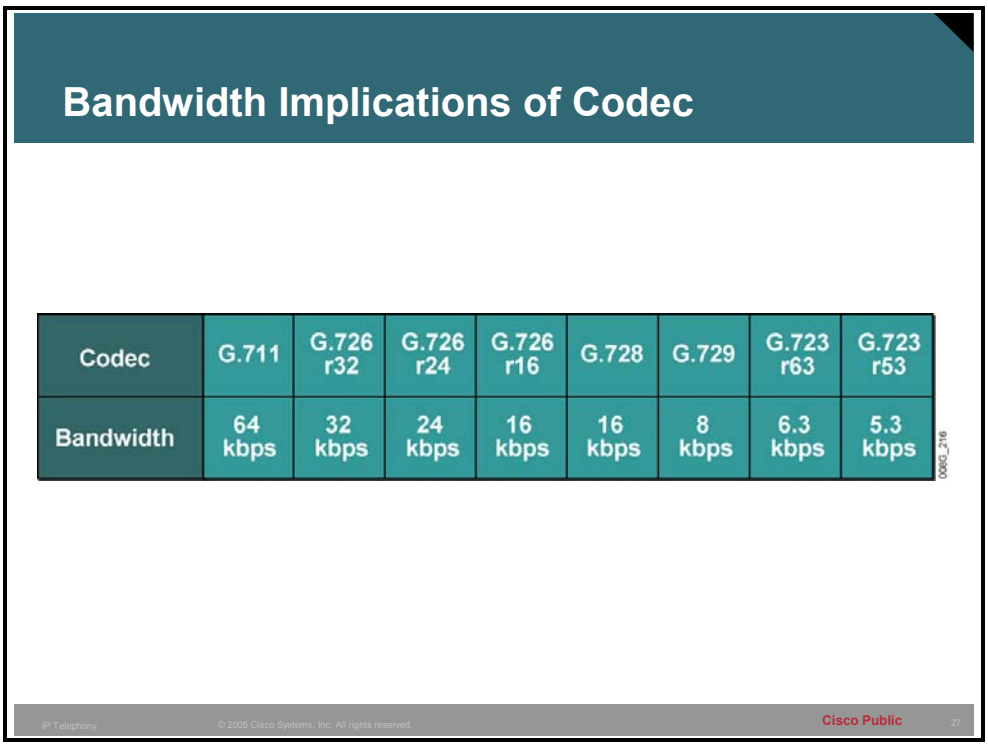
In some data networks, a high level of availability and reliability is not critical enough to warrant financing the hardware and links required to provide complete redundancy. If voice is layered onto the network, these requirements need to be revisited.

With Cisco Architecture for Voice, Video and Integrated Data (AVVID) technology, the use of Cisco CallManager clusters provides a way to design redundant hardware in the event of Cisco CallManager failure. When using gatekeepers, you can configure backup devices as secondary gatekeepers in case the primary gatekeeper fails. You must also revisit the network infrastructure. Redundant devices and Cisco IOS services, like Hot Standby Router Protocol (HSRP), can provide high availability. For proactive network monitoring and trouble reporting, a network management platform such as CiscoWorks2000 provides a high degree of responsiveness to network issues.

 Copyright © 2005, Cisco Systems, Inc.

Bandwidth Requirements in VoIP

This topic describes the bandwidth that each coder-decoder (codec) uses and illustrates its impact on total bandwidth.



One of the most important factors for the network administrator to consider while building voice networks is proper capacity planning. Network administrators must understand how much bandwidth is used for each Voice over IP (VoIP) call. With a thorough understanding of VoIP bandwidth, the network administrator can apply capacity-planning tools.

Following is a list of codecs and their associated bandwidth.

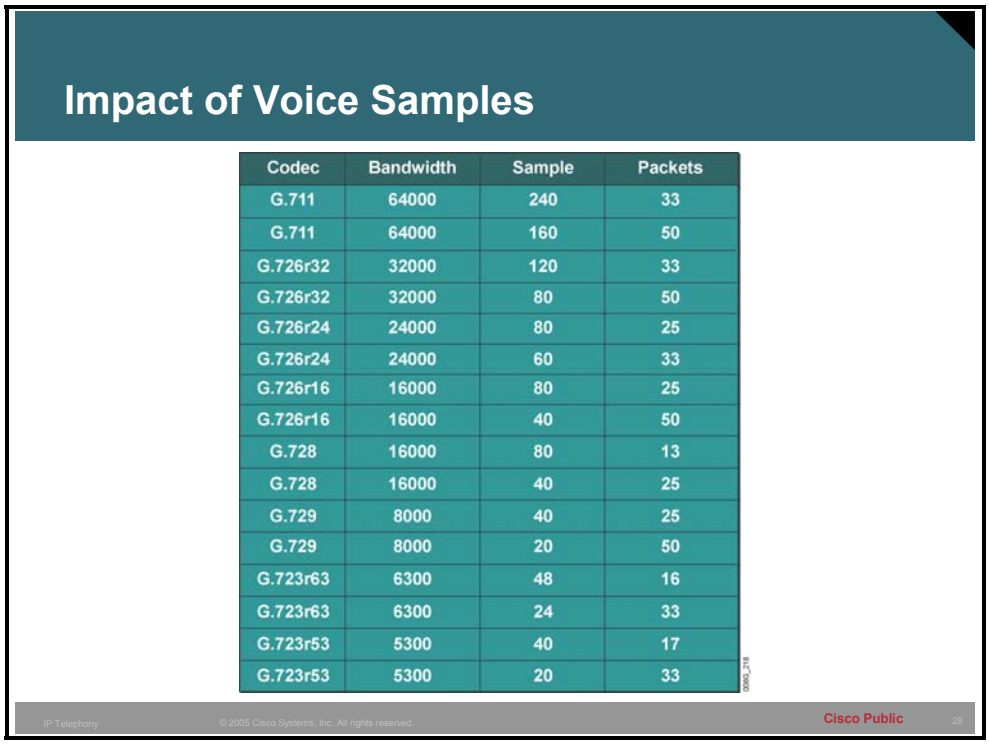
- The G.711 pulse code modulation (PCM) coding scheme uses the most bandwidth. It takes samples 8000 times per second, each of which is 8 bits in length, for a total of 64000 bps.
- The G.726 adaptive differential pulse code modulation (ADPCM) coding schemes use somewhat less bandwidth. While each coding scheme takes samples 8000 times per second like PCM, it uses 4, 3, or 2 bits for each sample. The 4, 3, or 2 bits for each sample results in total bandwidths of 32000, 24000, or 16000 bps.
- The G.728 low delay-code excited linear prediction (LD-CELP) coding scheme compresses PCM samples using codebook technology. It uses a total bandwidth of 16000 bps.
- The G.729 and G.729a Conjugate Structure Algebraic Code Excited Linear Prediction (CS-ACELP) coding scheme also compresses PCM using advanced codebook technology. It uses 8000 bps total bandwidth.

- The G.723 and G.723a multipulse maximum likelihood quantization (MPMLQ) coding schemes use a look-ahead algorithm. These compression schemes result in 6300 or 5300 bps.

The network administrator should balance the need for voice quality against the cost of bandwidth in the network when choosing codecs. The higher the codec bandwidth, the higher the cost of each call across the network.

Bandwidth Requirements in VoIP: Impact of Voice Samples

This topic illustrates the effect of voice sample size on bandwidth.



Codec	Bandwidth	Sample	Packets
G.711	64000	240	33
G.711	64000	160	50
G.726r32	32000	120	33
G.726r32	32000	80	50
G.726r24	24000	80	25
G.726r24	24000	60	33
G.726r16	16000	80	25
G.726r16	16000	40	50
G.728	16000	80	13
G.728	16000	40	25
G.729	8000	40	25
G.729	8000	20	50
G.723r63	6300	48	16
G.723r63	6300	24	33
G.723r53	5300	40	17
G.723r53	5300	20	33

Voice sample size is a variable that can affect total bandwidth used. A voice sample is defined as the digital output from a codec digital signal processor (DSP) that is encapsulated into a protocol data unit (PDU). Cisco uses DSPs that output samples based on digitization of 10 ms worth of audio. Cisco voice equipment encapsulates 20 ms of audio in each PDU by default, regardless of the codec used. You can apply an optional configuration command to the dial peer to vary the number of samples encapsulated. When you encapsulate more samples per PDU, total bandwidth is reduced. However, encapsulating more samples per PDU comes at the risk of larger PDUs, which can cause variable delay and severe gaps if PDUs are dropped.

Example

Using a simple formula, it is possible for you to determine the number of bytes encapsulated in a PDU based on the codec bandwidth and the sample size (20 ms is default):

Bytes_per_Sample = (*Sample_Size* * *Codec_Bandwidth*) / 8

If we apply G.711 numbers, the formula reveals the following:

 Copyright © 2005, Cisco Systems, Inc.

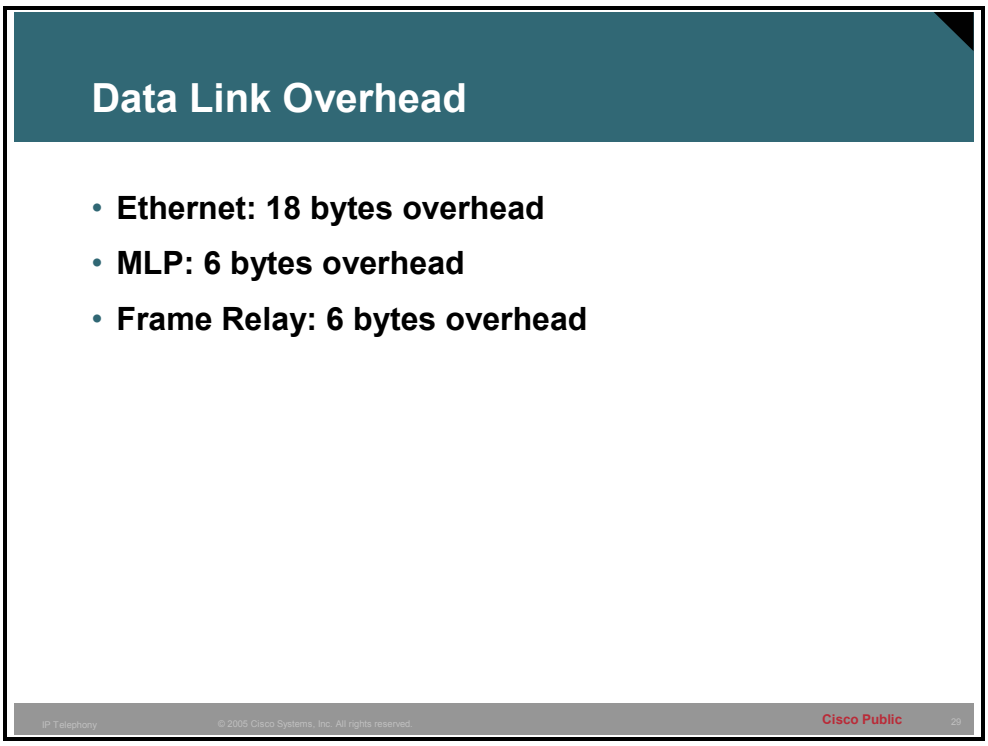
Bytes_per_Sample = (.020 x 64000) / 8

Bytes_per_Sample = 160

The figure illustrates various codecs and sample sizes and the number of packets that are required for VoIP to transmit one second of audio. The larger the sample size, the larger the packet, and the fewer the encapsulated samples that have to be sent (which reduces bandwidth).

Bandwidth Requirements in VoIP: Data Link Overhead

This topic lists overhead sizes for various Layer 2 protocols.

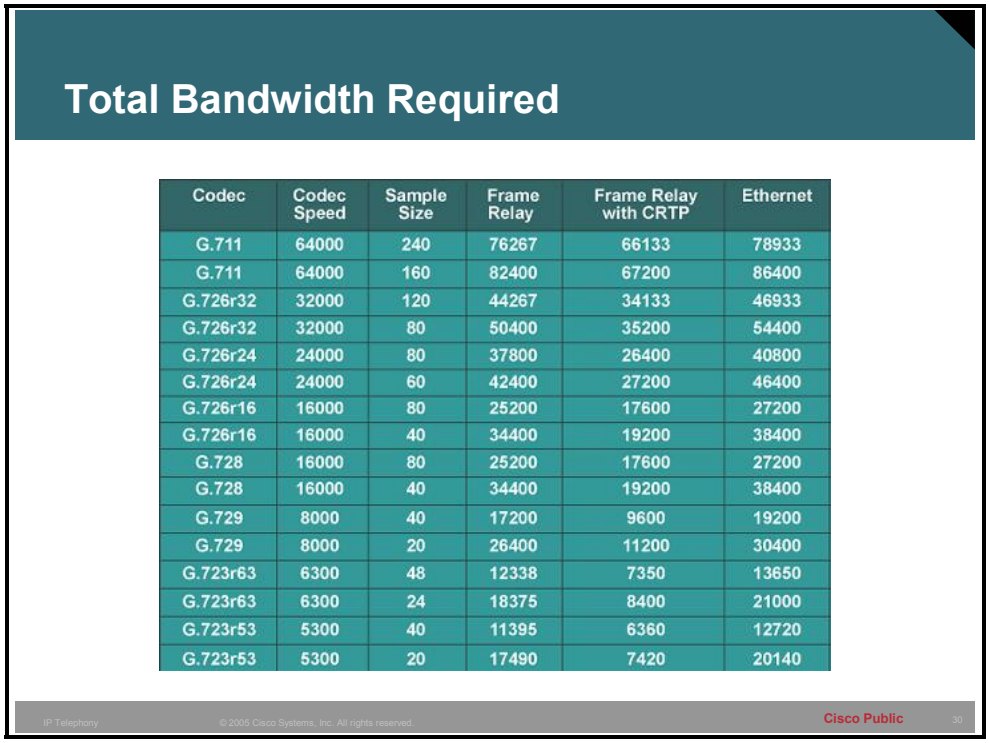


Another contributing factor to bandwidth is the Layer 2 protocol used to transport VoIP. VoIP alone carries a 40-byte IP/User Datagram Protocol/Real-Time Transport Protocol (IP/UDP/RTP) header, assuming uncompressed RTP. Depending on the Layer 2 protocol used, the overhead could grow substantially. The larger the Layer 2 overhead, the more bandwidth required to transport VoIP. The following points illustrate the Layer 2 overhead for various protocols:

- **Ethernet II:** Carries 18 bytes of overhead; 6 bytes for source MAC, 6 bytes for destination MAC, 2 bytes for type, and 4 bytes for cyclic redundancy check (CRC)
- **Multilink Point-to-Point Protocol (MLP):** Carries 6 bytes of overhead; 1 byte for flag, 1 byte for address, 2 bytes for control (or type), and 2 bytes for CRC
- **FRF.12:** Carries 6 bytes of overhead; 2 bytes for data-link connection identifier (DLCI) header, 2 bytes for FRF.12, and 2 bytes for CRC

Bandwidth Requirements in VoIP: Total Bandwidth Required

This topic calculates the total bandwidth required for a VoIP call using codec, data link, and sample size.



Codec	Codec Speed	Sample Size	Frame Relay	Frame Relay with CRTP	Ethernet
G.711	64000	240	76267	66133	78933
G.711	64000	160	82400	67200	86400
G.726r32	32000	120	44267	34133	46933
G.726r32	32000	80	50400	35200	54400
G.726r24	24000	80	37800	26400	40800
G.726r24	24000	60	42400	27200	46400
G.726r16	16000	80	25200	17600	27200
G.726r16	16000	40	34400	19200	38400
G.728	16000	80	25200	17600	27200
G.728	16000	40	34400	19200	38400
G.729	8000	40	17200	9600	19200
G.729	8000	20	26400	11200	30400
G.723r63	6300	48	12338	7350	13650
G.723r63	6300	24	18375	8400	21000
G.723r53	5300	40	11395	6360	12720
G.723r53	5300	20	17490	7420	20140

Codec choice, data-link overhead, sample size, and even compressed RTP, all have positive and negative impacts on total bandwidth. To perform the calculations, you must have all of the contributing factors as part of the equation:

- More bandwidth required for the codec = more total bandwidth required
- More overhead associated with the data link = more total bandwidth required
- Larger sample size = less total bandwidth required
- Compressed RTP = significantly reduced total bandwidth required

Example

The following calculation was used to produce the figure:

Total_Bandwidth = ([*Layer_2_Overhead* + *IP_UDP_RTP Overhead* + *Sample_Size*] / *Sample_Size*) * *Codec_Speed*

For example, assume a G.729 codec, 20-byte sample size, using Frame Relay without compressed Real-Time Transport Protocol (cRTP):

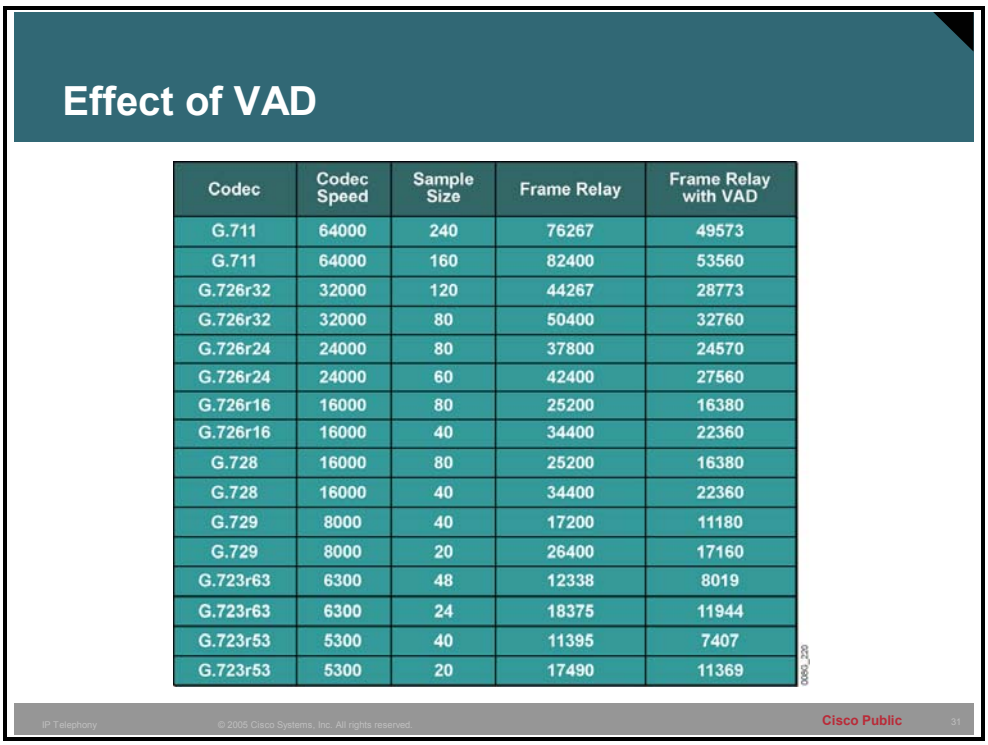
Total_Bandwidth = ([6 + 40 +20]/20) * 8000

 Copyright © 2005, Cisco Systems, Inc.

Total_Bandwidth = 26400 bps

Bandwidth Requirements in VoIP: Effect of VAD

This topic describes the effect of voice activity detection (VAD) on total bandwidth.



Codec	Codec Speed	Sample Size	Frame Relay	Frame Relay with VAD
G.711	64000	240	76267	49573
G.711	64000	160	82400	53560
G.726r32	32000	120	44267	28773
G.726r32	32000	80	50400	32760
G.726r24	24000	80	37800	24570
G.726r24	24000	60	42400	27560
G.726r16	16000	80	25200	16380
G.726r16	16000	40	34400	22360
G.728	16000	80	25200	16380
G.728	16000	40	34400	22360
G.729	8000	40	17200	11180
G.729	8000	20	26400	17160
G.723r63	6300	48	12338	8019
G.723r63	6300	24	18375	11944
G.723r53	5300	40	11395	7407
G.723r53	5300	20	17490	11369

On average, an aggregate of 24 calls or more may contain 35 percent silence. With traditional telephony voice networks, all voice calls use 64-kbps fixed-bandwidth links regardless of how much of the conversation is speech and how much is silence. With Cisco VoIP networks, all conversation and silence is packetized. VAD suppresses packets of silence. Instead of sending VoIP packets of silence, VoIP gateways interleave data traffic with VoIP conversations to more effectively use network bandwidth.

VAD provides a maximum of 35 percent bandwidth savings based on an average volume of more than 24 calls.

Note Bandwidth savings of 35 percent is an average figure and does not take into account loud background sounds, differences in languages, and other factors.

The savings are not realized on every individual voice call, or on any specific point measurement.

Note For the purposes of network design and bandwidth engineering, VAD should *not* be taken into account, especially on links that will carry fewer than 24 voice calls simultaneously.

Various features, such as music on hold (MOH) and fax, render VAD ineffective. When the network is engineered for the full voice call bandwidth, all savings provided by VAD are available to data applications.

VAD is enabled by default for all VoIP calls. VAD reduces the silence in VoIP conversations but it also provides comfort noise generation (CNG). Because you can mistake silence for a disconnected call, CNG provides locally generated *white noise* to make the call appear normally connected to both parties.

Example

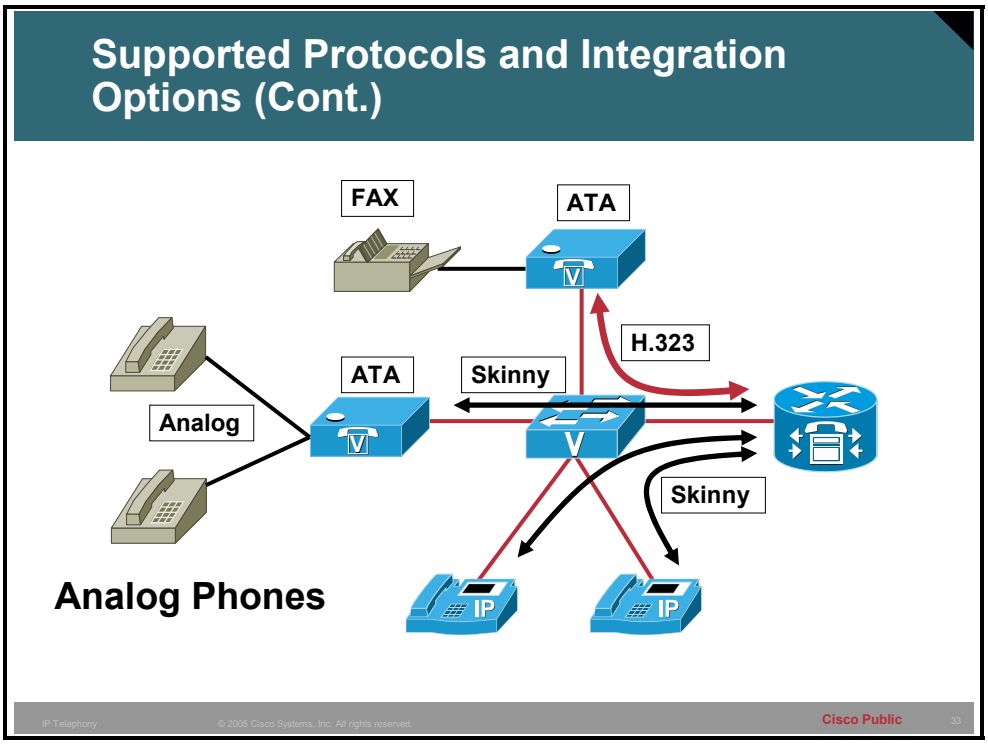
The figure shows examples of the VAD effect in a Frame Relay VoIP environment. In the example using G.711 with a 160-byte payload, the bandwidth required is 82400 bps. By turning VAD on, you can reduce the bandwidth utilization to 53560bps. This is a savings of 35 percent bandwidth.

 Copyright © 2005, Cisco Systems, Inc.

Cisco CME Features and Functionality

Supported Protocols and Integration Options

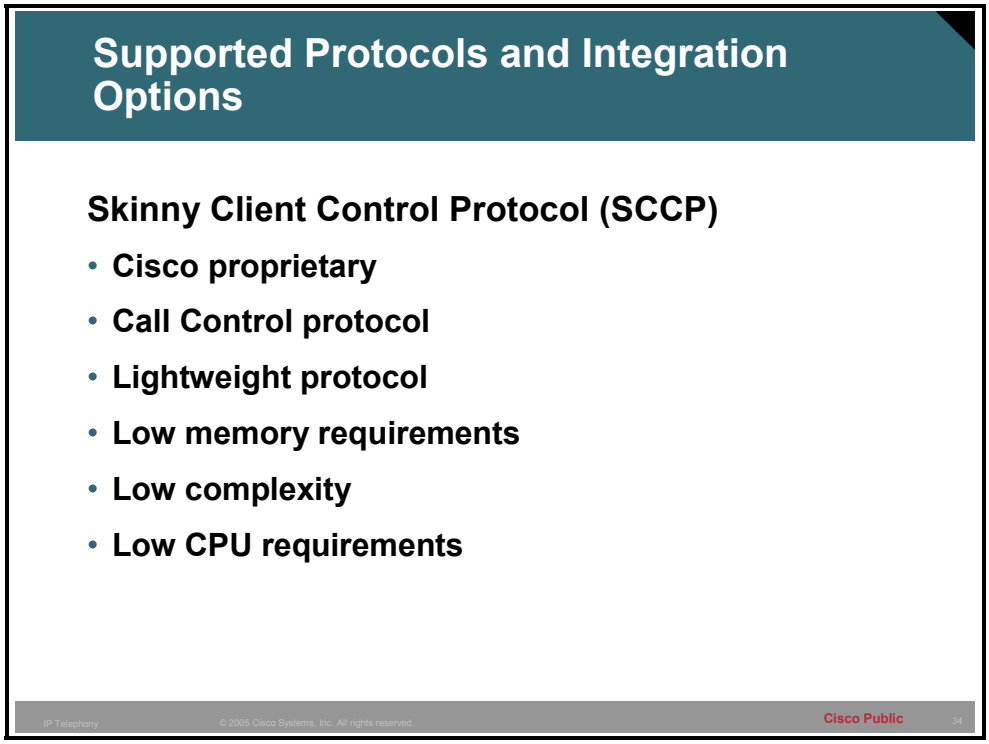
This topic describes the supported protocols and integration options of Cisco CME.



Cisco CME can use both H.323 and the Skinny protocol to control IP phones, analog phones, and faxes.

Supported Protocols and Integration Options: Skinny Client Control Protocol (SCCP)

This topic describes the supported protocols and integration options of Cisco CME.

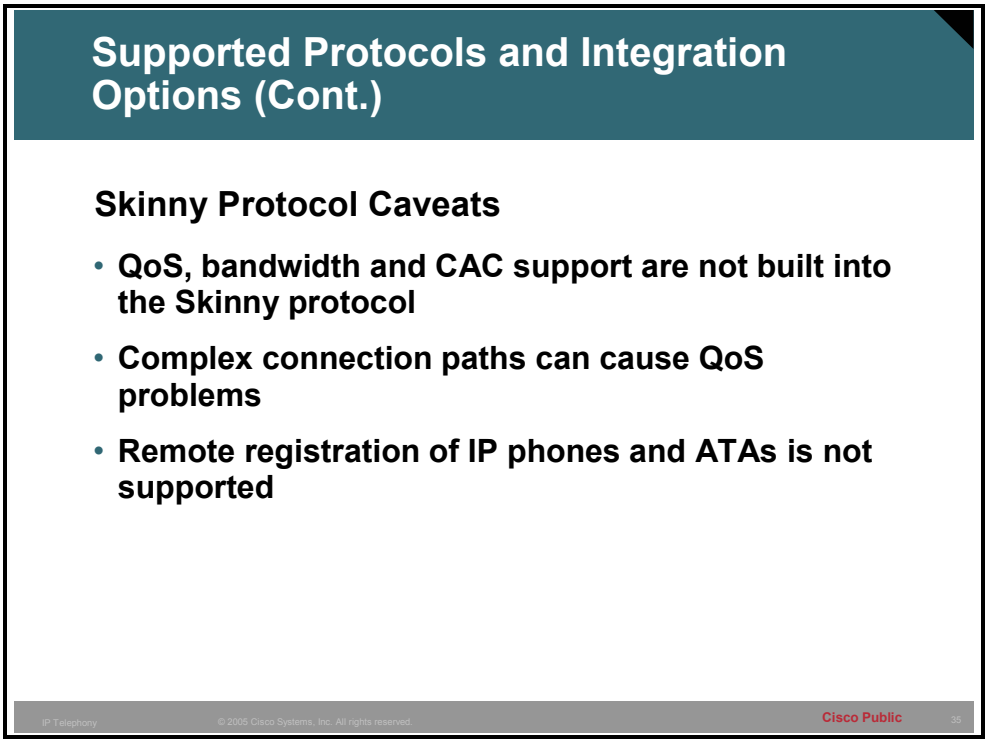


Cisco CME software provides call processing for IP Phones using the Skinny Client Control Protocol (SCCP). SCCP is the Cisco proprietary protocol for real-time calls and conferencing over IP. This generalized messaging set allows Cisco IP Phones to coexist in an H.323 environment. Savings in memory size, processor power, and complexity are benefits of SCCP.

 Copyright © 2005, Cisco Systems, Inc.

Supported Protocols and Integration Options: Skinny Protocol Caveats

This topic describes the supported protocols and integration options of Cisco CME.



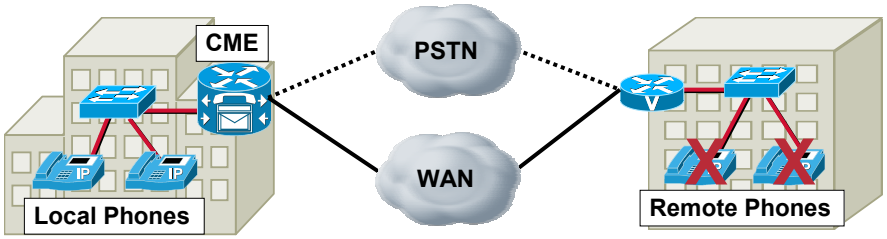
All IP phones must be connected locally to the Cisco CME router because of the factors shown here.

QoS, bandwidth management, and Call Admission Control (CAC) are not supported within the Skinny protocol context on Cisco CME. Complex connection paths could cause QoS problems.

Compressed Real-time Transport Protocol (CRTP) is not supported.

Supported Protocols and Integration Options (Cont.)

- **Cisco CME does not support remotely registered phones**



IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 36

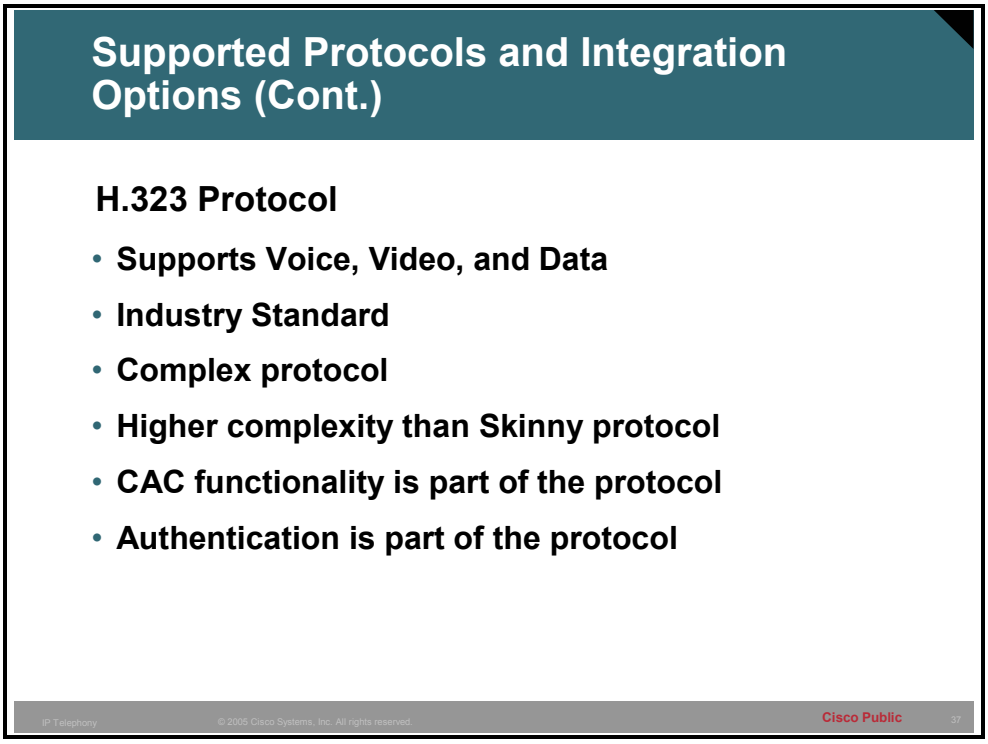
Cisco CME does not support remotely registered phones via a WAN or virtual private network (VPN) connection because the Skinny interface does not have the necessary set of QoS tools; these tools have been built into the H.323/VoIP interface to cope with operating across non-local networks. Cisco CME also does not support bandwidth control or accounting, RSVP, or the max-conn attribute for remotely registered SCCP phones via a WAN or virtual private network (VPN) connection.

Each remote site should have a Cisco CME router so IP phones can register locally. VoIP interworking between multiple Cisco CME routers across the WAN is supported via the H.323 protocol.

 Copyright © 2005, Cisco Systems, Inc.

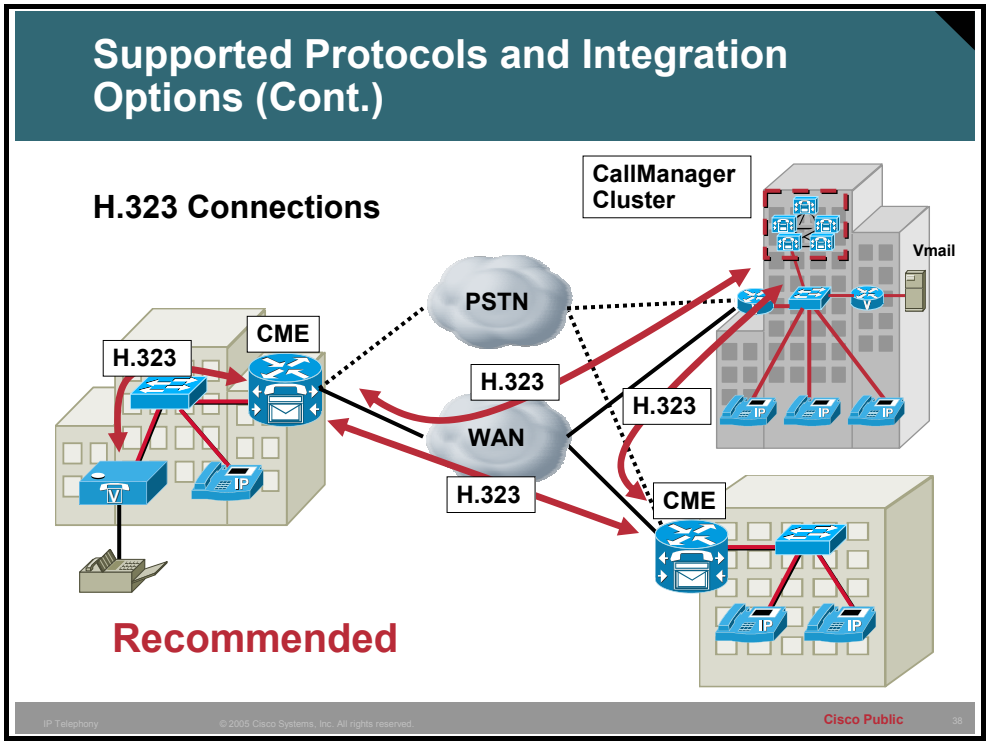
Supported Protocols and Integration Options: H.323 Protocol

This topic describes the supported protocols and integration options of Cisco CME.



H.323 is a specification for transmitting audio, video, and data across an IP network, including the Internet. H.323 is an extension of the ITU Telecommunication Standardization Sector standard H.320.

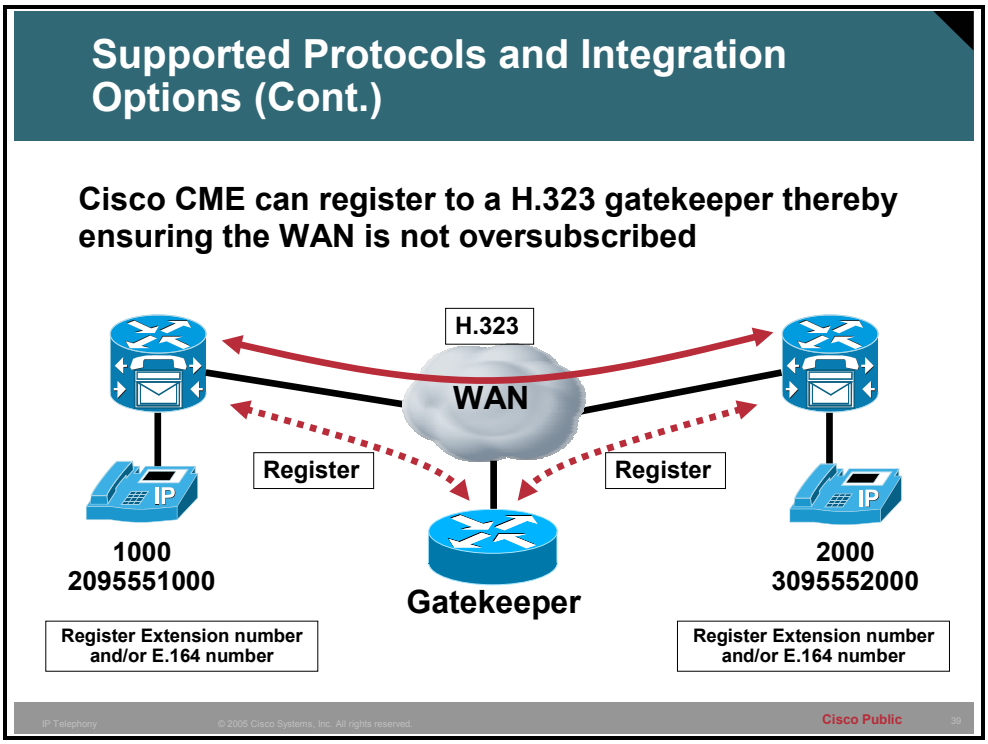
Tip	The ATA will need to be configured with H.323 when fax machines are connected to the analog ports.



H.323 is a specification for transmitting audio, video, and data across an IP network, including the Internet. H.323 is an extension of the ITU Telecommunication Standardization Sector standard H.320.

In this slide, the H.323 protocol is used to connect the Cisco CME router together and for controlling the analog fax connected to the ATA.

 Copyright © 2005, Cisco Systems, Inc.



The Cisco CME system can be configured to register the ephone-dns with a H.323 Gatekeeper. In addition, the IP phone may have both an extension number and an E.164 number defined, and one or both of the numbers may be registered with the H.323 Gatekeeper. H.323 can also be used to allow one Cisco CME to communicate with another Cisco CME or Voice Gateways. A router separate from Cisco CME must be used if gatekeeper is going to be configured.

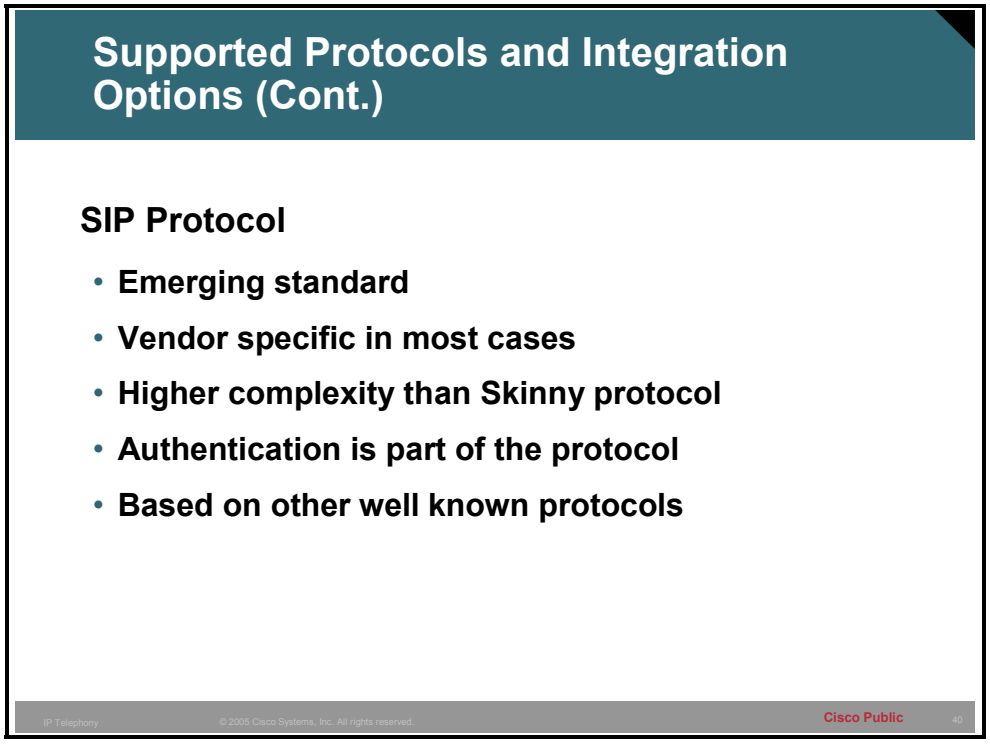
The H.323 Gatekeeper can provide the following functions:

- **CAC –** Call Admission Control over a WAN link to ensure that the WAN link is not oversubscribed
- **Dial plan administration -** Centralizing the dial plan for inter-site numbering
- **IP-to-IP Gateway –** Provides a network to network point for billing, security, and for joining two VoIP call legs together

Please refer to other Cisco documentation for details on Cisco Gatekeepers.

Supported Protocols and Integration Options: SIP Protocol

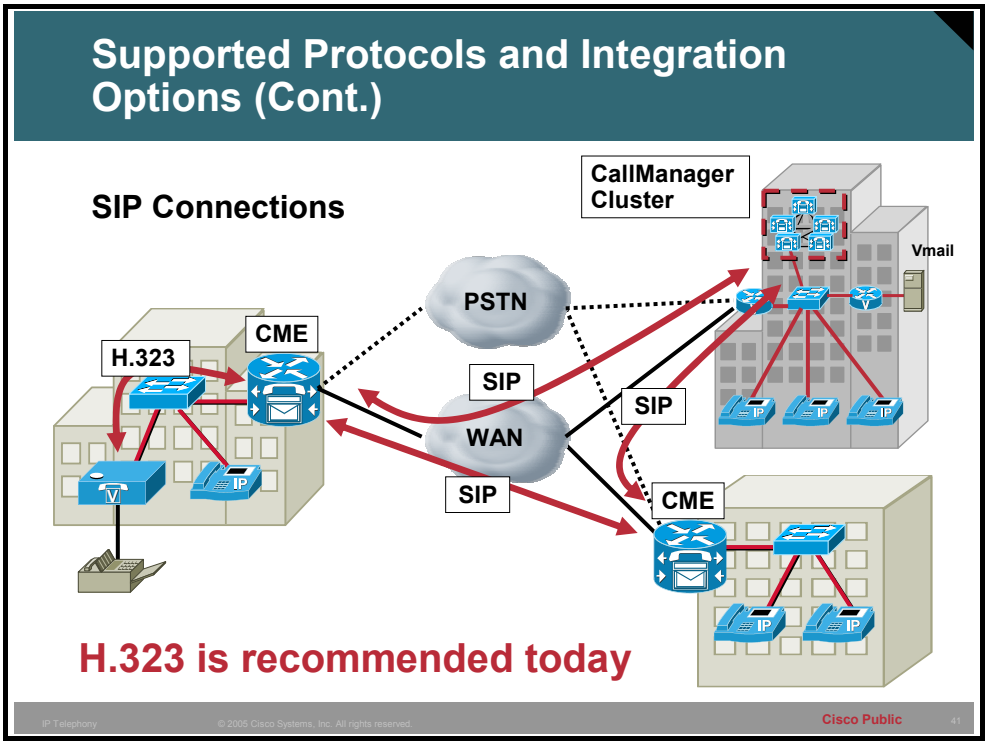
This topic describes the supported protocols and integration options of Cisco CME.



SIP was designed as a multimedia protocol that could take advantage of the architecture and messages found in popular Internet applications. By using a distributed architecture—with URLs for naming and text-based messaging—SIP attempts to take advantage of the Internet model for building VoIP networks and applications. In addition to VoIP, SIP is used for videoconferencing and instant messaging.

As a protocol, SIP only defines how sessions are to be set up and torn down. It utilizes other IETF protocols to define other aspects of VoIP and multimedia sessions, such as SDP for capabilities exchange, URLs for addressing, Domain Name System (DNS) for service location, and Telephony Routing over IP (TRIP) for call routing.

 Copyright © 2005, Cisco Systems, Inc.



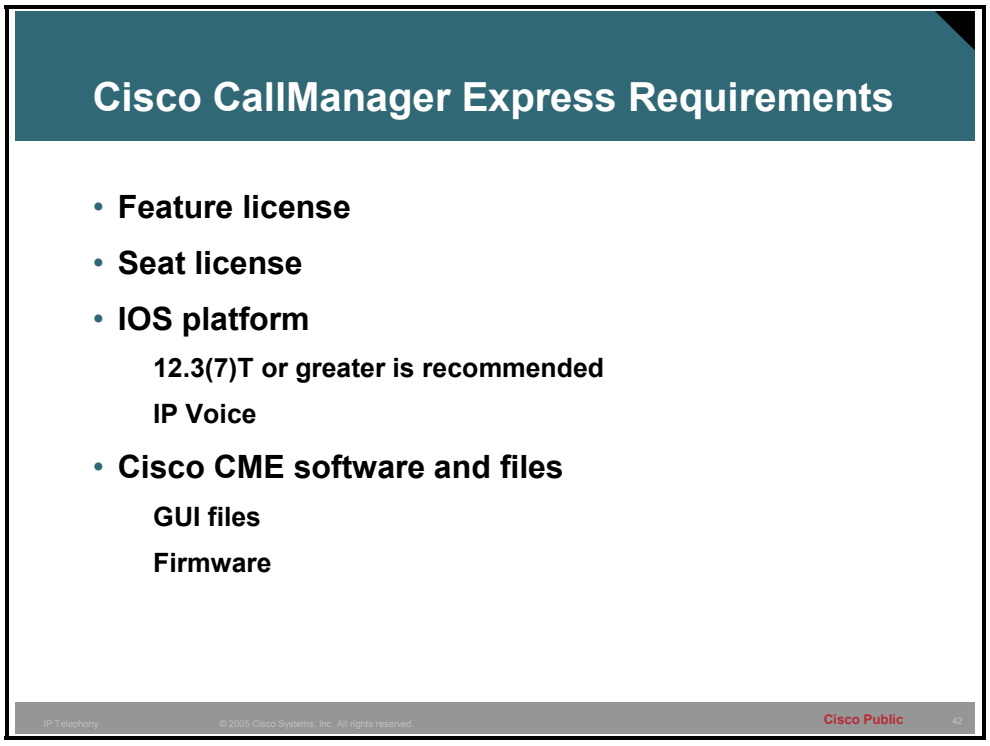
The SIP protocol can be used to connect calls between two Cisco CME systems. This is currently not the recommended solution and vendor compatibility is problematic.

Note	It is recommended to use H.323 to connect Cisco CME systems together.

.

Cisco CallManager Express Requirements

This topic describes Cisco CME requirements.

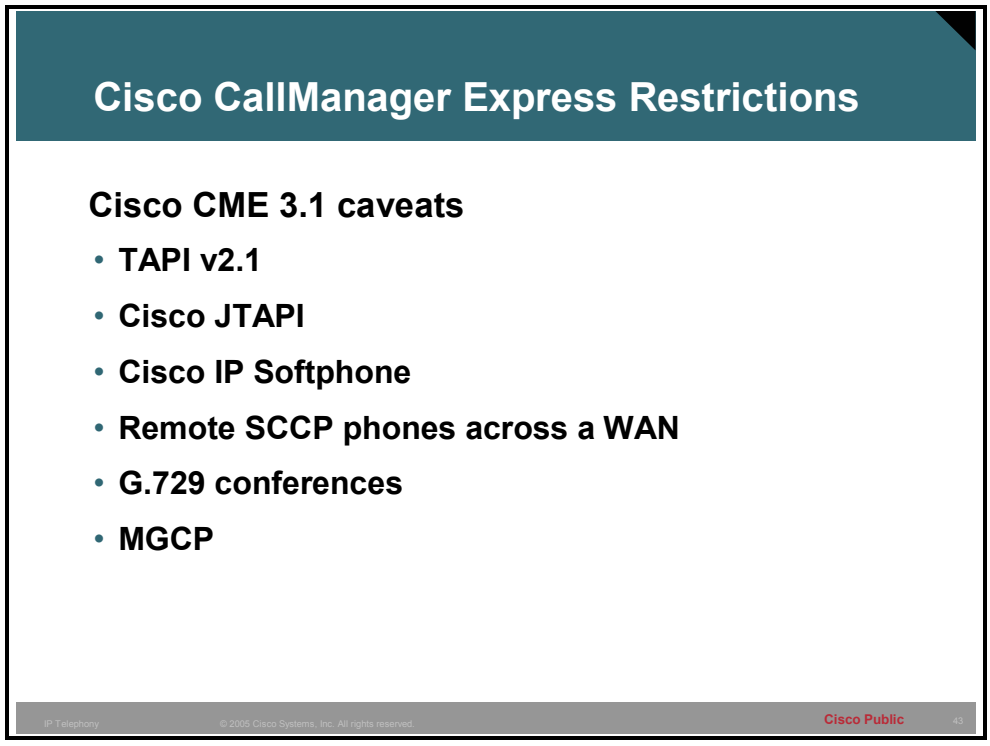


Cisco CME requires a Cisco CME feature license. This is licensed based on the number of IP phones that will be deployed. The router itself will need to have the correct IOS that is Cisco CME-capable. Each IP Phone or ATA port also requires a Cisco CME seat license, which can be purchased with the IP phone. You also need an account on Cisco.com to download Cisco CME files, such as phone firmware and GUI files and firmware.

 Copyright © 2005, Cisco Systems, Inc.

Cisco CallManager Express Restrictions

This topic describes Cisco CME restrictions.



There is subset or TAPI 2.1 support in the Cisco CME. This will be covered in detail on the next page. Cisco JTAPI is not currently supported and this limitation restricts the use of a Cisco IP Softphone. The newer softphone called IP communicator is also not currently supported although it may be in future versions. Currently only third party softphones from IP Blue will work with the Cisco CME.

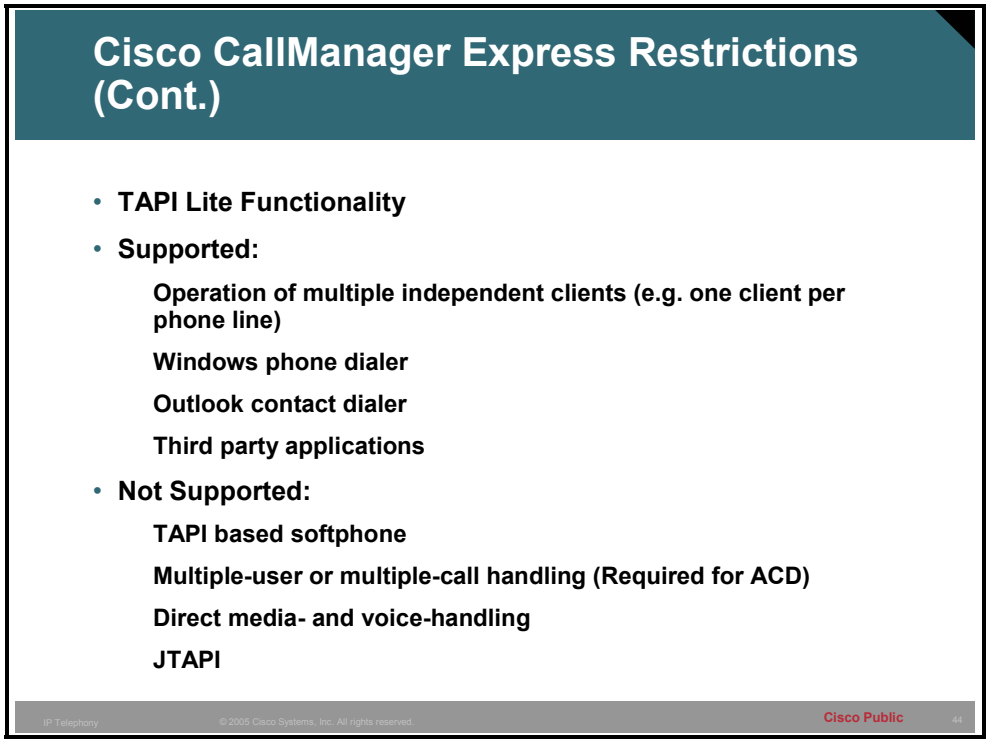
There are some restrictions when working with Cisco CME. The Cisco CME supports only phones that are local to the Cisco CME LAN and does not support remote SCCP phones that are connected across WAN links. The Cisco CME system and IP phones support the G.711 and G.729 codec. However, only the G.711 codec is supported for conferencing. This is due to a lack of support for hardware Digital Signal Processing (DSP)-based transcoding. This should be available in future versions of Cisco CME.

Media Gateway Control Protocol (MGCP) is not supported in Cisco CME.

Note	Upcoming releases of Cisco CME will support transcoding and IP communicator.

Cisco CallManager Express Restrictions: TAPI Lite Functionality

This topic describes Cisco CME restrictions.



Cisco CME does not support TAPI v2.1. Cisco CME TAPI implements only a small subset of TAPI functionality. It does support operation of multiple independent clients (for example, one client per phone line) but not full support for multiple-user or multiple-call handling, which is required for complex features such as automatic call distribution (ACD).

Applications like Windows phone dialer and the Outlook contact dialer can use TAPI Lite to dial, place on hold, transfer, and terminate a call on an associated line on an IP phone. JTAPI is not supported and neither are TAPI-based softphones. TAPI Lite allows for the control of a line on an associated PC but not for the termination of voice on the PC.

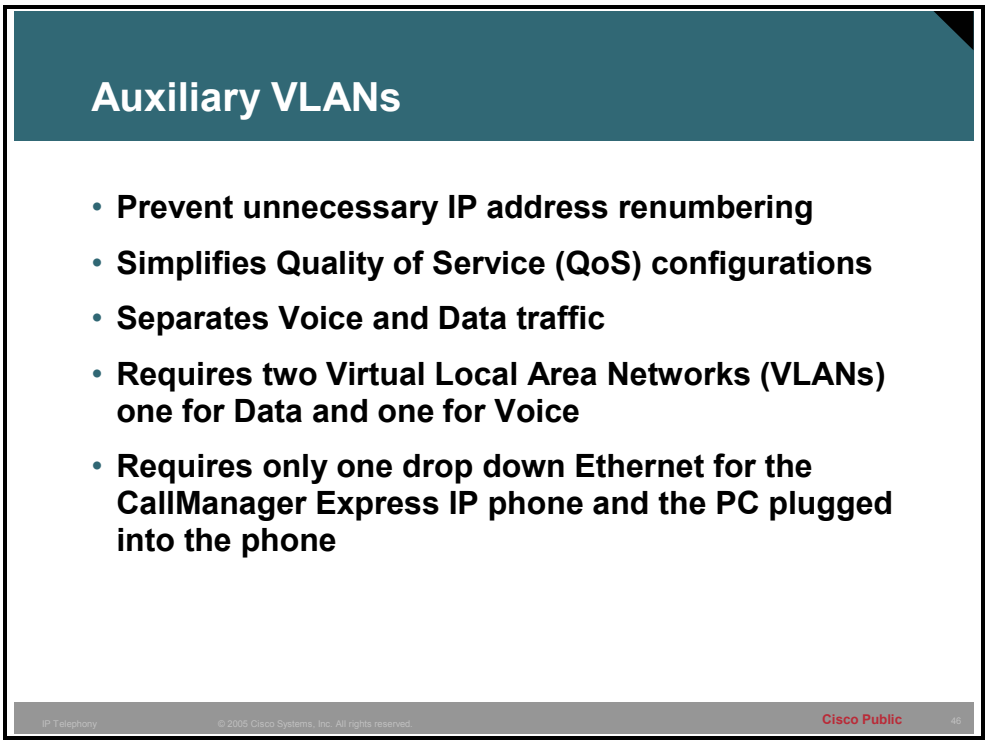
Note	Third-party applications can be developed that take advantage of TAPI Lite to control a line.

 Copyright © 2005, Cisco Systems, Inc.

Cisco CME Network Parameters

Auxiliary VLANs

This topic describes auxiliary VLANs.



Cisco IP phones can act as a three-port switch. Just like a switch they can support trunking between themselves and another switch. This allows for the existence of more than one VLAN to be supported between the IP phone and the access switch that it is plugged into.

The three ports of the IP phone are the port that connects to the 10/10 Ethernet switch, the 10/100 Ethernet port that a PC can be plugged into, and an internal port where voice traffic is originated and terminated. The 10/100 Ethernet port which attaches to a switch, supports the 802.1Q trunking protocol. This allows for the existence of two VLANs arriving at the phone, one for the voice traffic and the other for the PC data traffic. The VLAN that the voice traffic goes across is called the auxiliary VLAN or the voice VLAN.

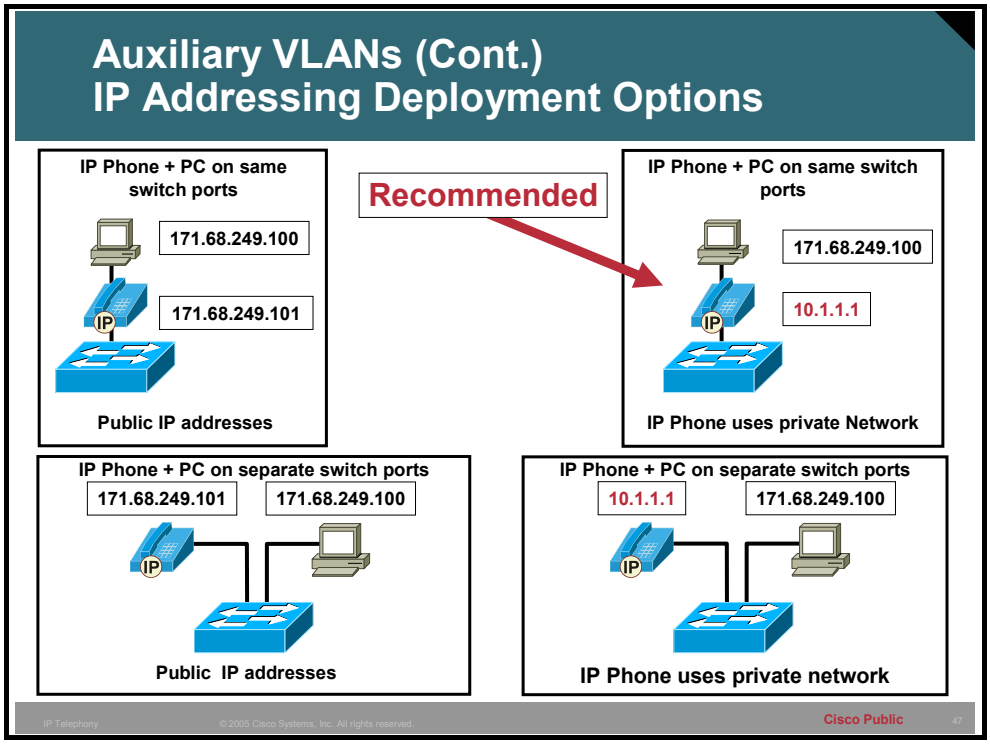
Note Inter Switch Link (ISL) trunking is not supported on the Cisco IP phone.

The benefits of this type of configuration include the following:

- This solution allows the deployment of IP phones onto the network without scalability problems from an addressing perspective. IP subnets usually have more than 50 percent (often more than 80 percent) of their IP addresses allocated. A separate VLAN (separate IP subnet) to carry the voice traffic allows an introduction of a large number of new devices,

such as IP phones, in the network without extensive modifications to the IP addressing scheme.

- This solution allows the logical separation of data and voice traffic that have different characteristics. This separation allows the network to individually handle each of these traffic types and apply differing Quality of Service (QoS) policies.
- The data and voice traffic are separated and can be monitored and managed separately.
- This solution allows you to connect two devices to the switch using only one physical port and one Ethernet cable between the wiring closet and the IP Phone and /or PC location.



Cisco IP Phones require network IP addresses. Cisco makes the following recommendations for IP addressing deployment:

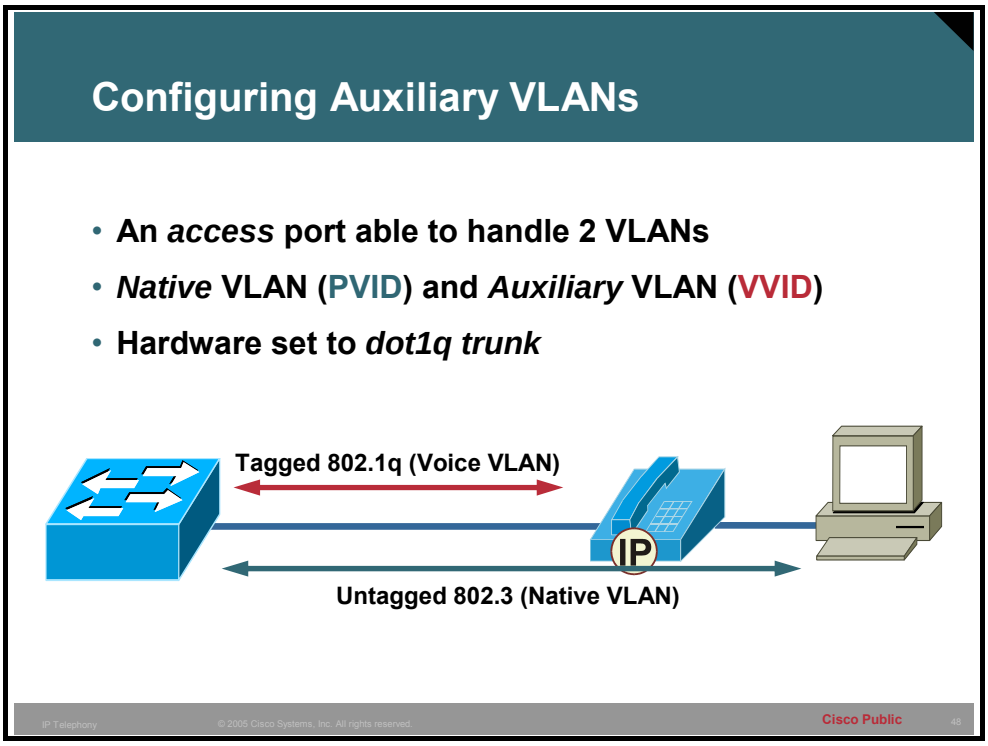
- Continue to use existing addressing for data devices (PCs, workstations, and so forth).
- Add IP Phones with Dynamic Host Configuration Protocol (DHCP) as the mechanism for obtaining addressees.
- Use subnets for IP Phones if they are available in the existing address space.
- Use private addressing (network 10 or network 172.16 – 172.20) if subnets are not available in existing address space.

LANs and private IP WANs will carry these routes between both of the address spaces. The WAN gateway to the Internet should block private addresses, which data devices currently block.

 Copyright © 2005, Cisco Systems, Inc.

Configuring Auxiliary VLANs

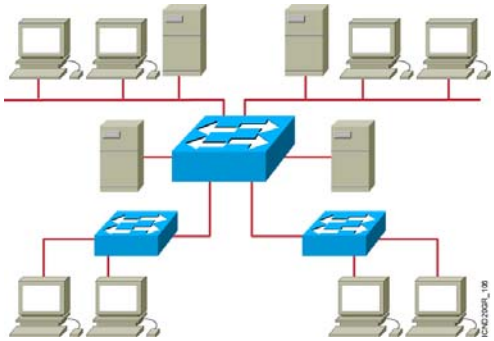
This topic describes how to configure auxiliary VLANs on the Catalyst 3550 and EtherSwitch Network Modules.



All data devices typically reside on data VLANs in the traditional switched scenario. You may need a separate voice VLAN when you combine the voice network into the data network. The Catalyst software command-line interface (CLI) refers to this new voice VLAN as the auxiliary VLAN for configuration purposes. You can use the new auxiliary VLAN to represent other types of devices. Currently, the device is an IP phone, so you can think of it as a voice VLAN. In the future, other types of non-data devices will reside in the auxiliary VLAN.

These non-data devices (such as IP phones) should reside in a separate VLAN (auxiliary VLAN), which will make it easier for customers to automate the process of deploying IP Phones. IP Phones will boot up and reside in the auxiliary VLAN if you configure the switch to support them; just as data devices come up and reside in the native VLAN (also referred to as the default VLAN) of the switch. The IP phone communicates with the switch via Cisco Discovery Protocol (CDP) when it powers up. The switch will provide the telephone with the appropriate VLAN ID, known as the Voice VLAN ID (VVID). This VVID is analogous to the data VLAN ID, known as Port VLAN ID (PVID).

Configuring Auxiliary VLANs - Switching Review



- **Address learning**
- **Forward/filter decision**
- **Loop avoidance**

IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 49

A layer 2 switch provides layer 2 services and intelligence. Address learning is performed by the Ethernet switch and allows the switch to listen on ports for source MAC addresses and build a table that will be stored in RAM. These addresses that have been learned will be used to forward unicast frames to the appropriate port based on the destination MAC address. This allows the switch to make more efficient use of bandwidth by only forwarding frames out the port where the destination MAC address resides. Broadcasts are sent out all ports in the same VLAN except the port on which it was received.

Note	Unknown MAC addresses will be treated like broadcasts and forwarded to all ports in the same VLAN.

In the layer 2 Ethernet header there is no loop avoidance mechanism and, as a result, the switch will have to perform this function. The protocol that is used for loop avoidance is called Spanning Tree Protocol (STP). This protocol only runs on layer 2 switches and, in most deployments, should be considered mandatory. The Spanning Tree Protocol can take a significant amount of time to converge or re-converge when there is a topology change. This re-convergence time can be minimized on ports where IP phones, PCs, or servers reside through the use of portfast. Portfast can take a convergence time of 30 seconds and reduce it down to 1-2 seconds.

Caution	Using portfast on interfaces that connect to other switches can result in temporary layer 2 loops.

 Copyright © 2005, Cisco Systems, Inc.

Configuring Auxiliary VLANs (Cont.)

Example 3550 switch or EtherSwitch Network Module

```
Console(config)#interface FastEthernet0/1
Console(config-if)#switchport trunk encapsulation dot1q
Console(config-if)#switchport trunk native vlan 1
Console)config-if)#switchport access vlan 12
Console(config-if)#switchport mode trunk
Console(config-if)#switchport voice vlan 112
Console(config-if)#spanning-tree portfast
```

- **802.1q trunking is enabled on the port**
- **The access VLAN is used for the PC plugged into the IP phone**
- **The voice VLAN is used for voice and signaling that originates and terminates on the IP phone**
- **Spanning tree portfast enables the port to initialize quickly**

© 2005 Cisco Systems, Inc. All rights reserved.

To configure the trunk on a physical interface between the access switch port and the IP phone, an 802.1Q trunk needs to be created. In addition the native or untagged VLAN will need to be defined as well as the auxiliary or voice VLAN.

The example above shows the configuration of a 3550 or an EtherSwitch network module.

Configuring Auxiliary VLANs (Cont.)

```
Switch# show interface fa0/17 switchport

Name: Fa0/17
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q

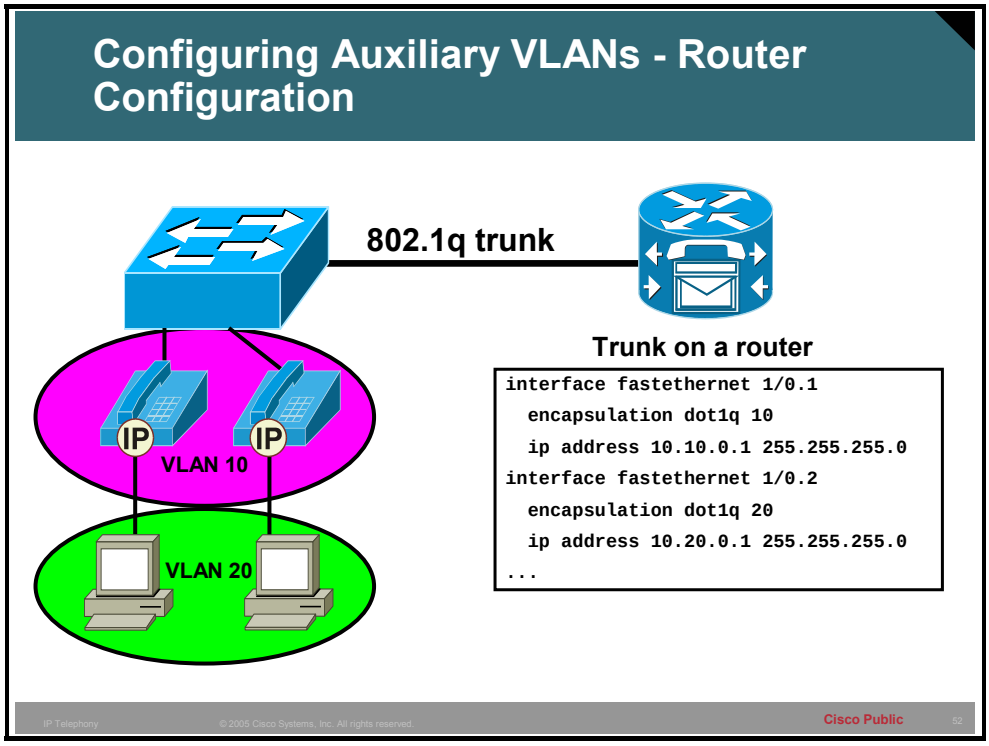
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 12 (VLAN0012)
Trunking VLANs Enabled: ALL
Trunking VLANs Active: 1-3,5,10,12
Pruning VLANs Enabled: 2-1001

Priority for untagged frames: 0
Override vlan tag priority: FALSE
Voice VLAN: 112
Appliance trust: none
```


© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc.

You can verify your voice VLAN configuration on the Catalyst switch by using the **show interface <mod/port> switchport** command.



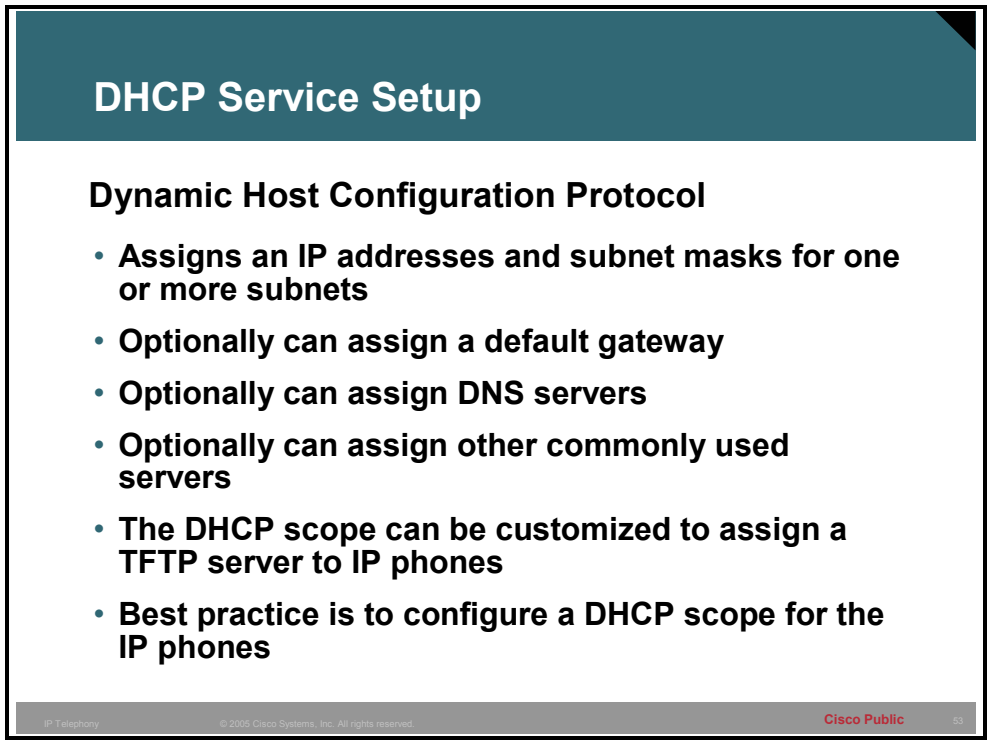
Routing between the different VLANs requires a layer 3 router. The router will need to have an interface local to all of the VLANs to which it will route. The most efficient way to get multiple VLANs to the router is by connecting a trunk between the switch and the router. This configuration is known as “router on a stick”.

The router will have one sub-interface local to each VLAN and only one VLAN can be assigned to that sub-interface.

 Copyright © 2005, Cisco Systems, Inc.

DHCP Service Setup

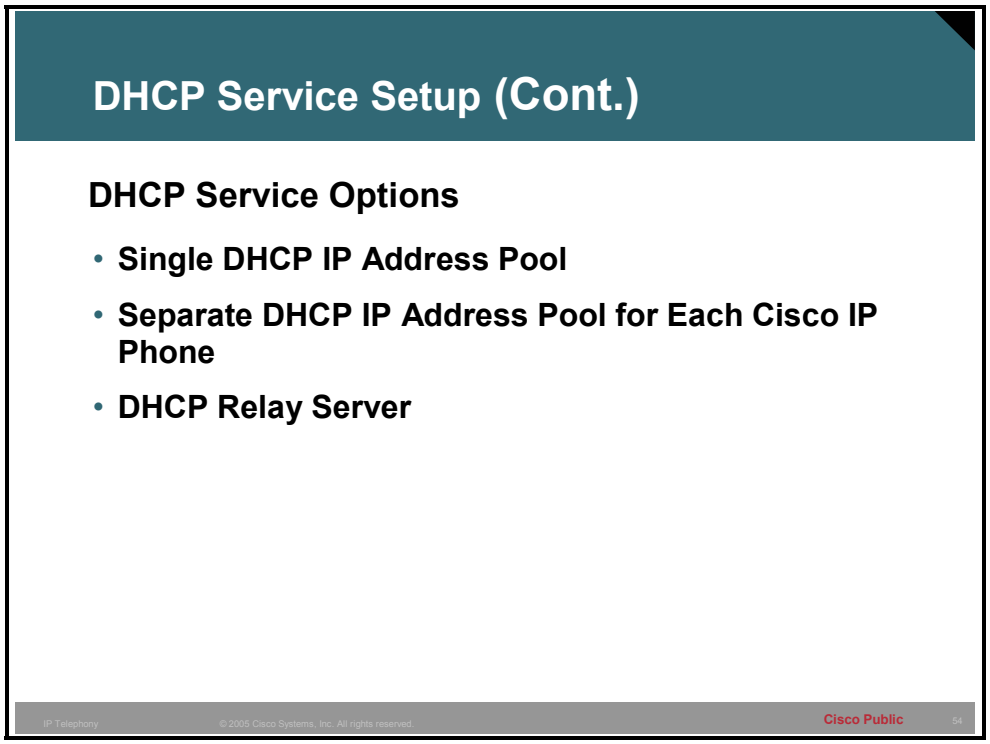
This topic identifies the DHCP service options.



DHCP is a very common and familiar protocol to many network administrators. A scope will be defined per subnet and is used to hand out IP addresses from a pool of available addresses, along with a subnet mask. Optionally, other values like the default gateway and DNS can be assigned to the scope by setting option values if desired. For example, the default gateway option is “003” and DNS is “006.”

These option values can include values specific to an implementation and can be customized by the administrator. Cisco phones look for an option 150 from their DHCP server, which will contain the IP address of the TFTP server where the IP phones configuration file will reside. The administrator will need to configure an option 150 with the IP address of the TFTP server, which is the Cisco CME router in the case of Cisco CME.

DHCP can be deployed on any platform that supports customized scope options. This includes Windows, Linux, Novell, UNIX and others operating systems.



You can set up DHCP service for IP Phones by defining a single DHCP IP address pool, defining a separate pool for each Cisco IP Phone, or defining a DHCP relay server.

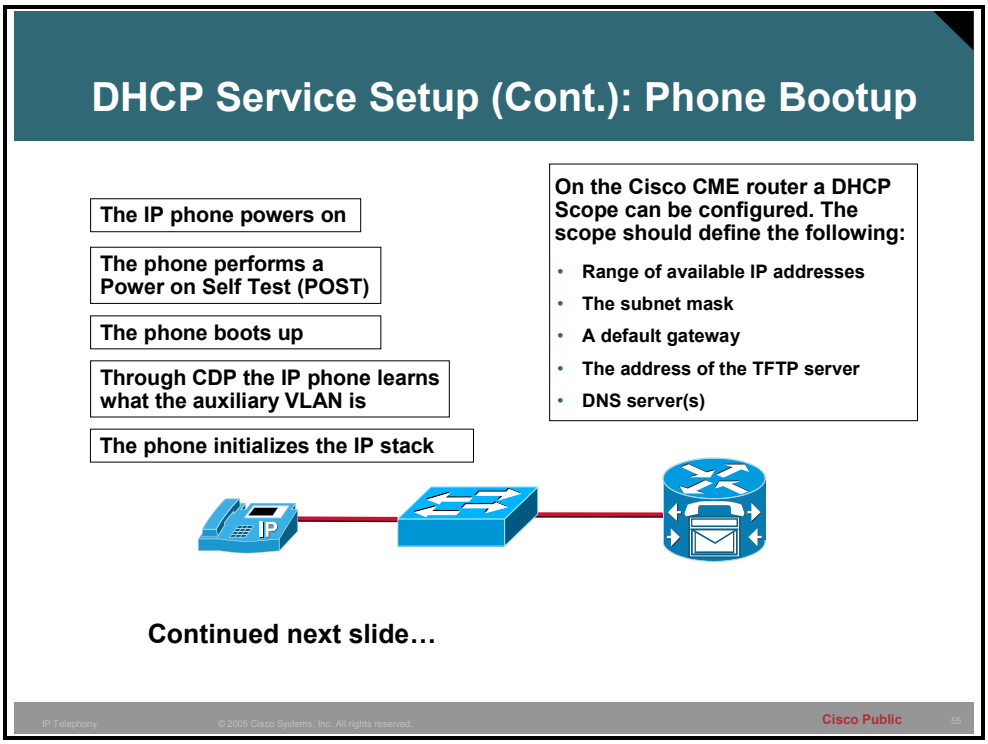
Single DHCP IP Address Pool: Define a single DHCP IP address pool if the Cisco CME router is a DHCP server and if you can use a single shared address pool for all your DHCP clients.

Separate DHCP IP Address Pool for Each Cisco IP Phone: Define a separate pool for each Cisco IP Phone if the Cisco CME router is a DHCP server and you need different settings on non-IP phones on the same subnet.

Note	This option should be avoided if possible because it adds configuration complexity.

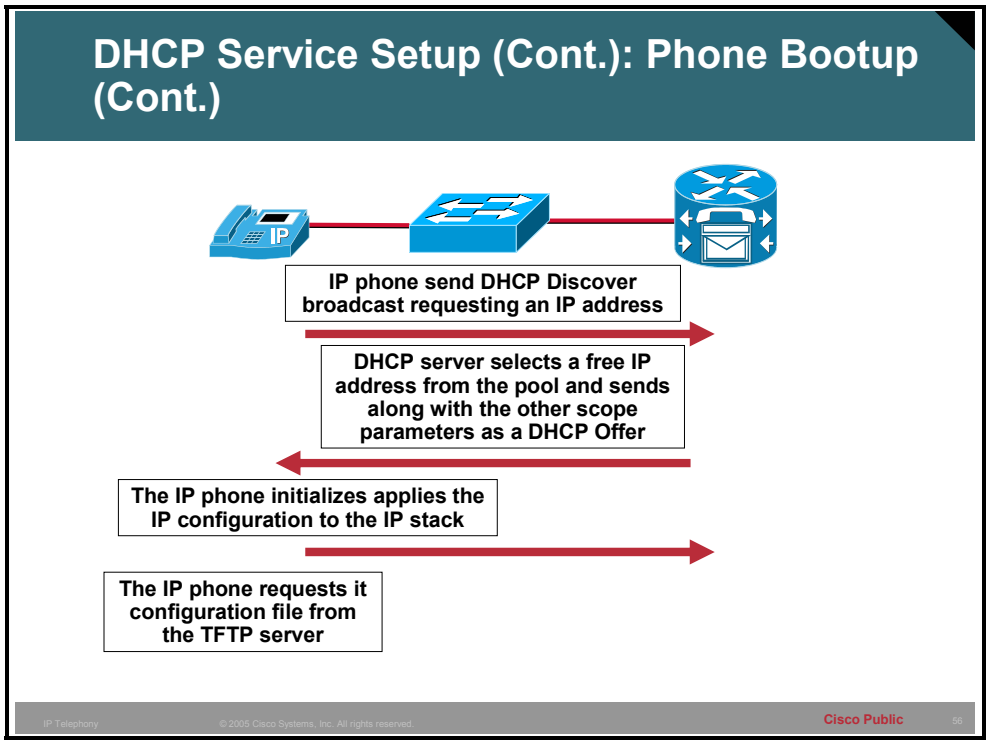
DHCP Relay Server: DHCP Relay Server: Define a DHCP relay server if the Cisco CME router is not a DHCP server and you want to relay DHCP requests from IP Phones to a DHCP server on a different subnet.

 Copyright © 2005, Cisco Systems, Inc.



When an IP phone first receives power, the following steps happen:

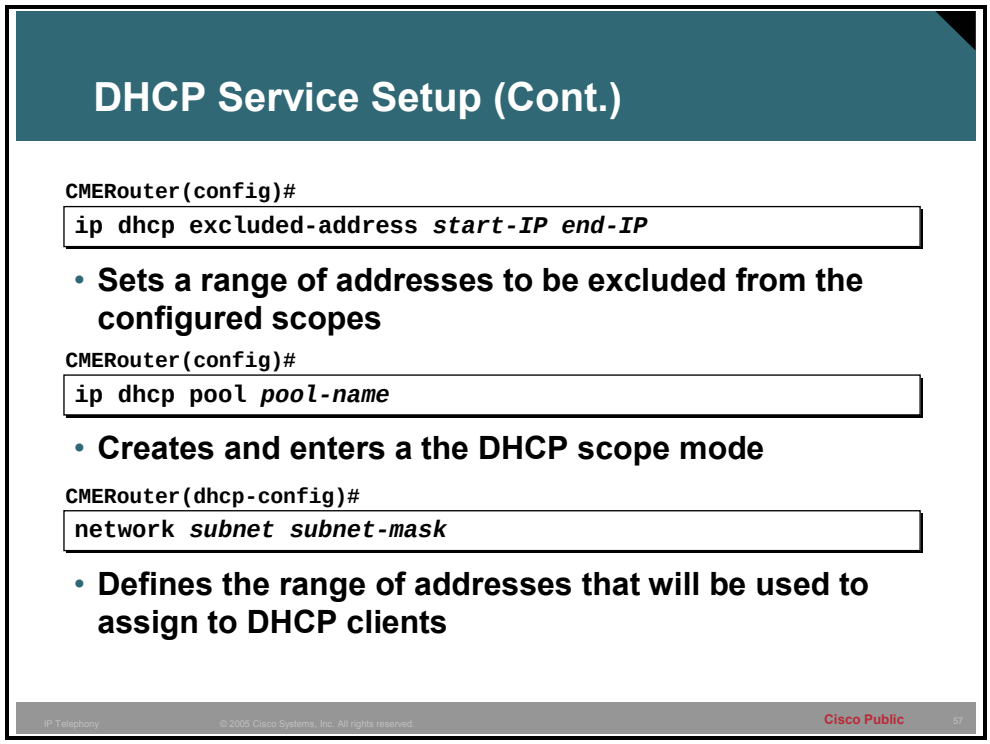
- **Receives power** - The IP phone receives power
- **POST** - The phone will perform some basic tests called a Power On Self Test (POST).
- **Boot** - The IP phone will then bootstrap
- **Discover the Voice VLAN** - Learn which VLAN is the voice VLAN through the layer 2 Cisco Discovery Protocol (CDP).
- **Initialize the IP stack** - The IP phone will then initialize a basic IP stack.



The process of a phone booting up continues with the following:

- **Send DHCP Discover –** By default, the IP phone (DHCP client) will then send a DHCP request to the 255.255.255.255 broadcast address
- **DHCP server assigns an IP address –** If this broadcast is heard by a local DHCP server, the server will assign a free IP address, the subnet mask for the scope, the default gateway for the scope, the DNS server (optional) for the scope, and a TFTP server (option 150) for the scope
- **DHCP Offer –**The Scope setting will be sent to the DHCP client (the IP phone) using the broadcast address of 255.255.255.255
- **IP phone initialized DHCP settings –** The IP phone will take the values received from the DHCP response and apply them to the IP stack of the IP phone
- **Request configuration from TFTP server –** The IP phone will use the value received in option 150 to attempt to get a configuration file from the TFTP server (Cisco CME router is always the TFTP server in Cisco CME)

 Copyright © 2005, Cisco Systems, Inc.



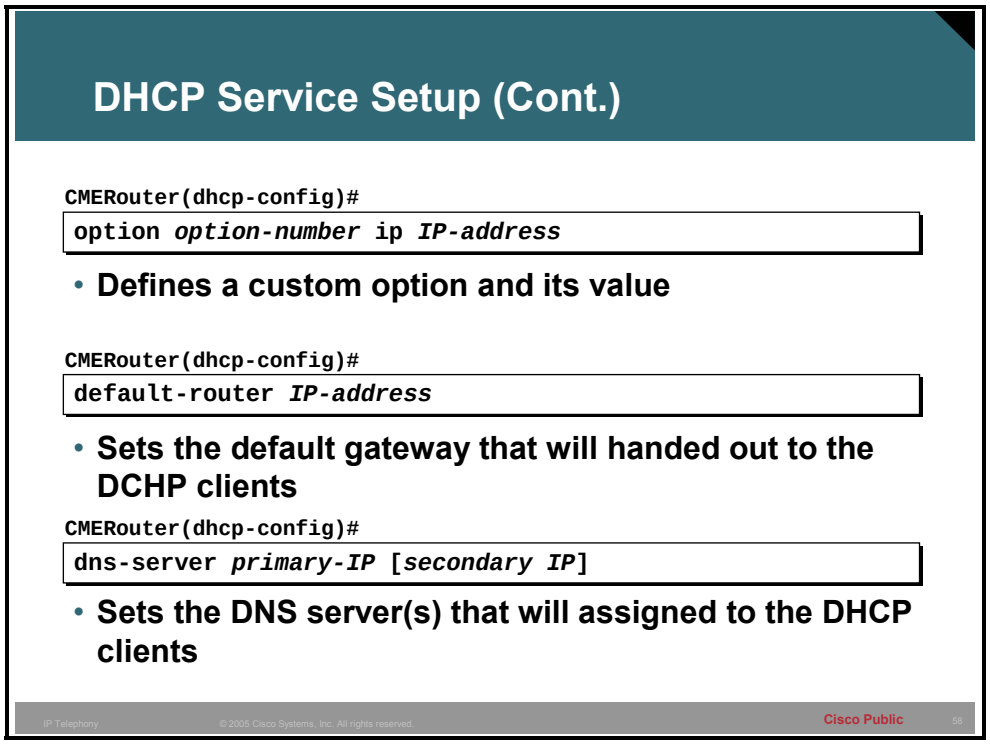
These commands are not needed for the IP phones if the automated setup is used because the setup will prompt for these setting and configure a DHCP scope automatically. However, if it is not configured or the administrator wishes to manually configure or change the settings the following commands will need to be used.

The command **ip dhcp exclude-address *start-IP end-IP*** allows the administrator to exclude static addresses within the scope range that might be statically assigned to a server or router interface. For Cisco CME the exclusions should include the IP address of the routers interface that may be local to the IP phones.

The command **ip dhcp pool *pool-name*** defines and creates a DHCP pool. After this command has been executed, the router will be in a DHCP sub mode. The automated setup mode will create a DHCP pool named ITS (the old name of the Cisco CME product).

Note The pool name is case-sensitive.

Within the DHCP sub mode under a pool, enter the **network *subnet subnet-mask*** command to assign a range of IP addresses to be available for DHCP clients to be assigned. This will not include any exclusion previously defined. The lowest available IP address will be used first when the addresses are assigned. In Cisco CME, this will be the subnet on which the IP phones are.



The command **default-router *IP-address*** will set option 003 on the DHCP scope that is being defined. This option will send the IP address of the default gateway to the DHCP client. The default gateway for Cisco CME will be the router interface that is on the same subnet as the IP phones.

The optional command **dns-server *primary-IP secondary-IP*** allows the DNS server to be sent in option 006 to the DHCP clients. For Cisco CME, this setting becomes important if names will be used for any of the URL values that can be assigned. Lack of a DNS server has the effect of requiring use of IP addresses only.

Finally, a critical command that must be configured correctly is the custom option for the TFTP server. This is configured using the command **option 150 ip *CallManagerExpress-IP***. This IP address must be the IP address on the Cisco CME router with which the IP phones register.

 Copyright © 2005, Cisco Systems, Inc.

DHCP Service Setup (Cont.)

Configuring DHCP on an IOS router

```
CMERouter(config)#ip dhcp exluded-address 10.90.0.1 10.90.0.10
CMERouter(config)#ip dhcp pool mypool
CMERouter(dhcp-config)#network 10.90.0.0 255.255.255.0
CMERouter(dhcp-config)#option 150 ip 10.90.0.1
CMERouter(dhcp-config)#default-router 10.90.0.1
CMERouter(dhcp-config)#dns-server 10.100.0.1 10.100.0.2
CMERouter(dhcp-config)#exit
```

- **Option 150 sets the TFTP server on the IP phone**
- **The TFTP server contains the configuration files and firmware for the IP phone**

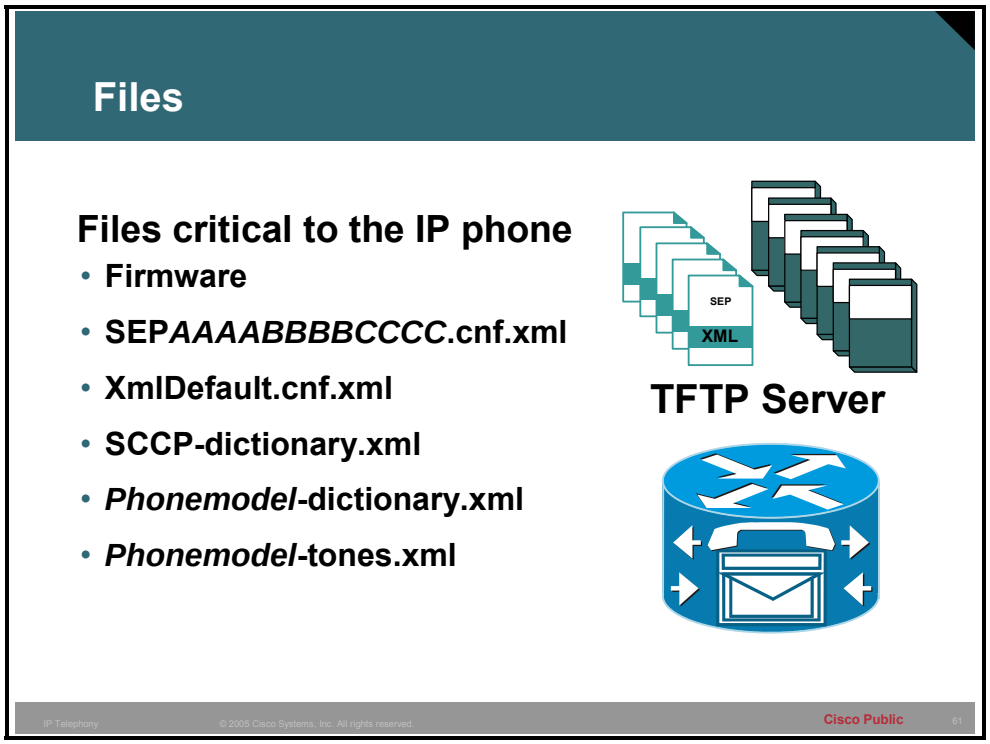
IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 59

This is a sample configuration in which the DHCP server is the Cisco CME router. This shows the command **option 150 ip 10.90.0.1**, where 10.90.0.1 is the IP address of a local interface on the Cisco CME router.

IP Phone Registration

Files

This topic describes IP phone firmware files and XML configuration files.



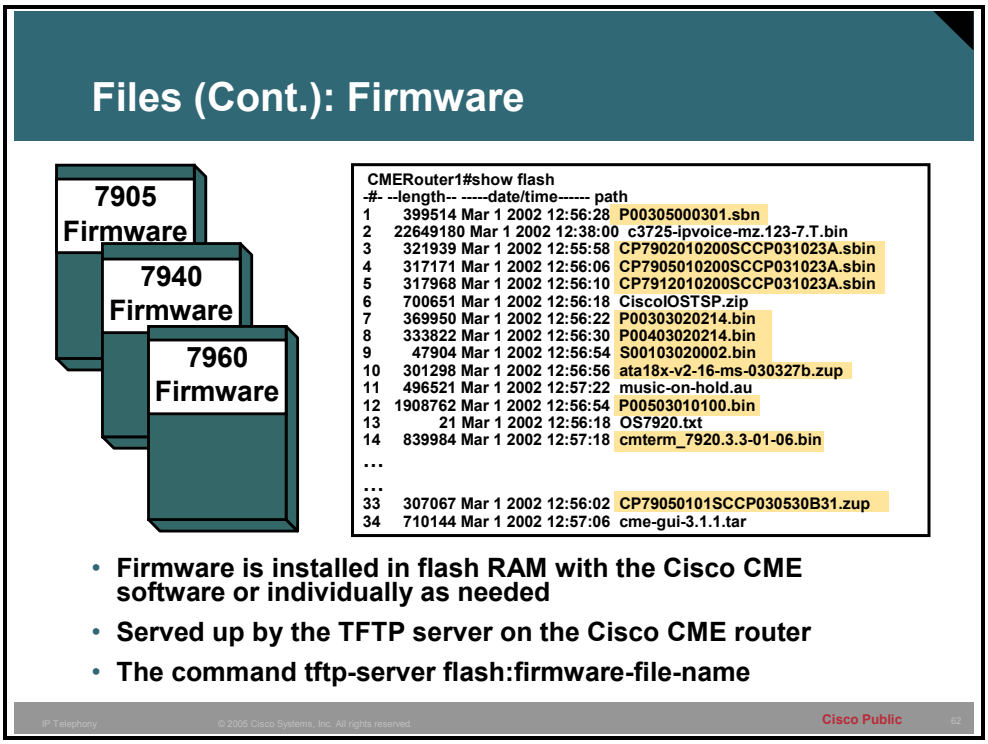
There are some files that are necessary for the proper operation of the IP phone or analog device so that it may register successfully with the Cisco CME router. The files that will be needed include:

- **Firmware –** The firmware is loaded into memory on the IP phone and will survive a reboot
- **XMLDefault.cnf.xml –** An XML configuration file that will specify the proper firmware, address, and port needed for the new phone to register
- **SEP*AAAABBBBCCCC*.cnf.xml –** An XML configuration file that is specific for one device based on the MAC address
- **SCCP-dictionary.xml –** An XML file that contains the device labels for the locale selected
- ***Phonemodel*-dictionary.xml –** An XML file that contains possible messages and dialogs that can appear on the screen of the IP phone for the selected locale
- ***Phonemodel*-tones.xml –** An XML file that contains the cadence and rings for the specified locale

All of the necessary firmware files for IP phones are stored internally on the Cisco CME router flash, so an external database or file server is not required. IP Phones will download firmware files from the router flash using Trivial File Transfer Protocol (TFTP) during registration. All

 Copyright © 2005, Cisco Systems, Inc.

Cisco CME configuration and language files are located in the Dynamic RAM (DRAM) of the router under system:/its/.



The firmware of the supported devices within Cisco CME is stored in the flash memory of the Cisco CME router. These firmware files are installed in flash memory when the Cisco CME software is extracted and installed. The firmware required will vary with the devices, and needs to be available when a new phone or a phone with a different version of firmware comes online. The firmware files need to be made available through a TFTP server. This is done with the command **tftp-server flash:*firmware-file-name***.

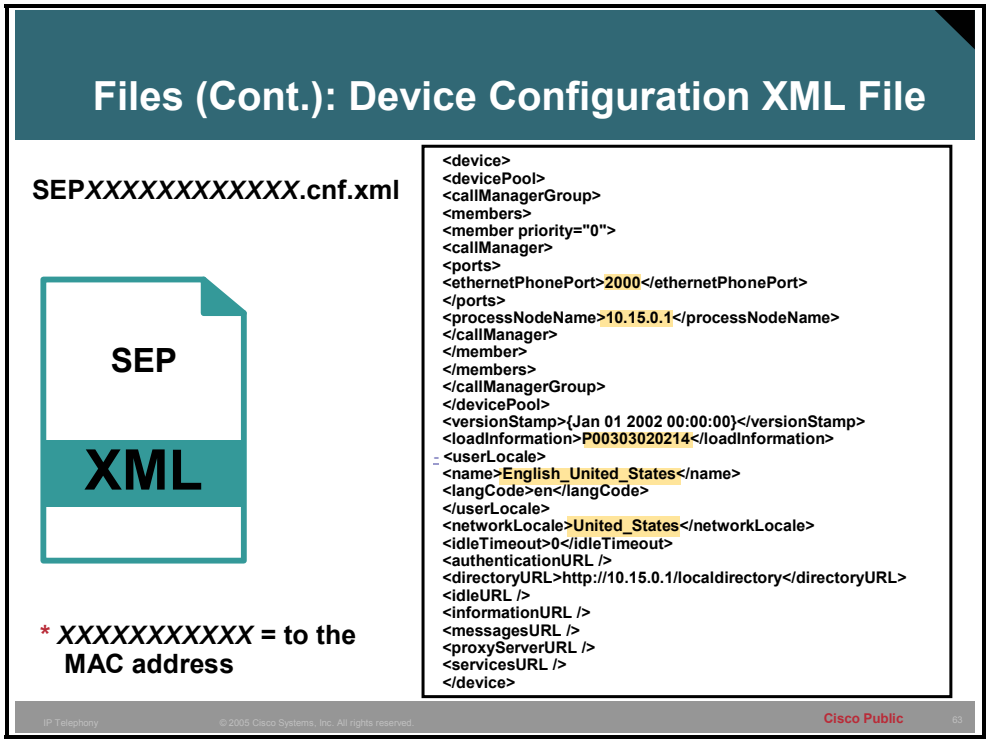
This command as well as other related commands will be covered in more detail in the next lesson.

The firmware names with .sbin are signed phone loads. Once a signed phone load is installed on a phone, that phone cannot go back to an unsigned phone load. The phone will always have to use a signed phone load even if used by CallManager.

Note These files are specific to Cisco CME 3.1 and will vary with the version of Cisco CME.

Model	Firmware file
ATA-186	ata18x-v2-16-ms-030327b.zup
ATA-188	ata18x-v2-16-ms-030327b.zup
7902	CP7902010200SCCP031023A.sbin

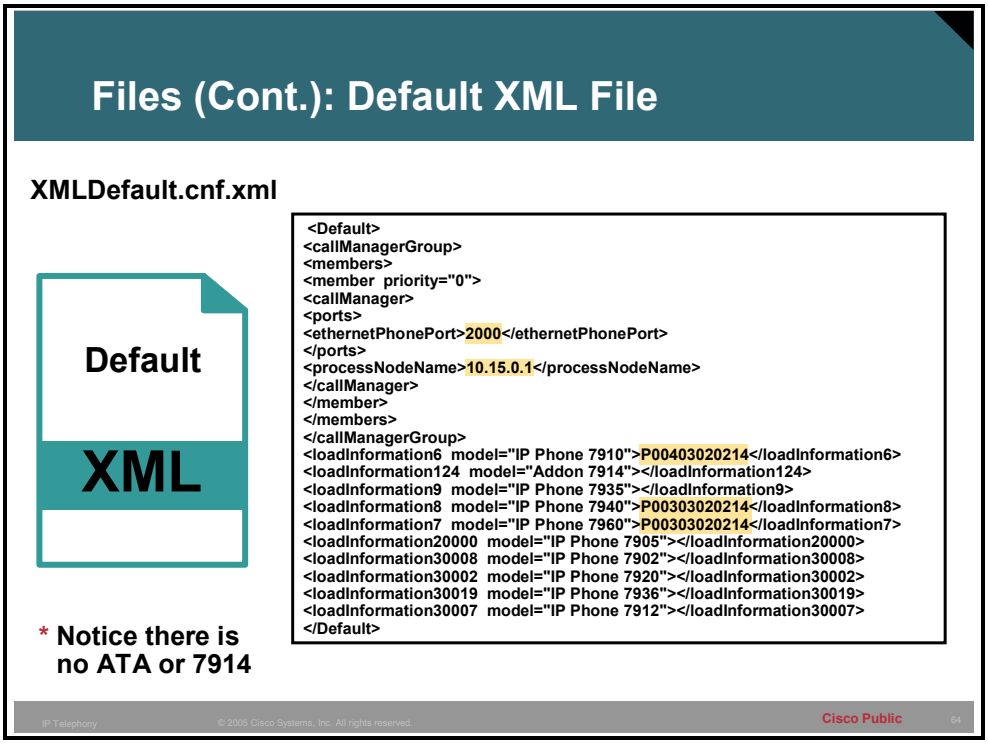
7905G	CP7905010200SCCP031023A.sbin
7910	P00403020214.bin
7912G	CP7912010200SCCP031023A.sbin
7914	S00103020002.bin
7920	cmterm_7920.3.3-01-07.bin
7935	P00503010100.bin
7936	P00503010100.bin
7940G	P00303020214.bin
7940G	P00305000301.sbn
7960G	P00303020214.bin
7960G	P00305000301.sbn



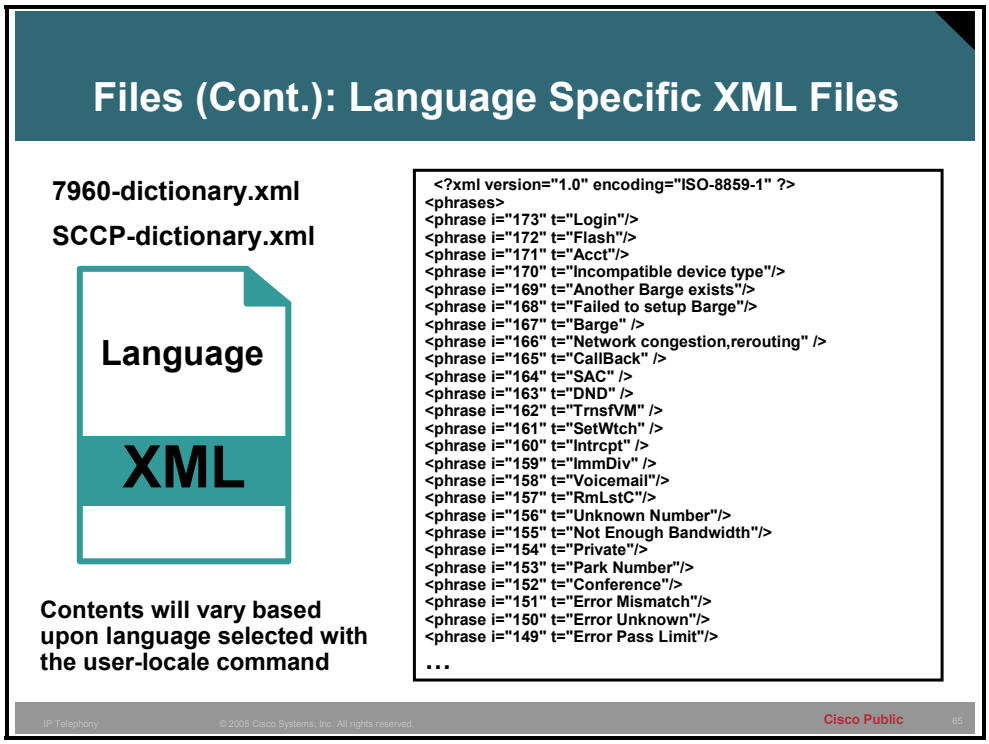
The XML file SEP*AAAABBBBCCCC.cnf.xml* (where *AAAABBBBCCCC* is the MAC address of the IP phone) contains the IP address, port, firmware, locale, directory URL and many others, some of which cannot be currently used in Cisco CME. This file is generated by the system during the initialization of the Cisco CME software when the command **create-cnf-files** is found in the startup-config. This command and other related commands will be covered in more detail in the next lesson.

 Copyright © 2005, Cisco Systems, Inc.

In the graphic, the configuration file contains the IP address and port representing the interface and port to which the phone will attempt to register on the Cisco CME router. Within the configuration file there is also a language defined that will be applied to the IP phone in question.



The file XMLDefault.cnf.xml is used by IP phones and devices that did not find a more specific SEP*AAAABBBBCCCC*.cnf.xml file. The IP phones that download this XML file through TFTP will now know the IP address and port of the Cisco CME router, as well as the required version of firmware that it will need to have to function with the Cisco CME properly. The file is generated by the Cisco CME system when the command **create-cnf** is entered in telephony service mode. This and other related commands will be covered in more detail in the next lesson.



The files SCCP-dictionary.xml and *phonemodel*-dictionary.xml configure the language for the IP phones in the system. These contain the labels for buttons as well as messages that could be displayed on the screen of the IP phones. This is set with the **user-locale *locale*** command and this will be covered along with related commands in more detail in the next lesson.

Note	A language is installed on the IP phone by these two files.

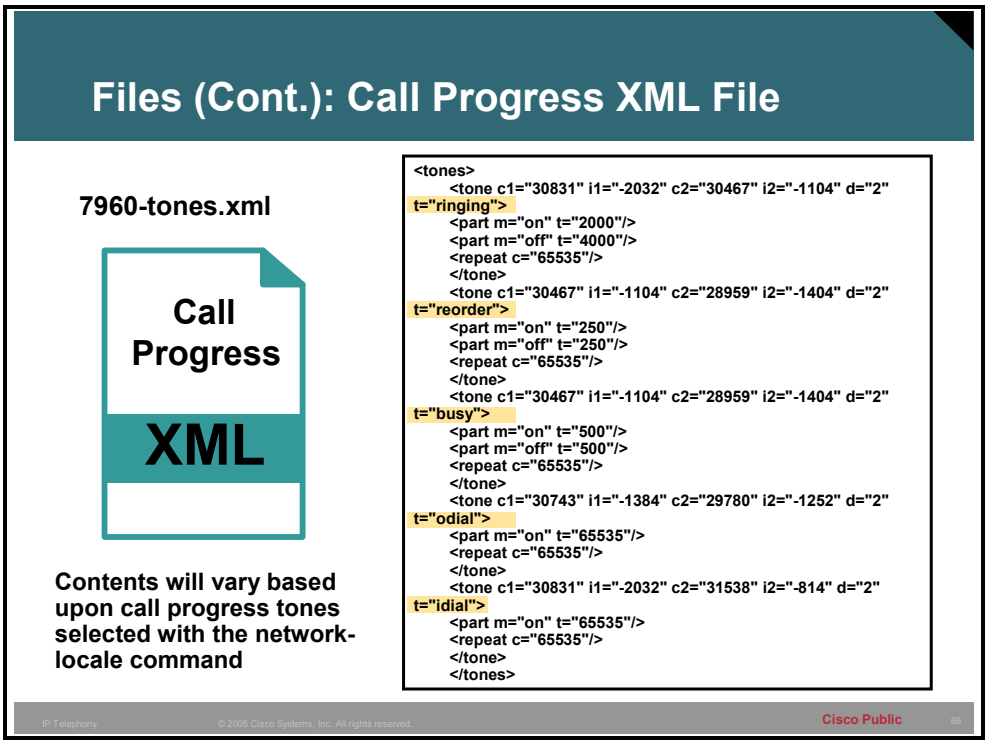
The following languages are supported on the IP phones:

CMERouter1(config-telephony)#user-locale ?

DE	*Germany*
DK	*Denmark*
ES	*Spain*
FR	*France*
IT	*Italy*
NL	*Netherlands*
NO	*Norway*
PT	*Portugal*
RU	*Russian Federation*

 Copyright © 2005, Cisco Systems, Inc.

SE	*Sweden*
US	*United States*



The file named *phonemodel*-tones.xml contains the cadence, rings, and progress tones that the phones in the Cisco CME system will use. This command sets the country-specific tones that the users of that country are familiar with. This is set with the command **network-locale *locale***. This and other related commands will be covered in detail in the next module.

This is a system-wide setting that will apply to all IP phones in the system. The call progress tones file is loaded into RAM at start up and will be how the call progress tones are defined.

CMERouter1(config-telephony)#**network-locale ?**

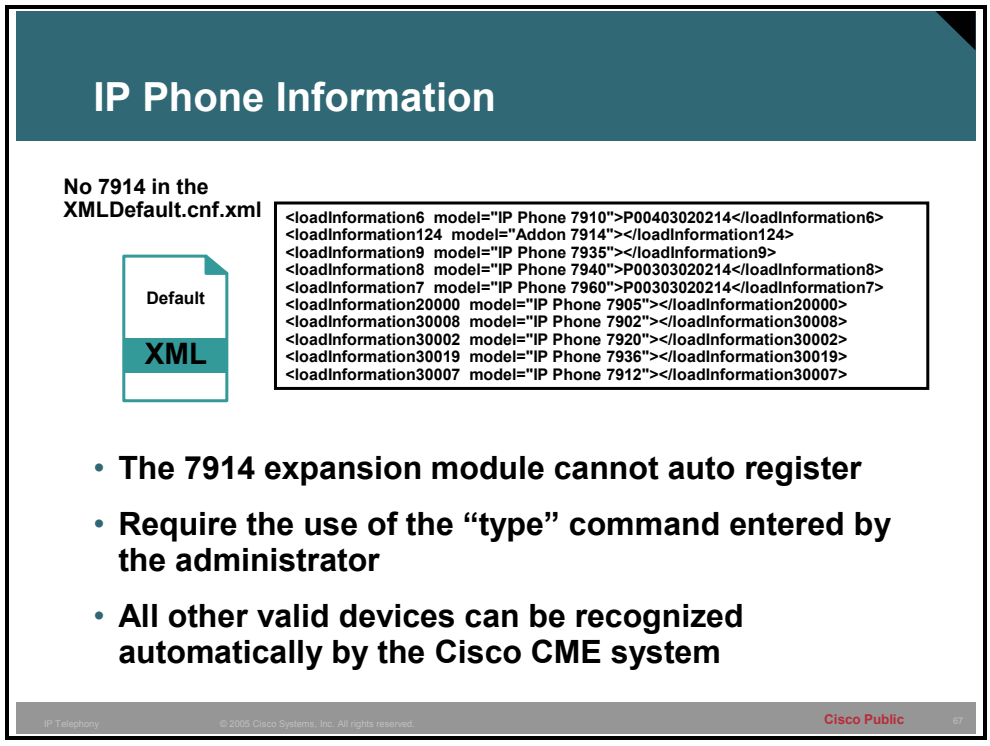
AT	Austria
CA	Canada
CH	Switzerland
DE	Germany
DK	Denmark
ES	Spain
FR	France
GB	United Kingdom

IT	Italy
NL	Netherlands
NO	Norway
PT	Portugal
RU	Russian Federation
SE	Sweden
US	United States

 Copyright © 2005, Cisco Systems, Inc.

IP Phone Information

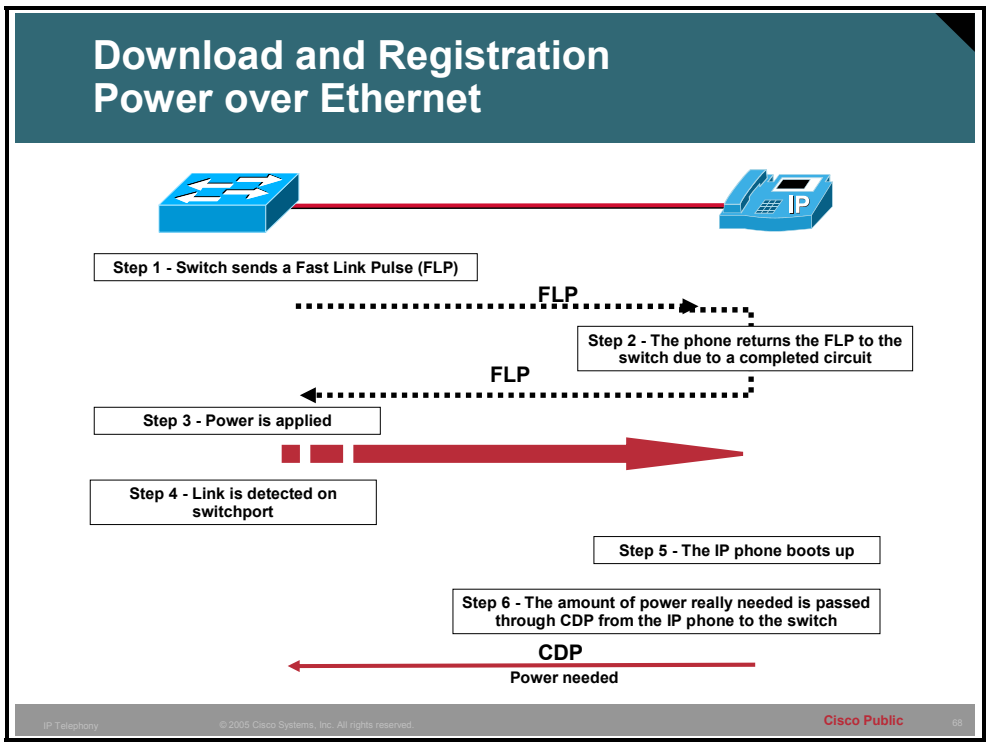
This topic describes the process of Cisco CME identifying IP phones.



The 7914 module cannot auto register and the use of the **type** command under the ephone is required. This command will be covered in the next lesson in more detail. None of the other valid IP phones and ATA devices in Cisco CME require the type command, and can be determined automatically by the system.

Download and Registration

This topic describes the mechanism of an IP phone obtaining its XML configuration file and IP address.



Step 1 – The switch sends a special tone called a Fast Link Pulse (FLP) out the interface. This FLP will go to the Powered Device (PD) which is an IP phone in this case.

Step 2 – The PD has a physical link when there is no power between the pin on which the FLP arrives and a pin that goes back to the switch. This creates a circuit and the end result is that the FLP arrives back at the switch. This will never happen when the device attached is not a PD, like a PC. As a result, if the FLP does not make it back to the switch, no power will be applied.

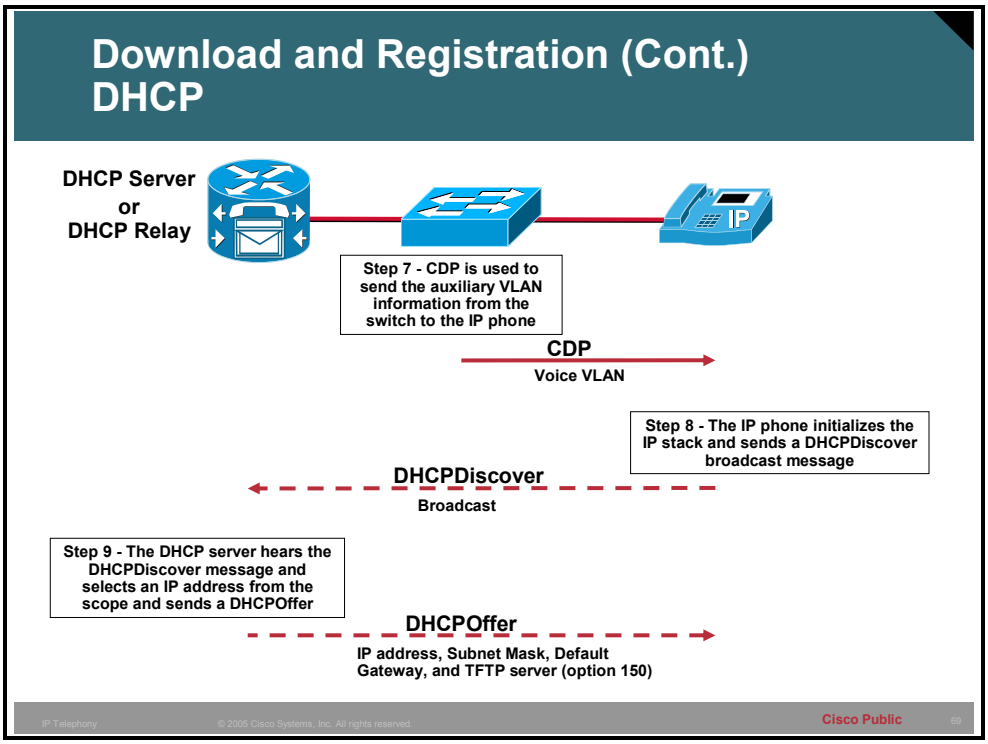
Step 3 – The switch applies power to the line.

Step 4 – Within five seconds the link should go up.

Step 5 – The PD (IP phone) boots up.

Step 6 – Through the Cisco Discovery Protocol (CDP), the IP phone tells the switch specifically how much power it needs.

 Copyright © 2005, Cisco Systems, Inc.

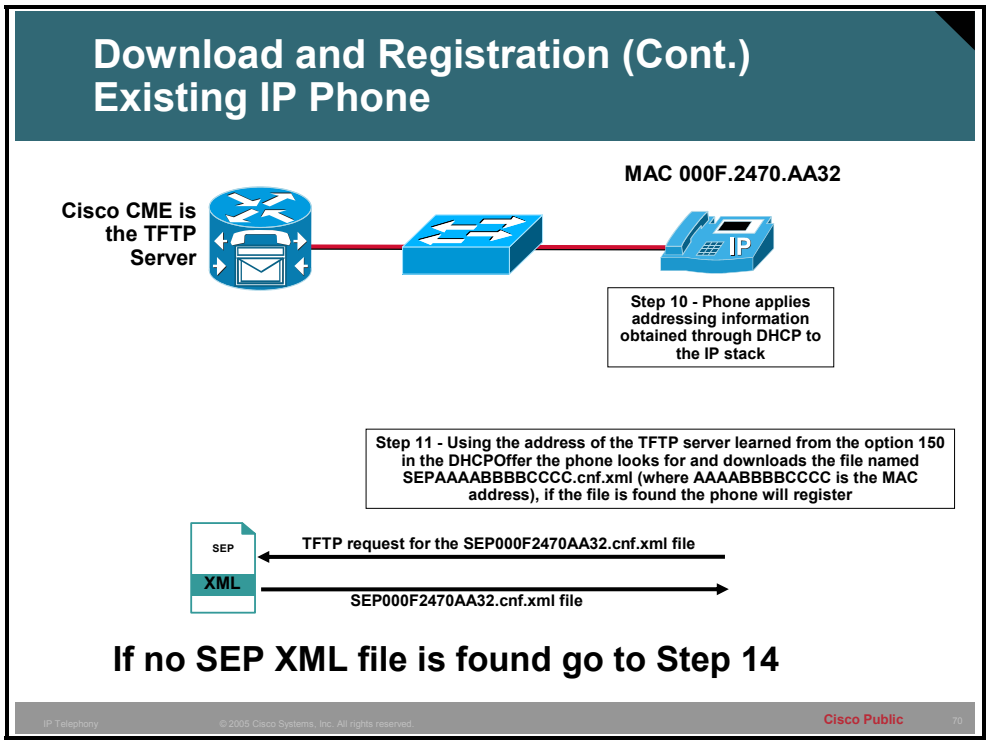


Step 7 – Through CDP, the switch informs the IP phone of its Voice VLAN (auxiliary VLAN).

Step 8 – The IP phone initializes the IP stack and sends out a DHCPDiscover broadcast looking for an IP address on the voice VLANs scope.

Note	It is possible to hard code the IP address, Subnet Mask, Default Gateway, DNS, and TFTP server on the IP phone and skip the DHCP steps. It is advised that DHCP be used to minimize administrative load required to hard code these settings.

Step 9 – The DHCP server hears the broadcast (or it was relayed to it) and assigns an IP address from the scope for the voice VLAN subnet, a subnet mask, default gateway, DNS (optional), and the address of the TFTP server (the CallManager Express router). All settings are then sent back to the IP phone in the form of a DHCPOffer message.



Step 10 – The phone receives the DHCPOffer and applies the values contained.

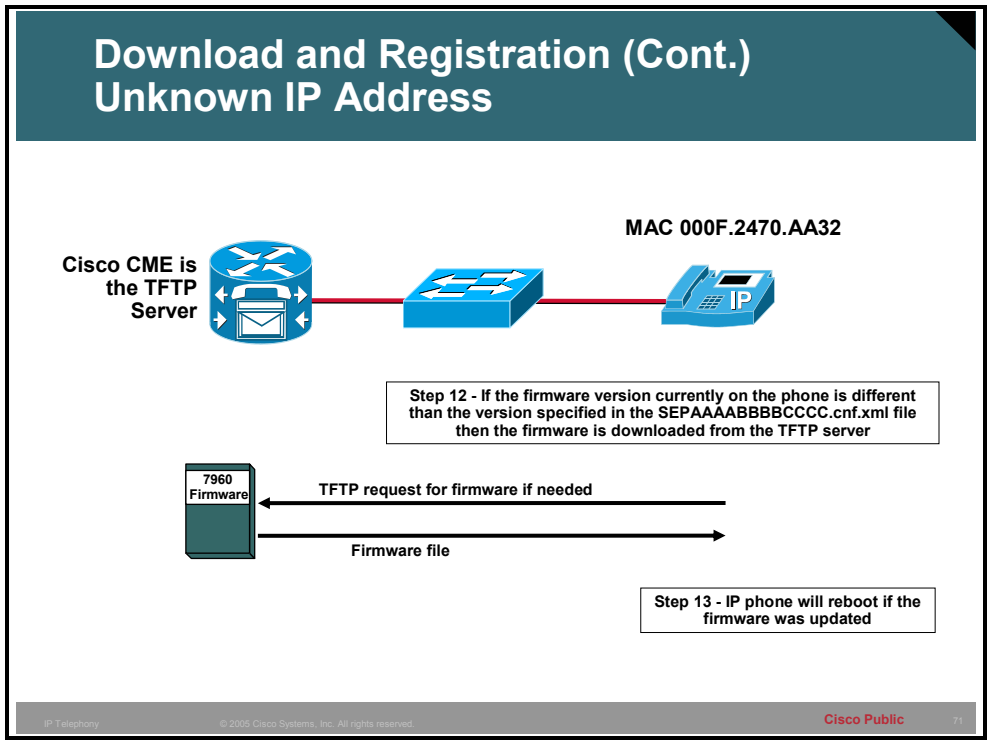
Step 11 – One of the values carried in the DHCPOffer message is the address of the TFTP server. The phone uses this information to make a connection to the TFTP server and attempt to download a file by the name of SEP000F2470AA32.cnf.xml. This file, if found, contains the information needed to register with the Cisco CME, including the IP address, port, locale, and the firmware file that should be loaded on the IP phone.

If the phone has the correct firmware, the IP phone will register and get its configuration. If the firmware is not correct, then proceed to the next step.

Note	The extension numbers, speed dials and other settings are assigned when the phone registers. They are not contained in the SEP XML file.

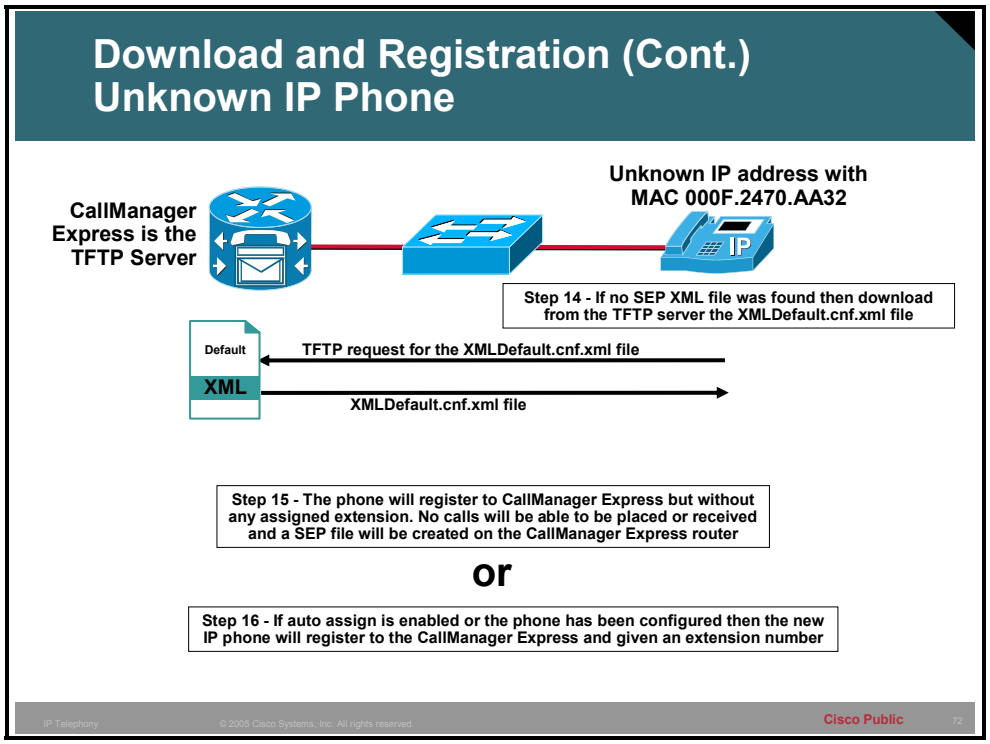
.

 Copyright © 2005, Cisco Systems, Inc.



Step 12 – If the firmware is out-of-date or different than the one specified, the IP phone will go back to the TFTP server and download the appropriate firmware.

Step 13 – The IP phone will reboot after the firmware is downloaded.



Step 14 – If no SEP XML file exists for the specific device, this indicates this device is new. The new IP phone will then proceed to get a file from the TFTP server called XMLDefault.cnf.xml. The XMLDefault.cnf.xml file specifies the IP address, port, and firmware file needed by the new IP phone. If needed, the new IP phone will download the correct firmware and reboot. If the firmware is correct, the new phone now has the information it needs to register with the Cisco CME.

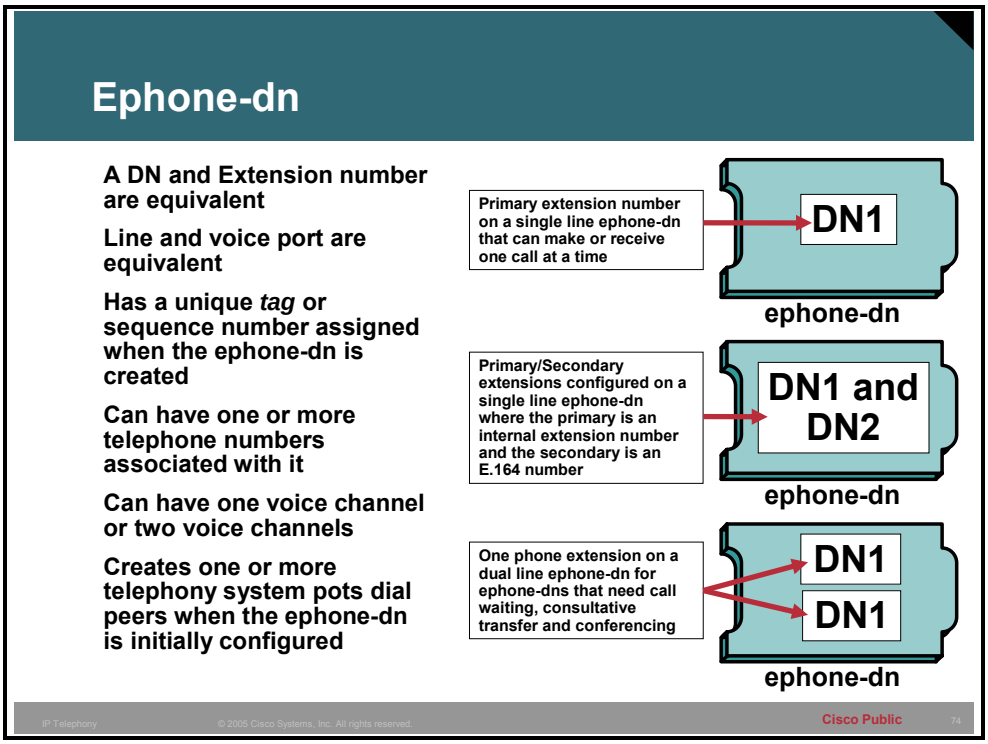
Step 15 – The phone will register with the Cisco CME system using SCCP messages and, if "auto assign" is set up, the IP phone will be assigned an extension automatically by the Cisco CME system. If "auto assign" is not configured, the phone will have no extension and will not be able to place or receive any calls. The "auto assign" function will be covered in more detail in the next lesson.

 Copyright © 2005, Cisco Systems, Inc.

Ephone-dn and Ephone

Ephone-dn

This topic defines ephone-dn and describes examples.

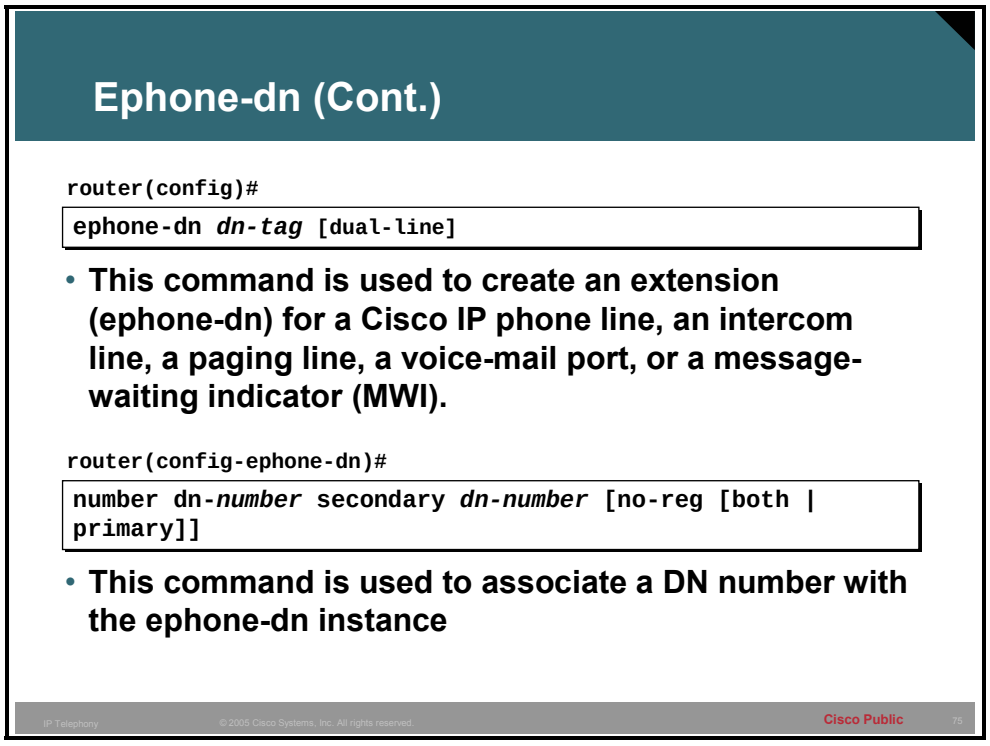


An ephone-dn, or "Ethernet phone directory number," is a software construct that represents the line that connects a voice channel to a phone instrument on which a user can receive and make calls. An ephone-dn has one or more extension or telephone numbers associated with it to allow call connections to be made. An ephone-dn is equivalent to a phone line in most cases, but not always. There are several types of ephone-dns, which have different characteristics.

Each ephone-dn has a unique dn-tag, or sequence number, to identify it during configuration. Ephone-dns are assigned to line buttons on ephones during configuration. The number of ephone-dns that you create corresponds to the number of simultaneous calls that you can have because each ephone-dn represents a virtual voice port in the router. This means that if you want more than one call to the same number to be answered simultaneously, you need multiple virtual voice ports (ephone-dns) with the same destination pattern (extension or telephone number).

Ephone-dns can be configured in various ways these include:

- Primary DN on a single line ephone-dn
- Primary and secondary DN on a single line the ephone-dn
- Primary DN on a dual-line ephone-dn (only one line has active voice at any time)



An ephone-dn is created by the **ephone-dn *dn-tag*** command, which builds one virtual voice port. The ***dn-tag*** field will need to contain a unique number if this is a new ephone-dn or an existing number if a current ephone-dn is being modified. If the ephone-dn is to be assigned an extension and assigned to a phone line it should be able to have two calls to the same line at the same time. The ephone-dn should then have the **dual-line** keyword at the end of the **ephone-dn** command. The **dual-line** keyword will need to be present to be able to use an ephone-dn for call-waiting, consultative transfers, and conferencing with only one line appearance on the phone. An ephone-dn without the **dual-line** keyword will be used when the ephone-dn is configured for paging functions, intercoms, voice mail ports, or MWI signals.

Note	The ***dn-tag*** numbers do not have to be entered sequentially.

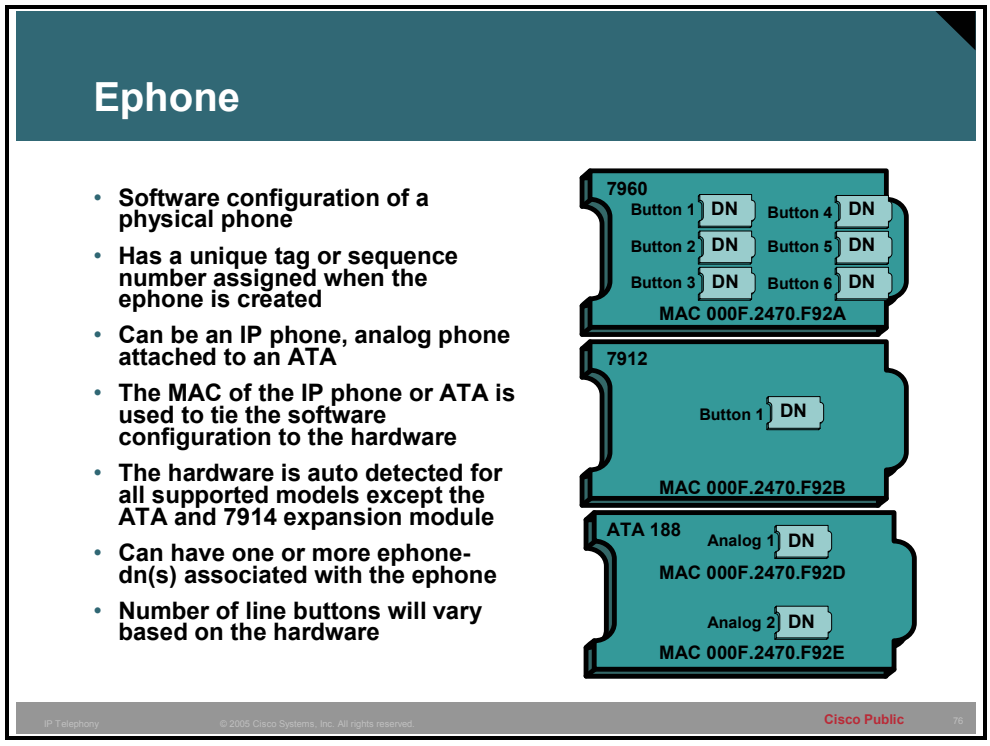
The command **number *dn-number*** assigns a primary and optionally a secondary number to the ephone-dn, and is entered in ephone-dn sub configuration mode.

The **no-reg** keyword can be used if either the primary extension or both the primary extension and the secondary extension should not be registered to either a H.323 gatekeeper or SIP proxy server. For example, a service provider that sells Cisco CME may not want to have the primary extension number registered because there may be many clients with the same dial plan. The secondary number which would most likely be an E.164 number would be registered with a H.323 Gatekeeper. The **number *dn-number* secondary *dn-number* no-reg primary** command would be added to the configuration of the ephone-dn to configure this.

 Copyright © 2005, Cisco Systems, Inc.

Ephone

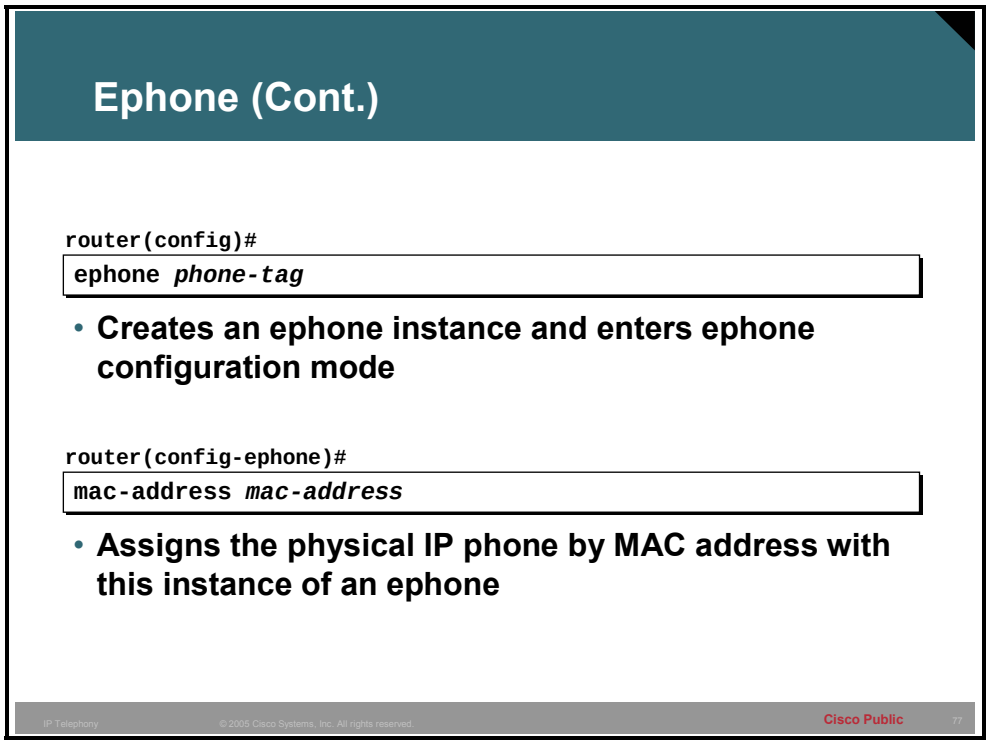
This topic defines ephone and describes examples.



An ephone, or "Ethernet phone," is a single instance of the software configuration of the physical instrument with which a phone user makes and receives calls in a Cisco CME system. The physical ephone is either a Cisco IP phone or an analog telephone adaptor (ATA) device with an attached analog phone or fax.

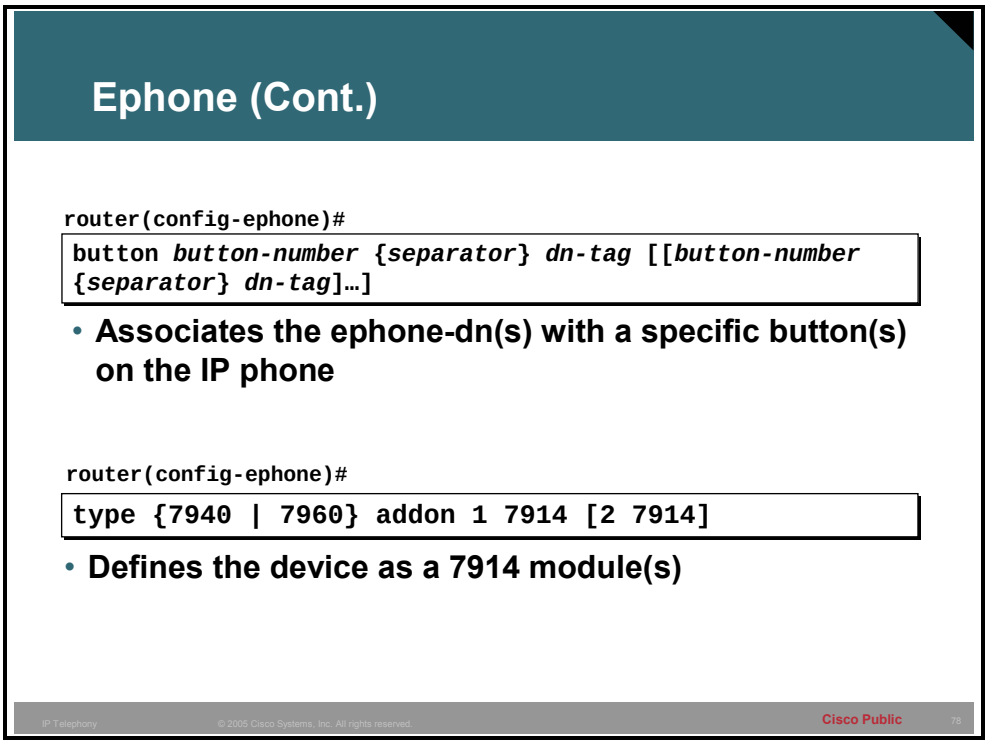
Note	The Cisco IP Softphone and IP Communicator are not currently supported as valid ephones. However, certain third-party vendors have a softphone that works (IP Blue).

Each ephone has a unique ***phone-tag***, or sequence number, to identify it during configuration. This phone tag number must be unique if configuring a new ephone or a preexisting number if modifying a current ephone. Once in the ephone sub-configuration mode the ephone must be tied to the physical device by using the MAC address. The type of phone must be defined if one or two 7914 add on module are present or if the device is an ATA 186 or ATA 188. All other types of phones will be auto detected by the Cisco CME system. The ephone-dns will then have to be assigned to the line buttons of the ephone or add on modules. The number of line buttons will vary with the model of IP phone.



The ephone is created or modified by entering the **ephone *phone-tag*** command from global configuration mode. Once the command is entered, the interface will be in ephone sub-configuration mode and the ephone-specific commands entered. The command **mac-address *mac-address*** is entered with twelve hex characters entered in groups of four separated by a period (Example 0000.0c12.3456). This associates the physical device the defined MAC address with the ephone.

 Copyright © 2005, Cisco Systems, Inc.

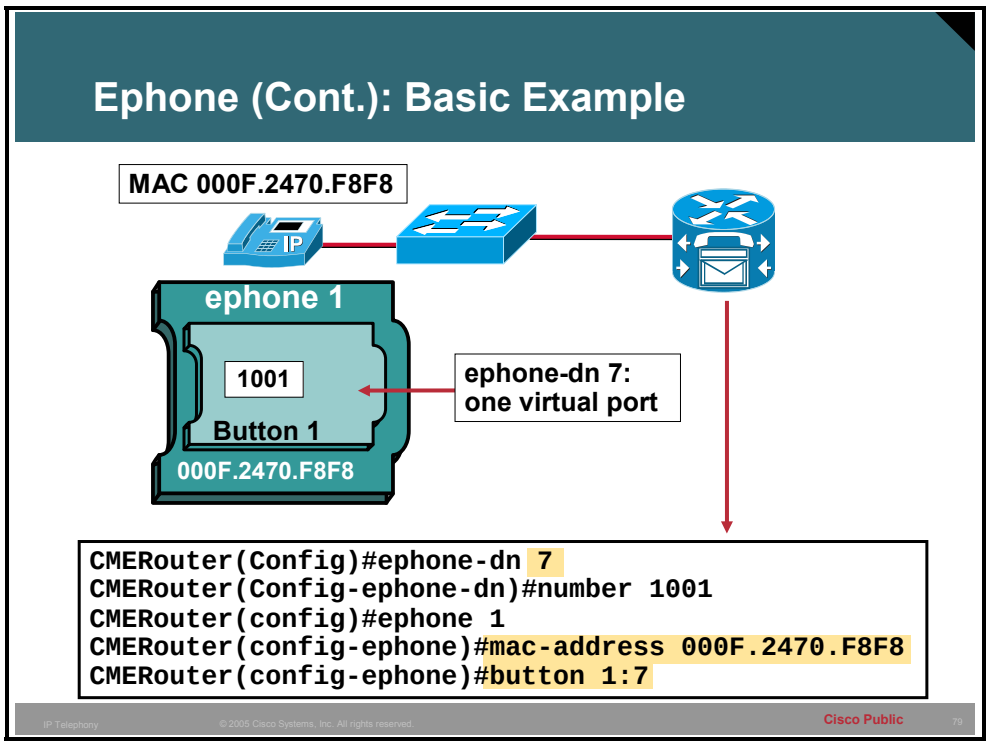


The **button** ***button-number {separator} dn-tag*** command allows a line button to have an ephone-dn assigned to it. The button number is the button on the IP phone starting with the top button being number one. The dn-tag is the ephone-dn tag or sequence number. The separator is a single character that defines the properties of the button and the extension, these include the following:

- **:** (colon)—Normal ring. For incoming calls on this extension, the phone produces audible ringing, a flashing ((< icon in the phone display, and a flashing red light on the handset. On the Cisco IP Phone 7914 Expansion Module, a flashing yellow light also accompanies incoming calls.
- **b**—Beep but no ring. Audible ring is suppressed for incoming calls, but call-waiting beeps are allowed. Visible cues are the same as those described for a normal ring.
- **f**—Feature ring. Differentiates incoming calls on a special line from incoming calls on other lines on the phone. The feature ring cadence is a triple pulse, as opposed to a single pulse for normal internal calls and a double pulse for normal external calls.
- **m**—Monitor mode for a shared line. Visible line status indicates in-use or not. Line cannot be used on this phone for incoming or outgoing calls.
- **o**—Overlay line. Multiple ephone-dns share a single button, up to a maximum of ten on a button. The *dn-tag* argument can contain up to ten individual dn-tags, separated by commas.
- **s**—Silent ring. Audible ring and call-waiting beep are suppressed for incoming calls. Visible cues are the same as those described for a normal ring.

The command **type {7940 | 7960} addon 1 7914** sets the ephone to have either a 7940 or 7960 with either one or two 7914 expansion modules assigned to. This command is required if using the 7914 expansion module.

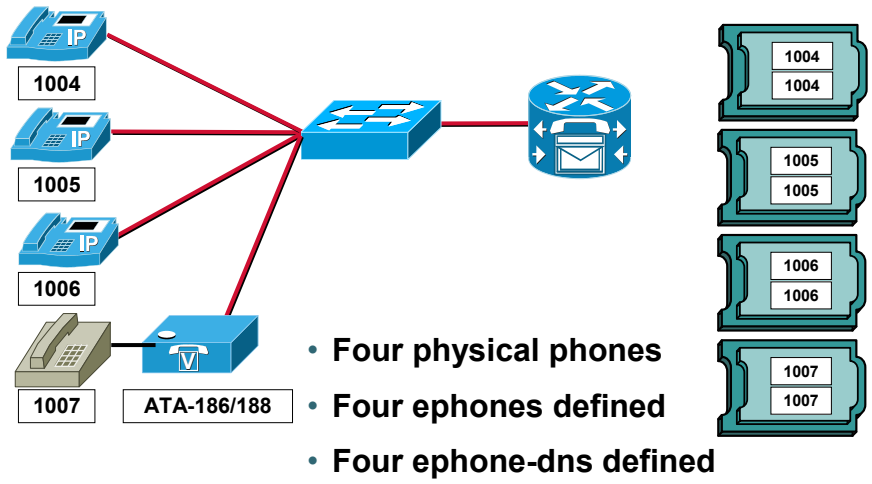
Example



This example shows an ephone-dn 7 being created and then assigned to the ephone 1. The ephone-dn is configured to be dual-line and is assigned to line button one on the IP phone at the specified MAC address.

 Copyright © 2005, Cisco Systems, Inc.

Ephone (Cont.): Example Multiple Ephones



© 2005 Cisco Systems, Inc. All rights reserved.

When there are multiple physical devices, there will need to be the same number of ephones defined. Each ephone will then have one or more ephone-dns assigned to line buttons on the physical device. The configuration for this example follows.

Example

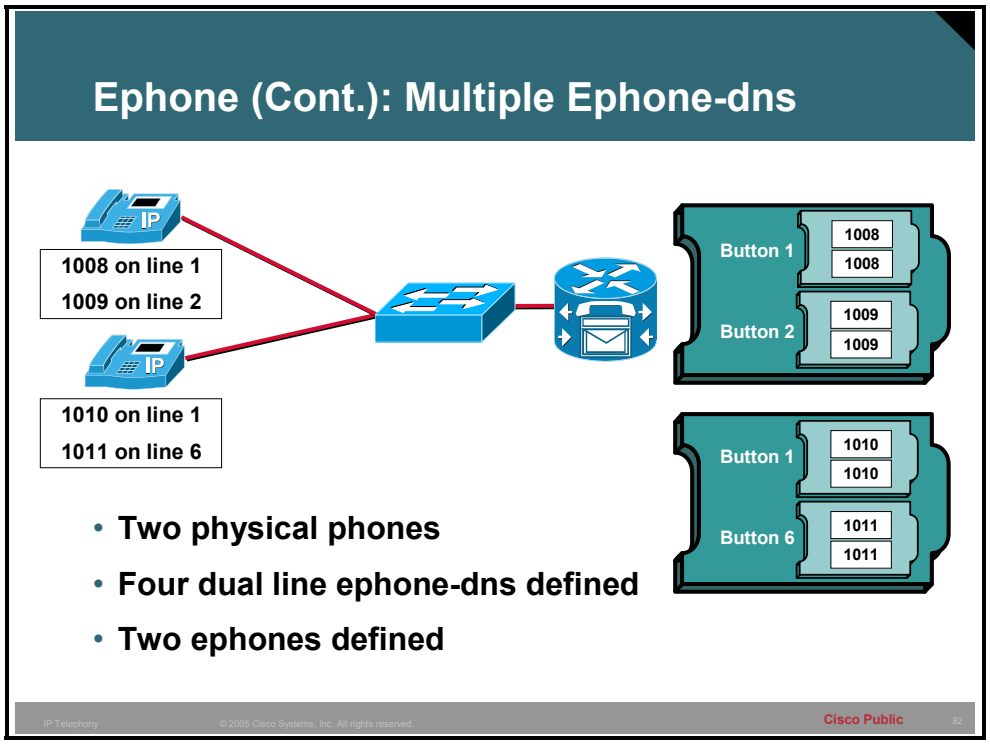
Ephone (Cont.): Example Multiple Ephones Configuration

Configuration example

```
CMERouter(config)#ephone-dn 10 dual-line
CMERouter(config-ephone-dn)#number 1004
CMERouter(config)#ephone-dn 11 dual-line
CMERouter(config-ephone-dn)#number 1005
CMERouter(config)#ephone-dn 12dual-line
CMERouter(config-ephone-dn)#number 1006
CMERouter(config)#ephone-dn 13 dual-line
CMERouter(config-ephone-dn)#number 1007
CMERouter(config)#ephone 1
CMERouter(config-ephone)#mac-address 000F.2470.F8F1
CMERouter(config-ephone)#button 1:10
CMERouter(config)#ephone 2
CMERouter(config-ephone)#mac-address 000F.2470.A302
CMERouter(config-ephone)#button 1:11
CMERouter(config)#ephone 3
CMERouter(config-ephone)#mac-address 000F.2470.66F6
CMERouter(config-ephone)#button 1:12
CMERouter(config)#ephone 4
CMERouter(config-ephone)#mac-address 000F.2470.7B54
CMERouter(config-ephone)#type ata
CMERouter(config-ephone)#button 1:13
```

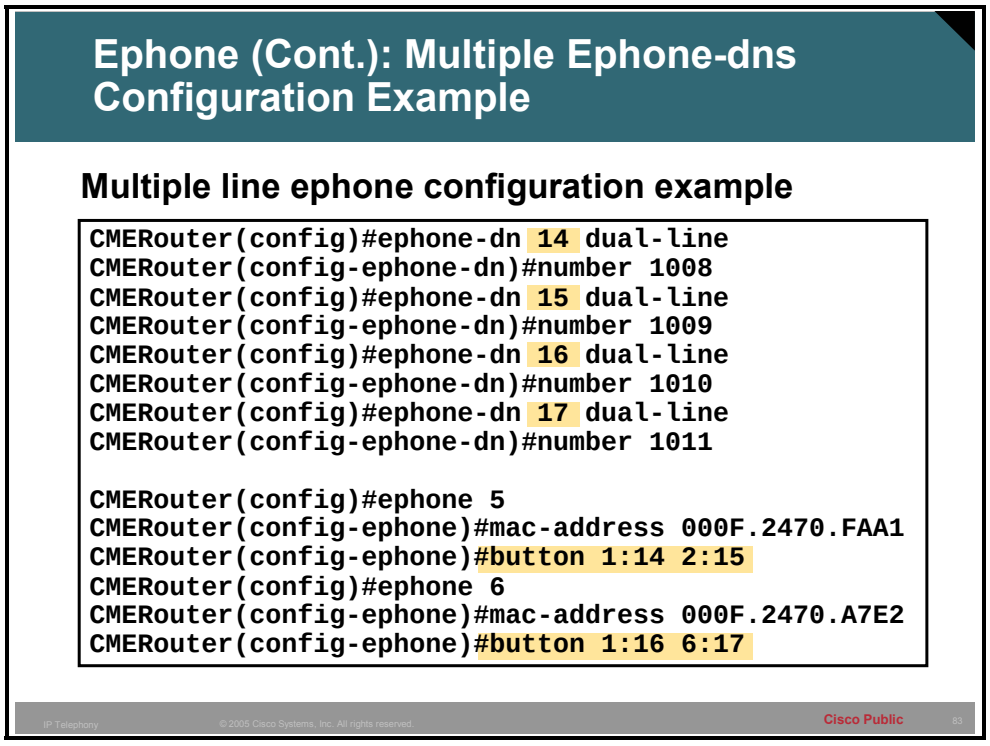

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc.



In this example, there are multiple ephone-dn assigned to the ephone. The ephone-dn is assigned to different buttons on the ephone. The configuration for this example follows.

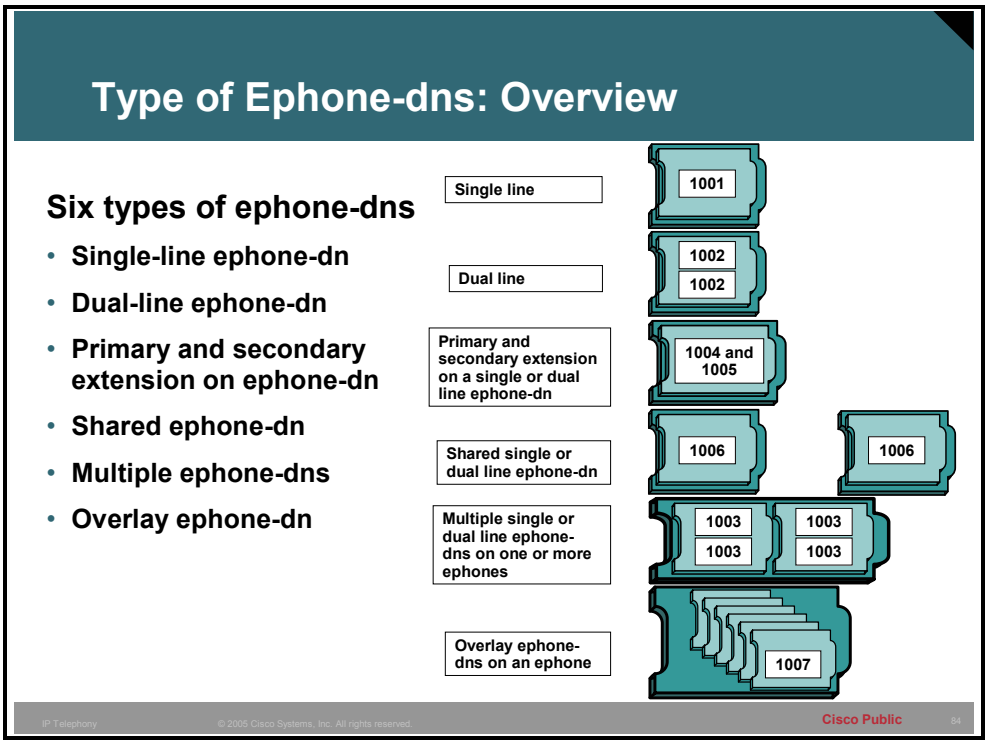
Example



 Copyright © 2005, Cisco Systems, Inc.

Type of Ephone-dns

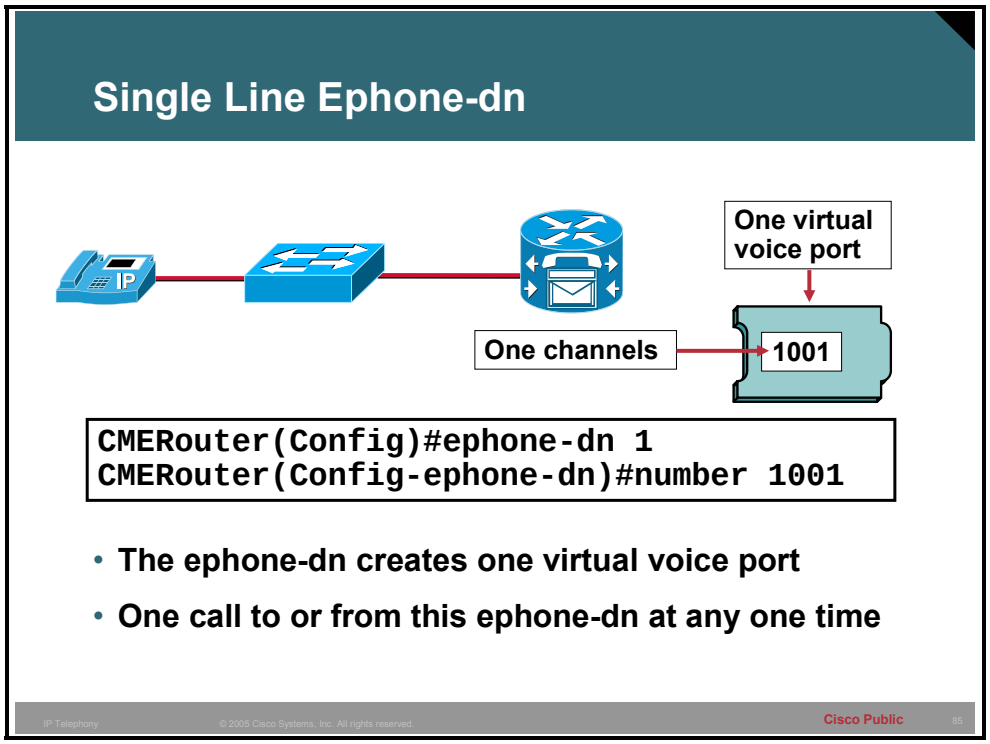
This topic describes the different types of ephone-dns.



The ephone-dn is the basic building block of a Cisco CME system. Six different types of ephone-dn can be combined in different ways for different call coverage situations. Each type will help with a particular type of limitation or call coverage need. For example, if you want to keep the number of ephone-dns low and provide service to a large number of people, you might use shared ephone-dns. Or if you have a limited number of extension numbers that you can use but need to have a large number of simultaneous calls, you might create two or more ephone-dns with the same number. The key is knowing how each type of ephone-dn works and what its advantages are.

The following sections will help you understand the types of ephone-dn in a Cisco CME system:

- Single-line ephone-dn
- Dual-line ephone-dn
- Primary and secondary extension on one ephone-dn
- Shared ephone-dn
- Multiple ephone-dns on one ephone
- Overlay ephone-dn

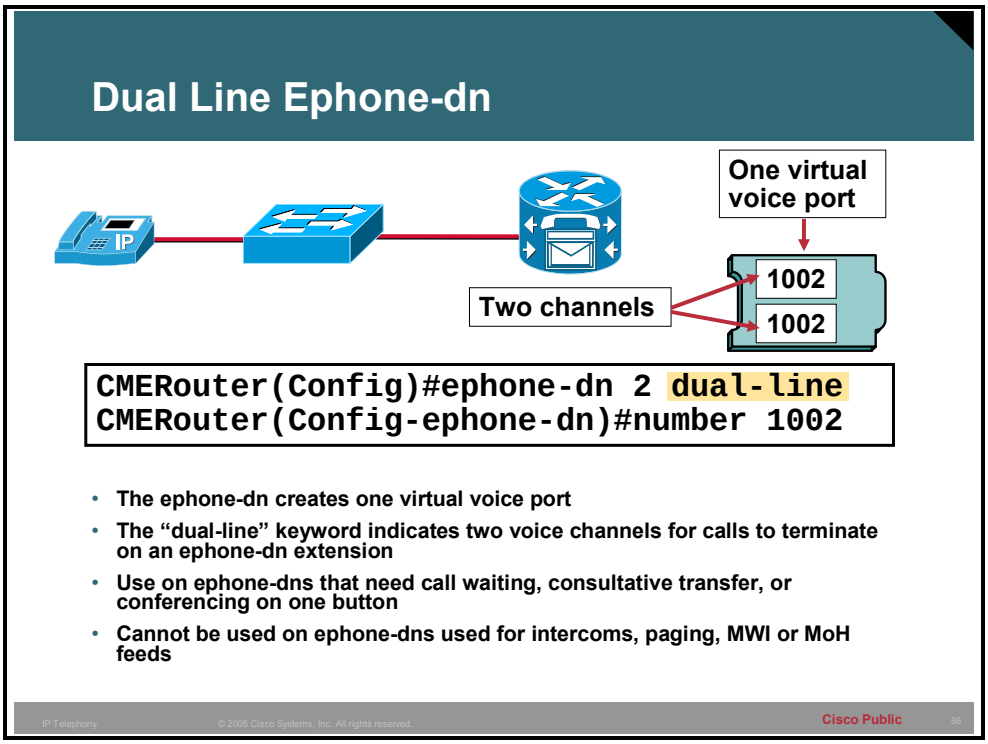


A single-line ephone-dn has the following characteristics:

- Makes one call connection at a time using one phone line button. A single-line ephone-dn has one telephone number associated with it.
- Should be used when phone buttons have a one-to-one correspondence to the PSTN lines that come into a Cisco CME system.
- Should be used for lines that are dedicated to intercom, paging, message-waiting indicator (MWI), loopback, and music-on-hold (MOH) feed sources.
- When used with multiple-line features like call waiting, call transfer, and conferencing, there must be more than one single-line ephone-dn on a phone.
- Can be combined with dual-line ephone-dns on the same phone.
- A multiple-line button phone must be used if call waiting, consultative transfer, or conferencing are needed

Note	A choice is made to configure each ephone-dn in the system as either dual-line or single-line when ephone-dn is initially created. If the selection made needs to be changed from single-line to dual-line, or dual-line to single-line, the ephone-dn must be deleted and then recreated.

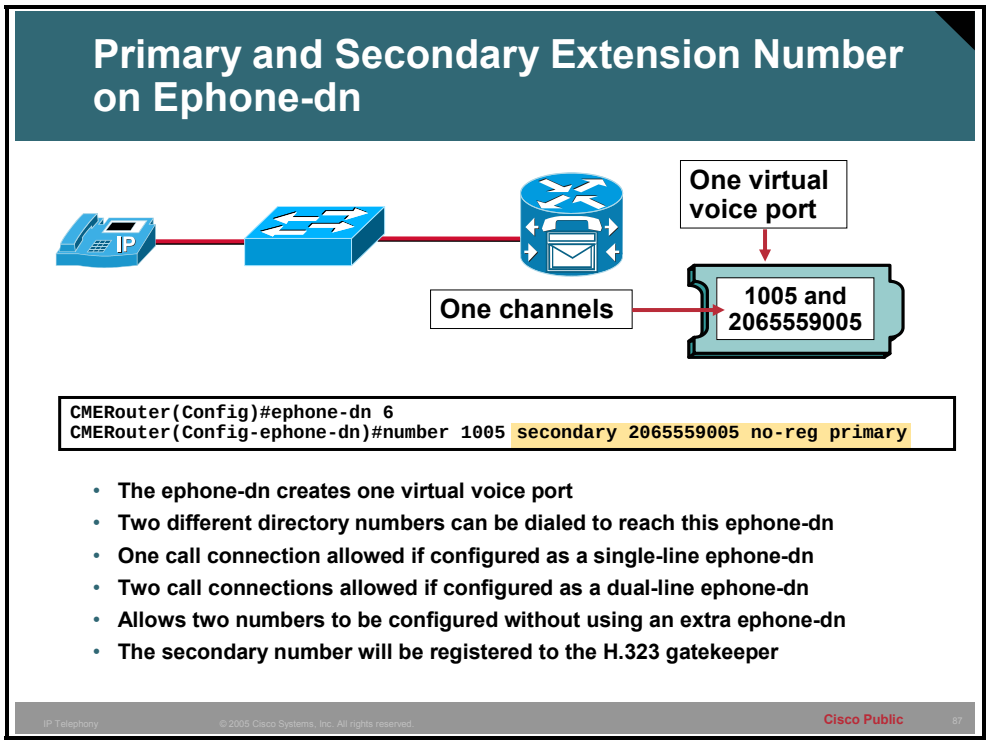
 Copyright © 2005, Cisco Systems, Inc.



A dual-line ephone-dn has the following characteristics:

- Can make two call connections at the same time using one phone line button. A dual-line ephone-dn has two channels for separate call connections.
- Can have one number or two numbers (primary and secondary) associated with it.
- Should be used for an ephone-dn that needs to use just a single button for features like call waiting, call transfer, or conferencing.
- Cannot be used for lines that are dedicated to intercom, paging, message-waiting indicator (MWI), loopback, and music-on-hold (MOH) feed sources.
- Can be combined with single-line ephone-dns on the same phone.

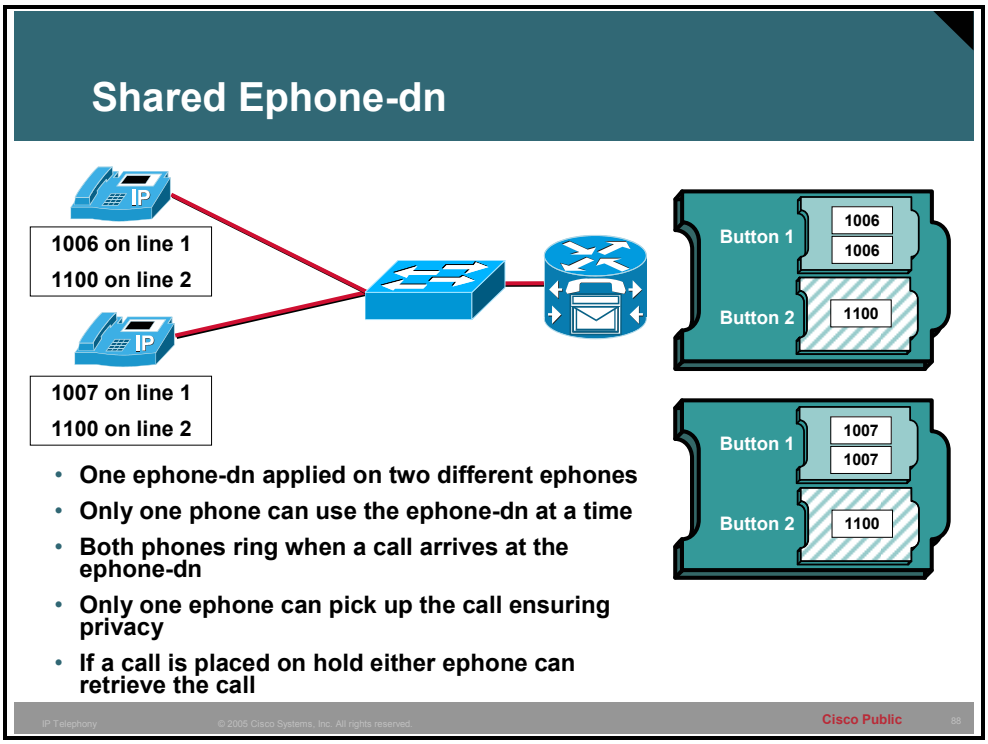
Note	A choice is made to configure each ephone-dn in the system as either dual-line or single-line when ephone-dn is initially created. If the selection made needs to be changed from single-line to dual-line, or dual-line to single-line, the ephone-dn must be deleted and then created again.



A dual-number ephone-dn has the following characteristics:

- Has two telephone numbers: a primary number and a secondary number
- Can make one call connection if it is a single-line ephone-dn
- Can make two call connections at a time if it is a dual-line ephone-dn
- Should be used when you want to have two different numbers for the same button without using more than one ephone-dn
- The secondary number will register with the H.323 gatekeeper

 Copyright © 2005, Cisco Systems, Inc.



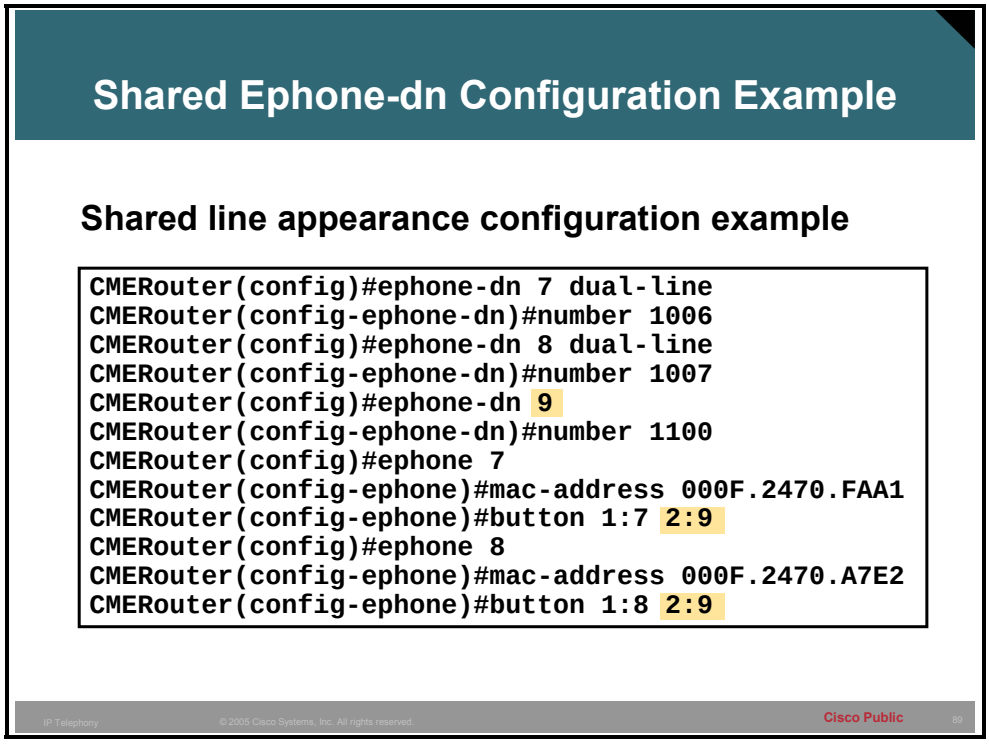
A shared ephone-dn has the following characteristics:

- Appears on two different phones but uses the same ephone-dn and number
- Can make one call at a time between the two phones, and that call appears on both phones
- Should be used when you want the capability to answer or pick up a call at more than one phone
- Only one ephone can pick up the call, ensuring privacy
- When the call is placed on hold, either ephone can retrieve the call

If the ephone-dn is connected to a call on one phone, that ephone-dn is unavailable for other calls on the second phone because these phones share the same ephone-dn. If a call is placed on hold on one phone, it can be retrieved on the second phone.

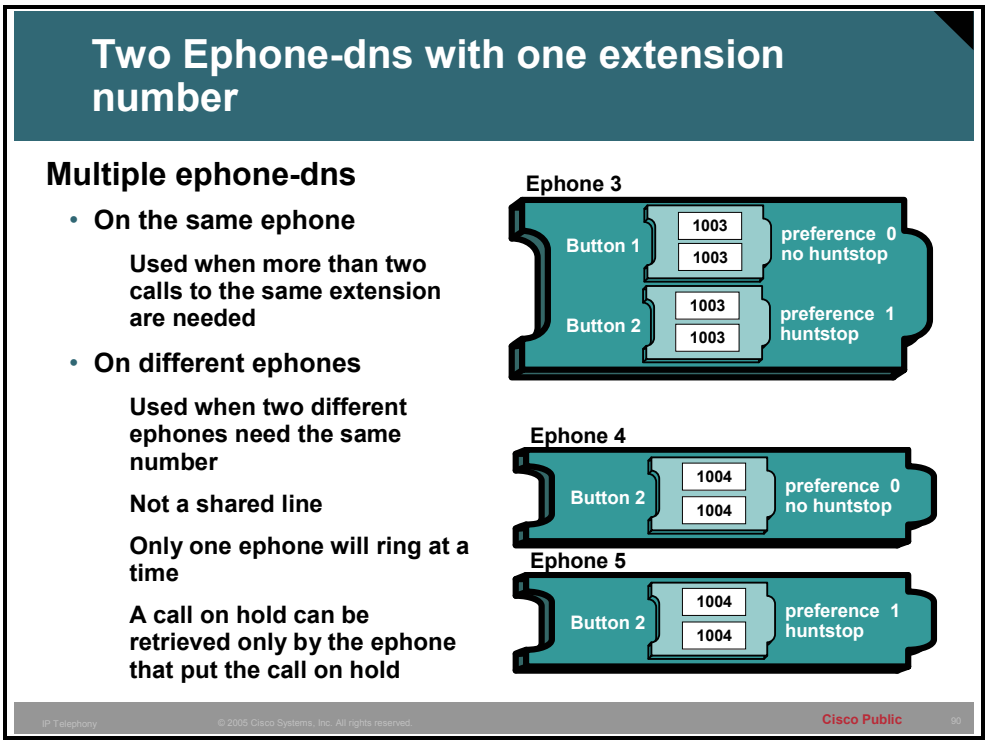
The configuration for this example follows.

Example



This example shows the configuration for the previous page.

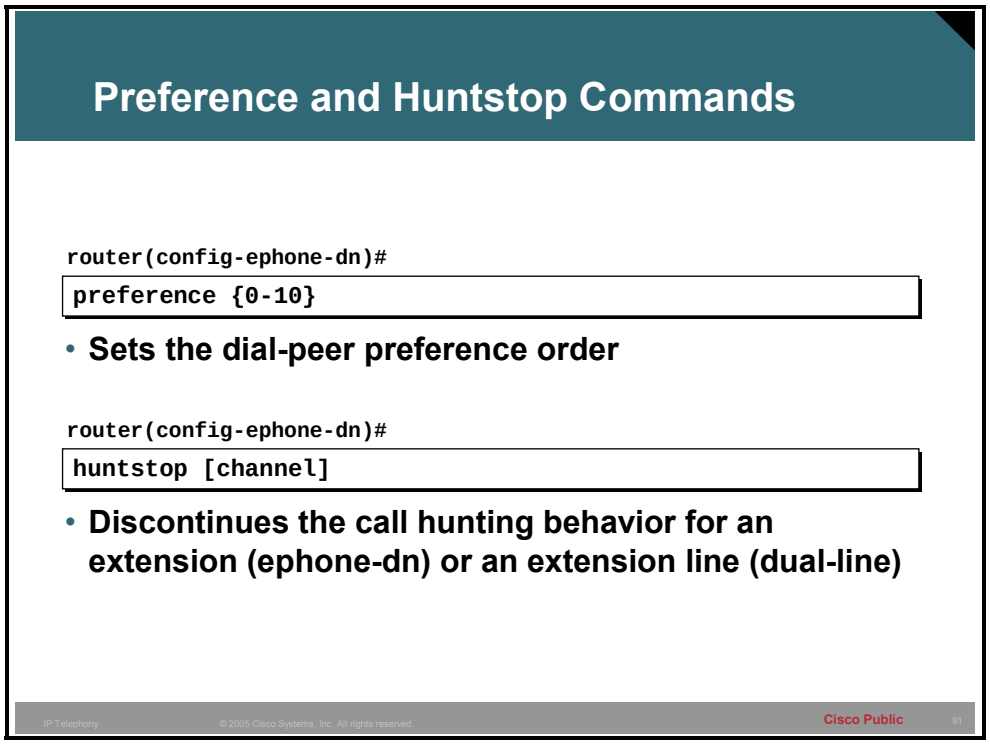
 Copyright © 2005, Cisco Systems, Inc.



There are two different ways for multiple ephone-dns with the same extension number to be utilized. One way is for multiple ephone-dns to be assigned to the same ephone but on separate line buttons. This type of configuration will be useful when more than two calls at a time may arrive at a destination and need to be handled. For example, if 6 calls at a time need to be handled, then 3 ephone-dns that are dual-line can all be configured with the same extension number.

The other way that multiple ephone-dns with the same extension number can be configured is on different ephones. This will be a different configuration than a shared line. This will be used when two or more ephones need to be able to answer the same number and this will also provide some very basic huntgroup functionality. The characteristics of this type of configuration will be:

- Two or more virtual ports with the same extension number
- Not a shared line
- Two call connections allowed per ephone-dn if configured as dual-line, one if not
- The preference and huntstop command are used to configure hunting behavior
- Only one ephone will ring at a time
- Call on hold can be retrieved by only the ephone that placed the call on hold initially



Values assigned in the **preference** command are passed to the dial peers created by the two ephone-dns. Both dial peers for the ephone-dns are matched when this extension number is dialed. The call is connected to the ephone-dn with the highest preference. The default preference value is 0 (the most preferred); the lowest preference value that can be set is 10 (the least preferred).

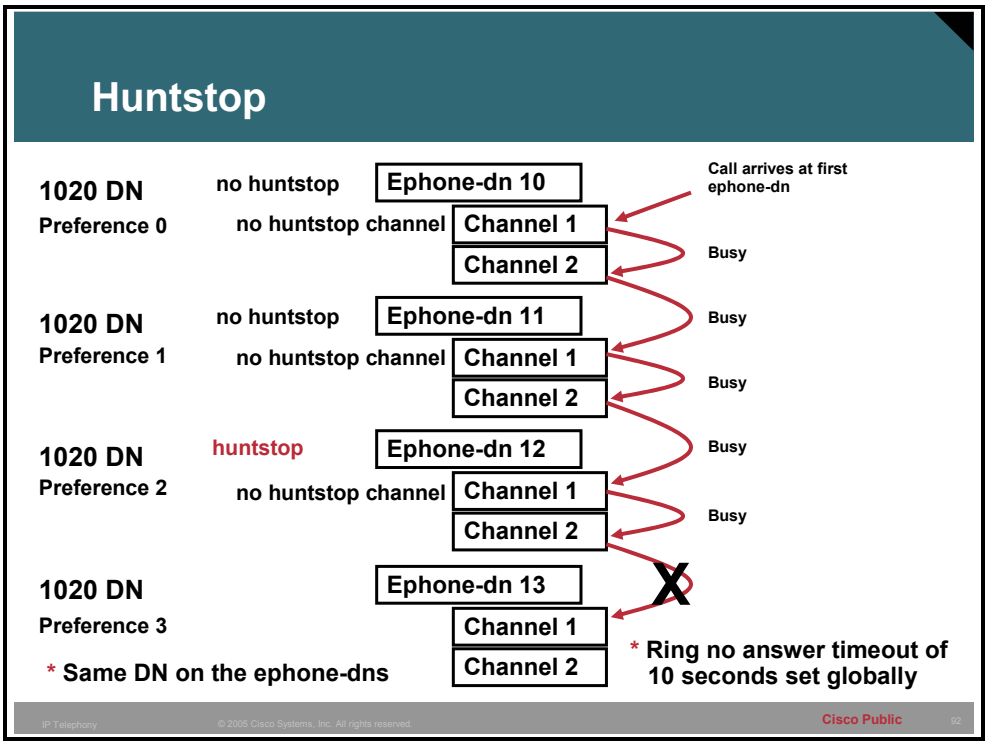
When using the **huntstop** (default setting on ephone-dns) command without the **channel** keyword, it effects call hunting behavior that relates to ephone-dns (lines or extensions). If the huntstop attribute is set, an incoming call does not roll over (hunt) to another ephone-dn when the called ephone-dn is busy or does not answer and a hunting strategy has been established that includes this ephone-dn. For example, this allows the prevention of hunt-on-busy from redirecting a call from a busy phone into a dial-peer setup with a catch-all default destination. Use the **no huntstop** command under the ephone-dn to disable huntstop and allow hunting for ephone-dns.

Channel huntstop works in a similar way but it effects call hunting behavior for the two channels of a single dual-line ephone-dn. If the **huntstop channel** command is used, incoming calls do not hunt to the second channel of an ephone-dn when the first channel is busy or does not answer. For example, an incoming call might search through the following ephone-dns and channels:

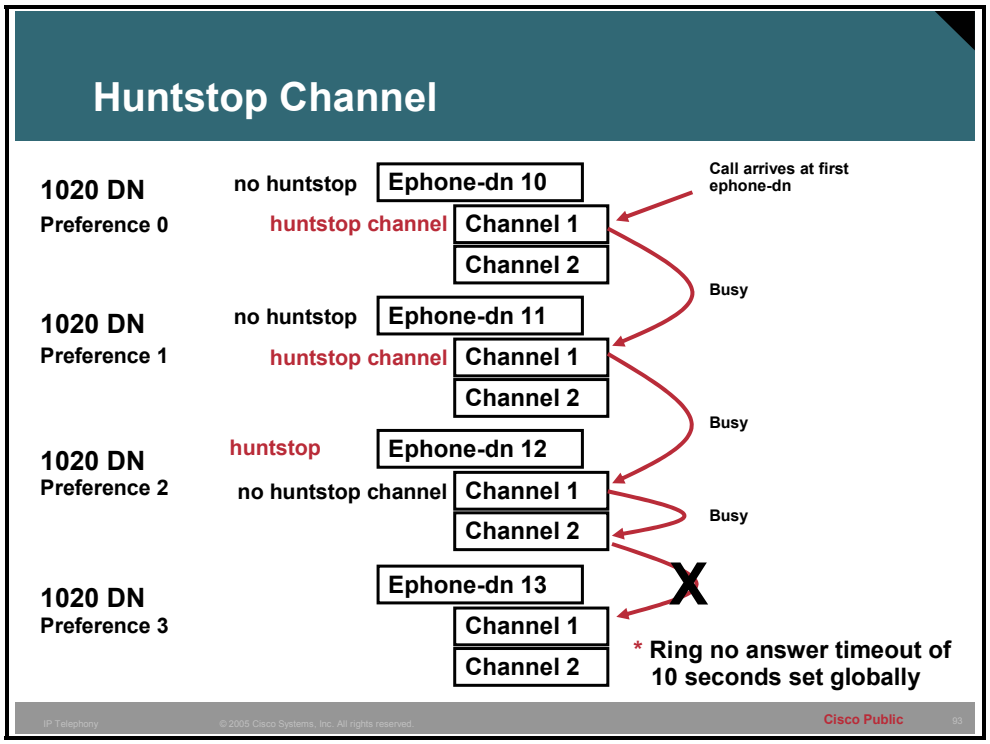
- ephone-dn 10 (channel 1)
- ephone-dn 10 (channel 2)
- ephone-dn 11 (channel 1)
- ephone-dn 11 (channel 2)
- ephone-dn 12 (channel 1)
- ephone-dn 12 (channel 2)

 Copyright © 2005, Cisco Systems, Inc.

When the **no huntstop channel** command is used (the default), you might have a call ring for 30 seconds on ephone-dn 10 (channel 1) and then after 30 seconds move to ephone-dn 10 (channel 2). This is usually not the behavior that you desire. Also, it is often useful to reserve the second channel of a dual-line ephone-dn for call transfer, call waiting, or conferencing. The **huntstop channel** command tells the system that if the first channel is in use or does not answer, an incoming call should hunt forward to the next ephone-dn in the hunt sequence instead of to the next channel on the same ephone-dn.



When the **no huntstop** command is used on the ephone-dn, the call would ring on the first ephone-dn and go through any hunting defined on the two channels in a dual-line ephone-dn before being sent to the next most preferred ephone-dn that also has a matching destination pattern. This will continue until an ephone-dn with huntstop configured is reached or no more dial peers (ephone-dns) have matching destinations patterns.



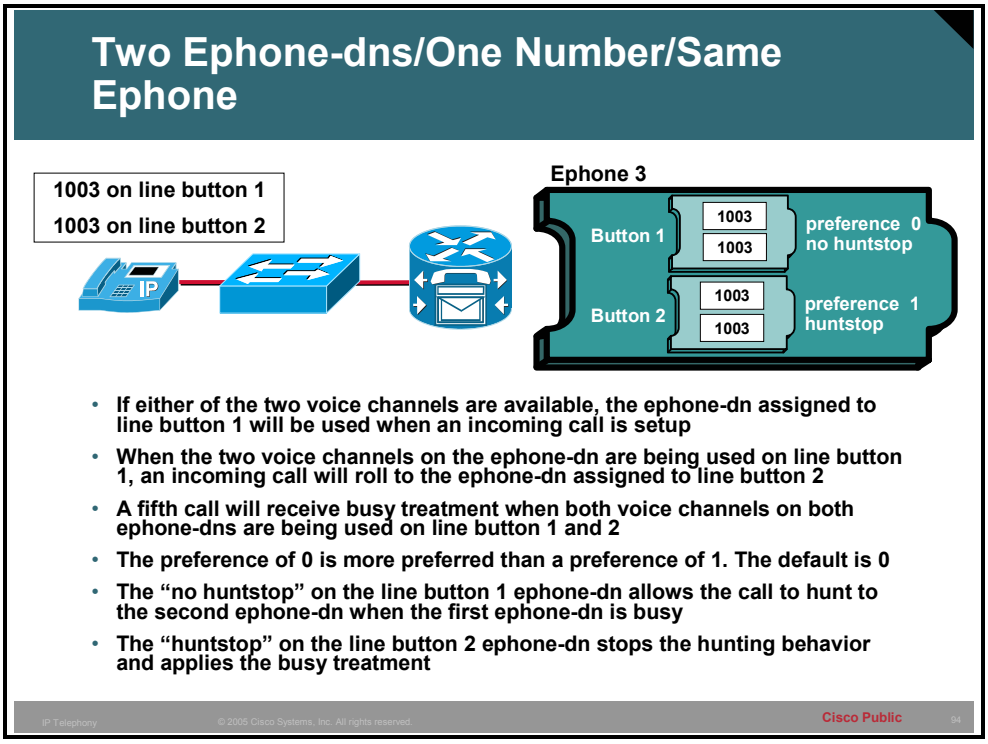
Channel huntstop works in a similar way, but it affects call hunting behavior for the two channels of a single dual-line ephone-dn. If the **huntstop channel** command is used, incoming calls do not hunt to the second channel of an ephone-dn when the first channel is busy or does not answer.

When the **no huntstop channel** command is used (the default), you might have a call ring for 10 seconds on ephone-dn 10 (channel 1) and then after 10 seconds move to ephone-dn 10 (channel 2). This is usually not the behavior that you desire in a dual line phone.

It is often useful to reserve the second channel of a dual-line ephone-dn for call transfer, call waiting, or conferencing. The **huntstop channel** command tells the system that if the first channel is in use or does not answer, an incoming call should hunt forward to the next ephone-dn in the hunt sequence instead of to the next channel on the same ephone-dn.

 Copyright © 2005, Cisco Systems, Inc.

Example



When the two different ephone-dns that have the same number are assigned to different buttons of the same ephone and a call arrives, it will go to the ephone-dn that is most preferred based upon the preference setting. If the first ephone-dn is busy or not answered, the call will go to the second ephone-dn. Because the buttons have different ephone-dns, the calls that are connected on these buttons are independent of one another.

The configuration for this example follows.

Two Ephone-dns/One Number/Same Ephone

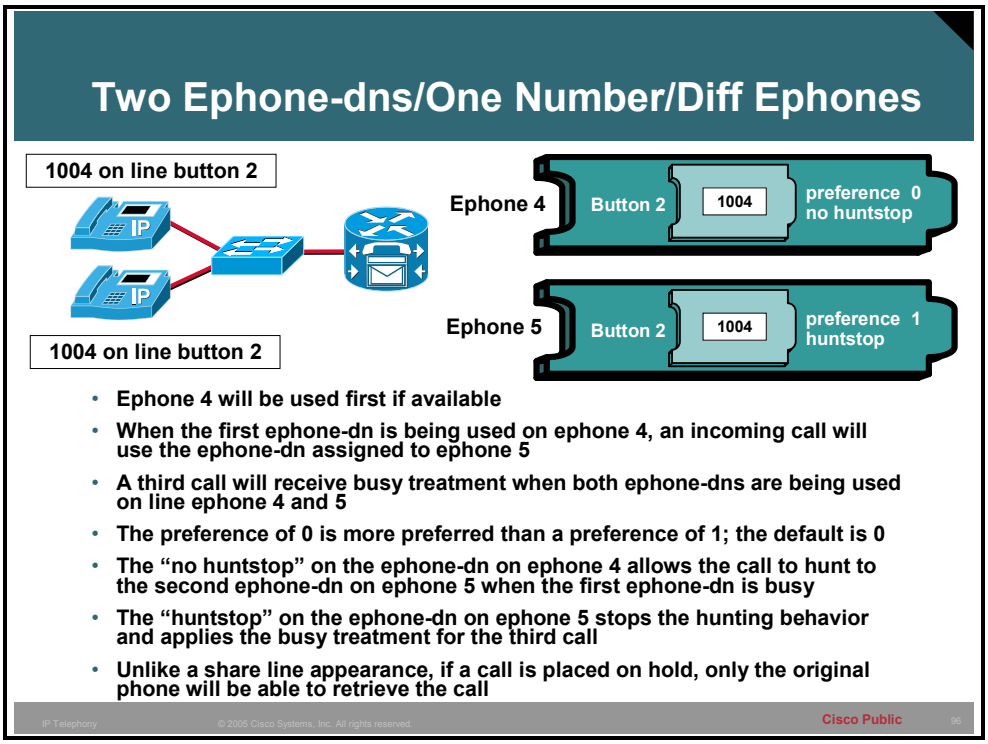
Two ephone-dns with one number on the same ephone configuration example

```
CMERouter(config)#ephone-dn 3
CMERouter(config-ephone-dn)#number 1003
CMERouter(config-ephone-dn)#preference 0
CMERouter(config-ephone-dn)#no huntstop
CMERouter(config)#ephone-dn 4
CMERouter(config-ephone-dn)#number 1003
CMERouter(config-ephone-dn)#preference 1
CMERouter(config-ephone-dn)#huntstop
CMERouter(config)#ephone 3
CMERouter(config-ephone)#mac-address 000F.2470.FAA1
CMERouter(config-ephone)#button 1:3 2:4
```

IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 95

This example shows the configuration for the previous page

 Copyright © 2005, Cisco Systems, Inc.

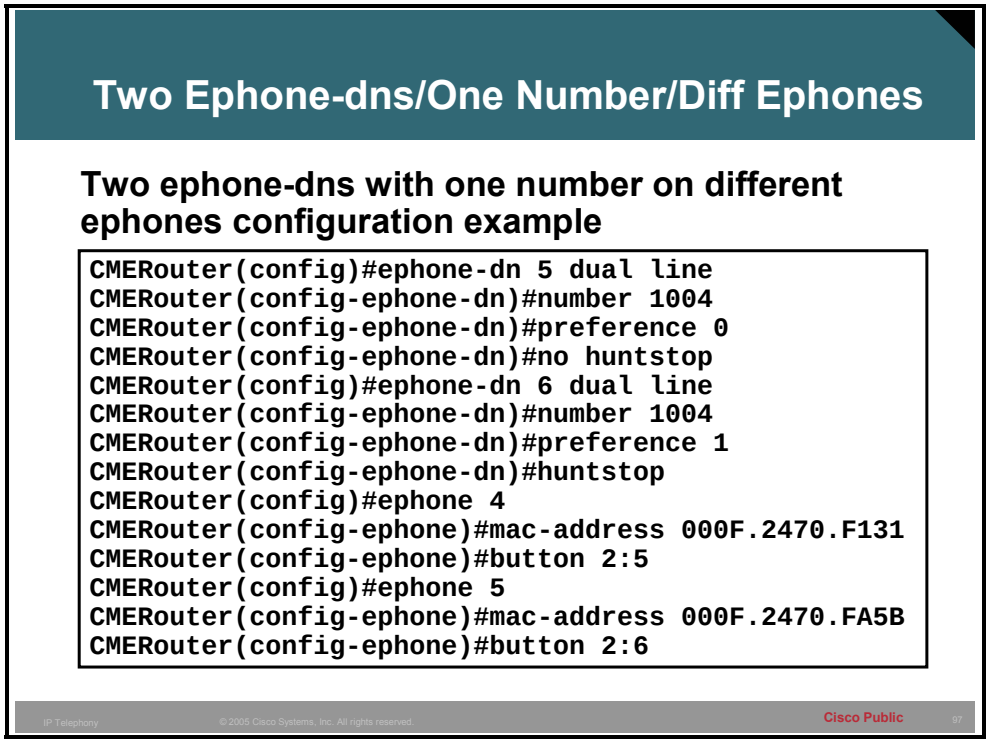


A shared line that also has two ephones with a line on each with the same number but has only one shared ephone-dn for both of them is different than two ephones having separate ephone-dns with the same number.

A shared ephone-dn will have the same call connection at all the buttons on which the shared ephone-dn appears. If a call on a shared ephone-dn is answered on one ephone and then placed on hold, the call can be retrieved from the second ephone on which the shared ephone-dn appears. But when there are two separate ephone-dns with the same number, a call connection appears only on the phone and button at which the call is made or received. If the call is placed on hold on one ephone, it cannot be retrieved from the other ephone with an ephone-dn with the same number because this is a different virtual voice port.

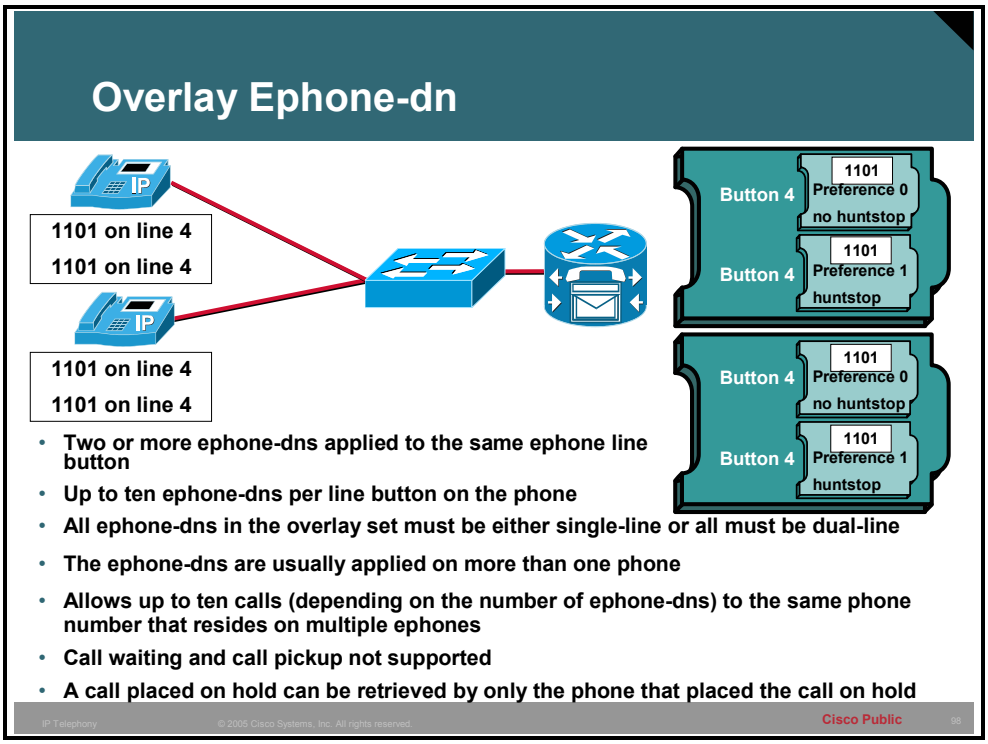
The configuration for this example follows.

Example



This example shows the configuration for the previous page.

 Copyright © 2005, Cisco Systems, Inc.



An overlay ephone-dn has the following characteristics:

- Is a member of an overlay set, which includes all the ephone-dns that have been assigned together to a particular phone button
- Can have the same telephone or extension number as other members of the overlay set or different numbers
- Can be single-line or dual-line, but cannot be mixed single-line and dual-line in the same overlay set
- Can be shared on more than one phone

Overlay ephone-dns provide call coverage similar to shared ephone-dns because the same number can appear on more than one phone. The advantage of using two ephone-dns in an overlay arrangement rather than as simple shared ephone-dns is that a call to the number on one phone does not block the use of the same number on the other phone as would happen if this was a shared ephone-dn.

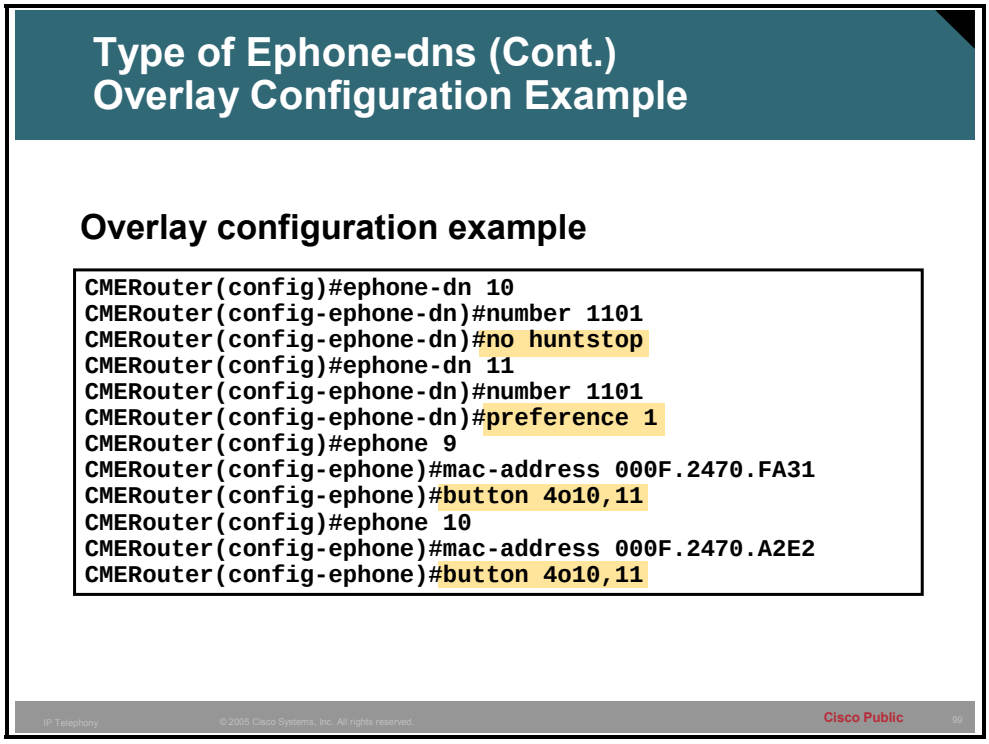
You can overlay up to ten lines on a single button and create a "10x10" shared line with ten lines in an overlay set shared by ten phones, resulting in the possibility of ten simultaneous calls to the same number.

An overlay is configured by use of an overlay separator with the **button** command. The separator is "**o**" to create the overlay. For example, the command **button 1o20,21,23,24,25** would configure ephone-dn 21, 22, 23, 24, and 25 on button 1 of the ephone.

The configuration for this example follows.

Example

This topic describes the different types of ephone-dns.

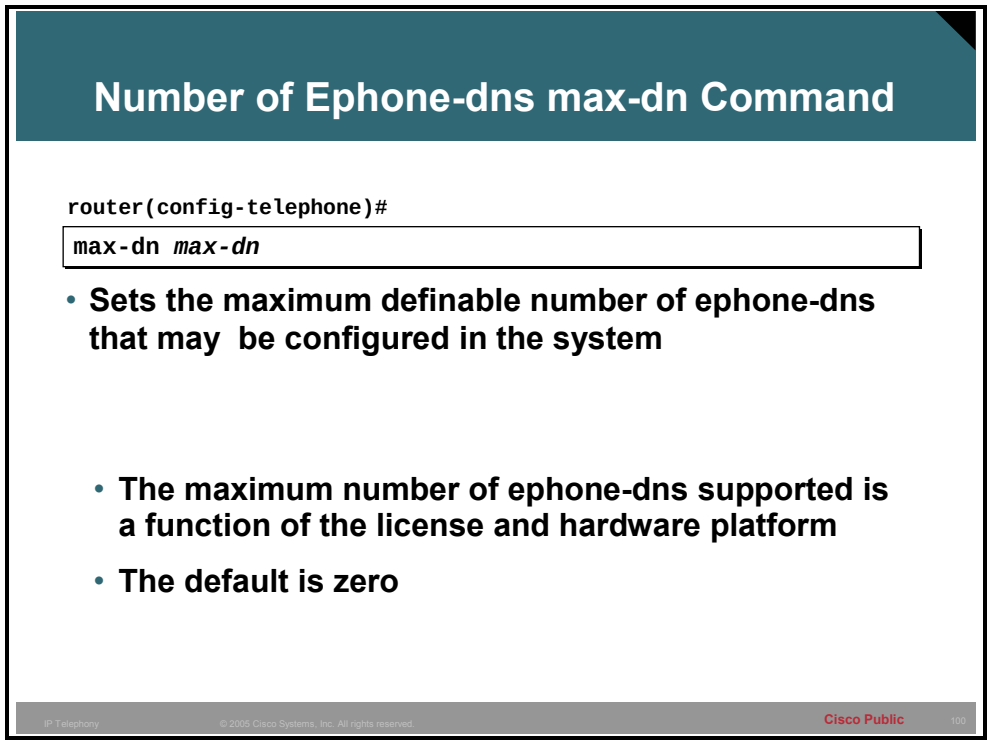


This example shows the configuration for the previous page.

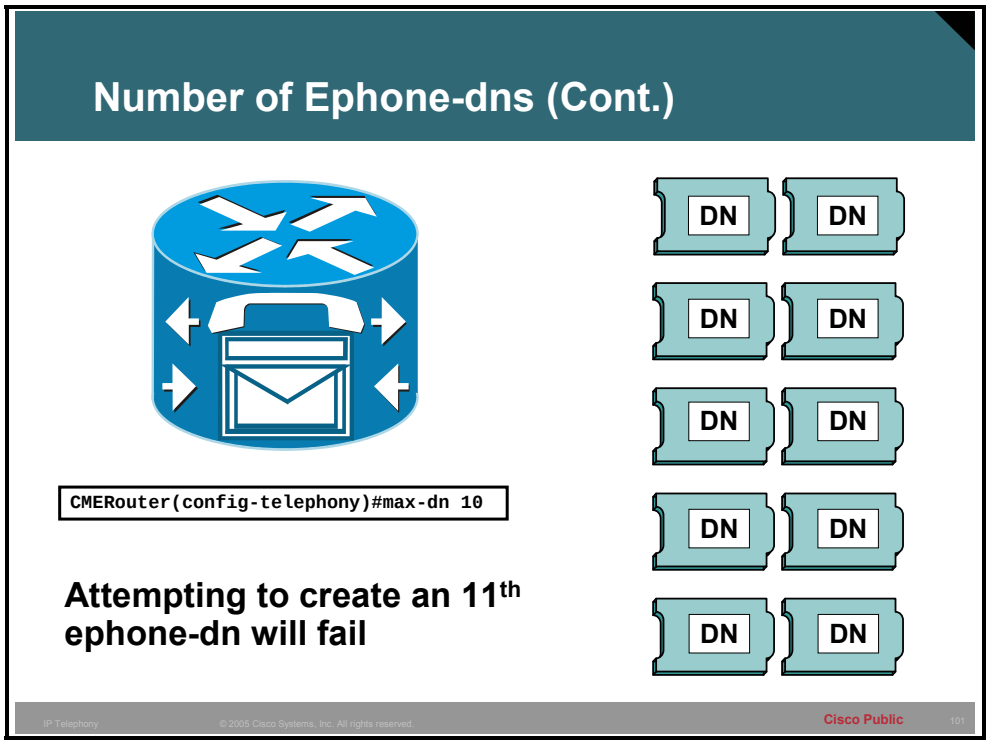
 Copyright © 2005, Cisco Systems, Inc.

Number of Ephone-dns

This topic explains the number of ephone-dn.



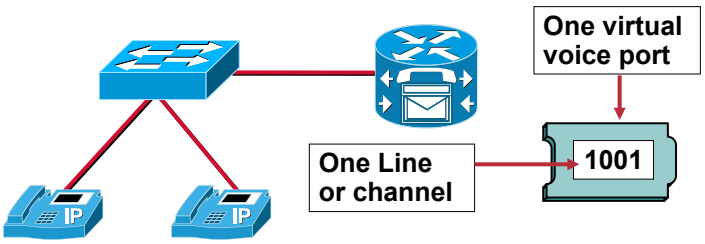
The maximum number of ephone-dns that can be configured is based upon the hardware platform that the Cisco CME software is installed on. The default of a newly installed Cisco CME system is that no ephone-dns can be configured. This is due to the command **max-dn** being set to zero. To allow the creation of ephone-dns set, use the command **max-dn ?** to determine the maximum allowable number of ephone-dns that the hardware supports. Set the value within that range to comply with the licensing.



In this graphic, the command **max-dn 10** is used and then 10 ephone-dns are created. The 11th ephone-dn to be created will send an error message to the console of the Cisco CME router and the creation of the ephone-dn will fail until the number of ephone-dns allowed is raised.

 Copyright © 2005, Cisco Systems, Inc.

Ephone-dn (Cont.): Basic Configuration




```
CMERouter(Config)#ephone-dn 7
CMERouter(Config-ephone-dn)#number 1001
```

- **Assigns a primary extension number to an ephone-dn**

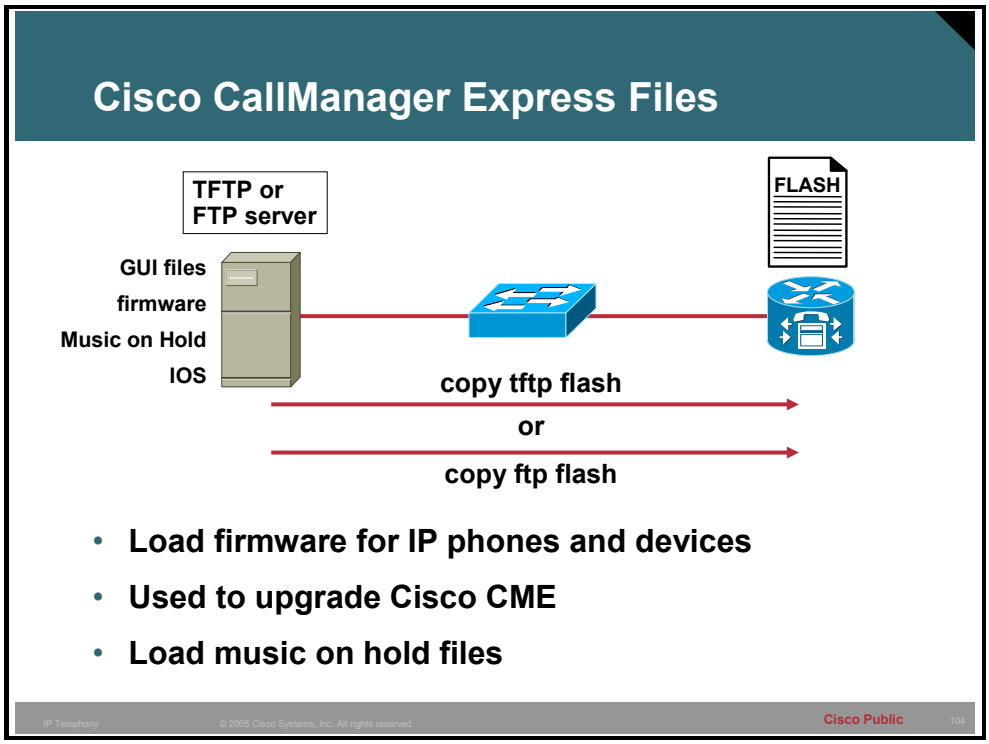
IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 102

When an ephone-dn is configured with a single line, one virtual voice port is configured and, since only a single line exists, only one call to or from the ephone-dn can be active. The second call that arrives while a call is active will receive whatever is the defined busy treatment. Configuring an ephone-dn in this fashion mimics typical functionality of a keyswitch line. This ephone-dn will lack some of the advanced PBX features.

Cisco CME Files

Cisco CME File

This topic describes Cisco CME files.



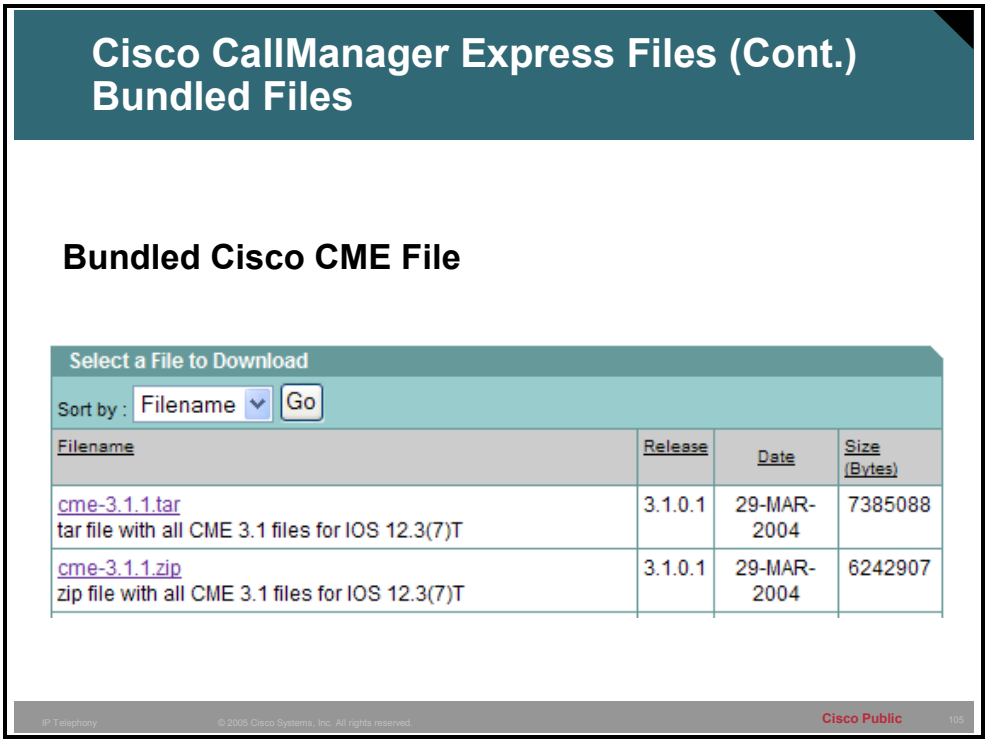
Cisco CME requires firmware files to be copied to the flash memory on your router and shared using Trivial File Transfer Protocol (TFTP) or the File Transfer Protocol (FTP). Download Cisco CME 3.1 files to a TFTP or FTP server that is accessible to your Cisco CME router. To move the files from the server to the flash memory, use the copy tftp flash command or the copy ftp flash command. You can download the files in a single bundle or individually.

When the Cisco CME router is upgraded, the new files like firmware, GUI files, and IOS will need to be moved to flash of the router. Other files like new firmware version and music on hold files may need to be periodically updated.

 Copyright © 2005, Cisco Systems, Inc.

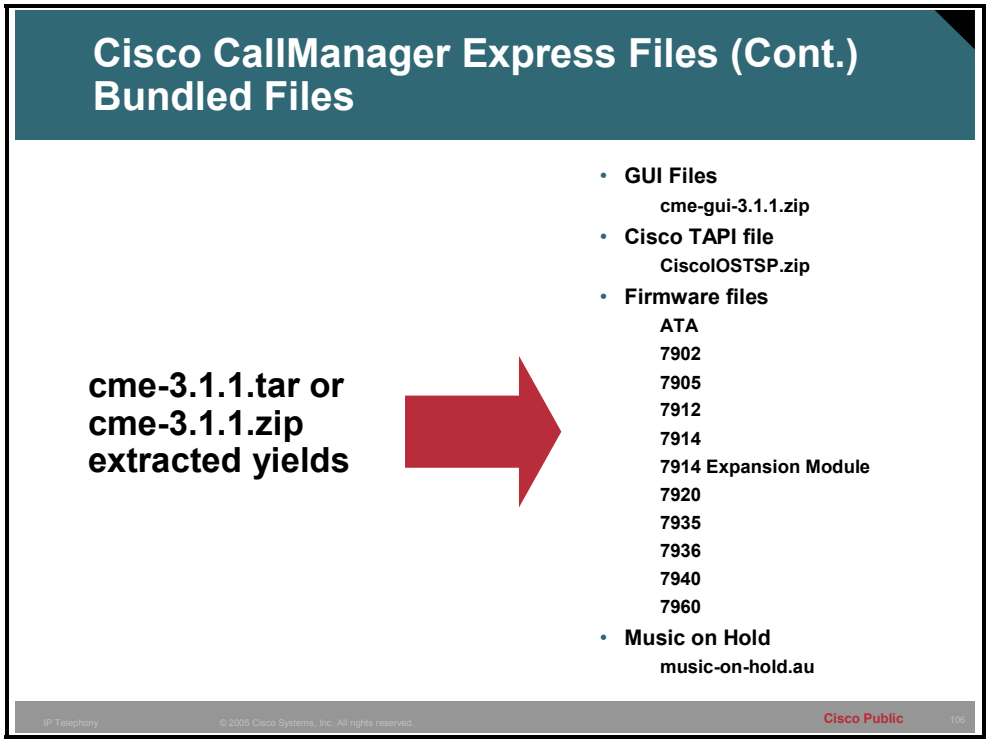
Bundled Cisco CME File

This topic describes downloading bundled Cisco CME files.



A bundled file with all of the Cisco CME files can be downloaded from cisco.com. The Cisco CME bundle comes in either a tar file or a zip file. These files can then be extracted on the FTP or TFTP server.

Reference The Cisco CME software can be found at the following URL:
http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml



The Cisco CME bundle contains all of the files needed to install and configure Cisco CME. The file contained in the bundle is listed in the graphic.

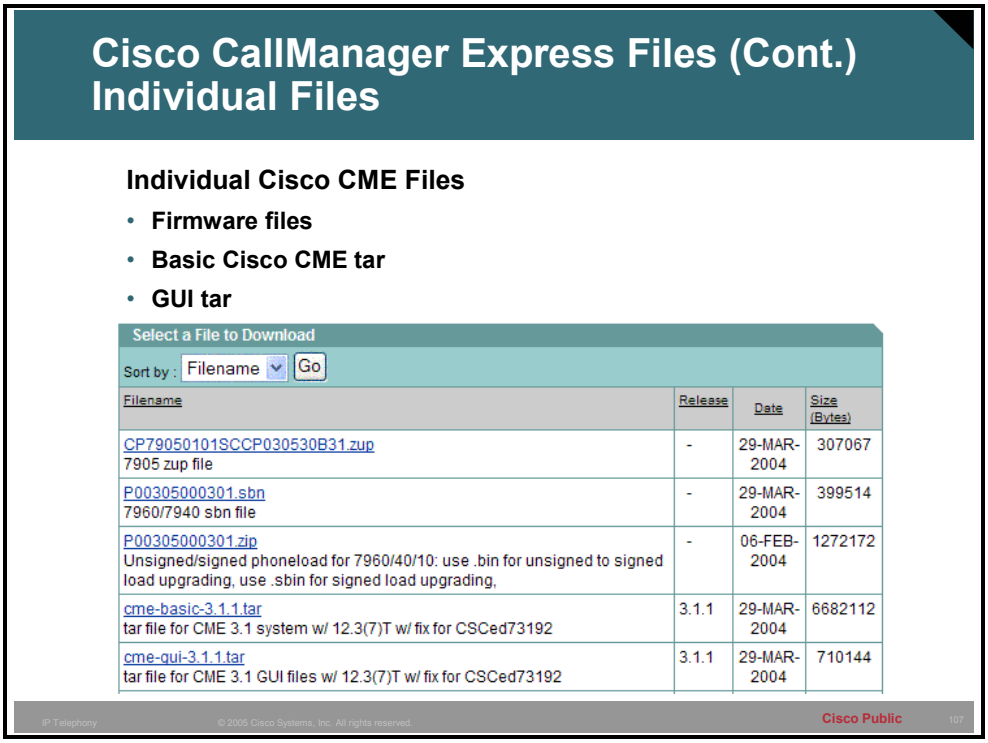
The cme-gui-3.1.1.zip file contains all the files needed to run the GUI Web interface for Cisco CME. These files will also be needed for the GUI of Cisco Unity Express.

The music-on-hold.au file can be used to provide music on hold from a file in flash. This can be replaced with a custom .wav or .au file if desired.

 Copyright © 2005, Cisco Systems, Inc.

Individual Cisco CME Files

This topic describes downloading individual Cisco CME files.

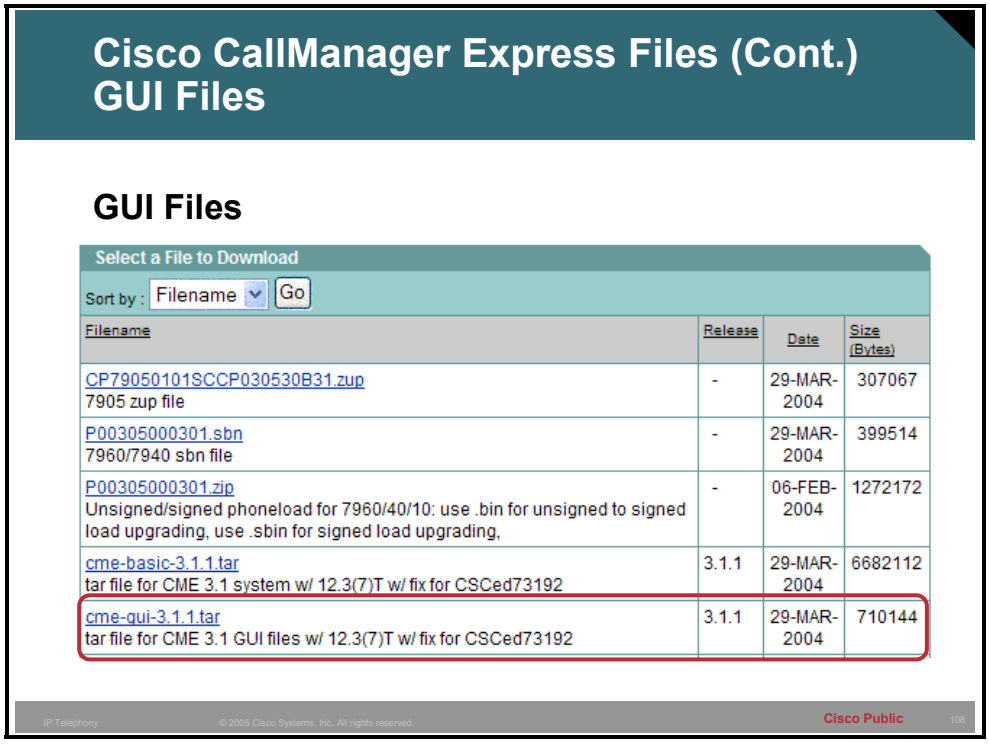


The files can be downloaded individually as well as in a bundle.

Note These files are version-specific and are not backwards compatible

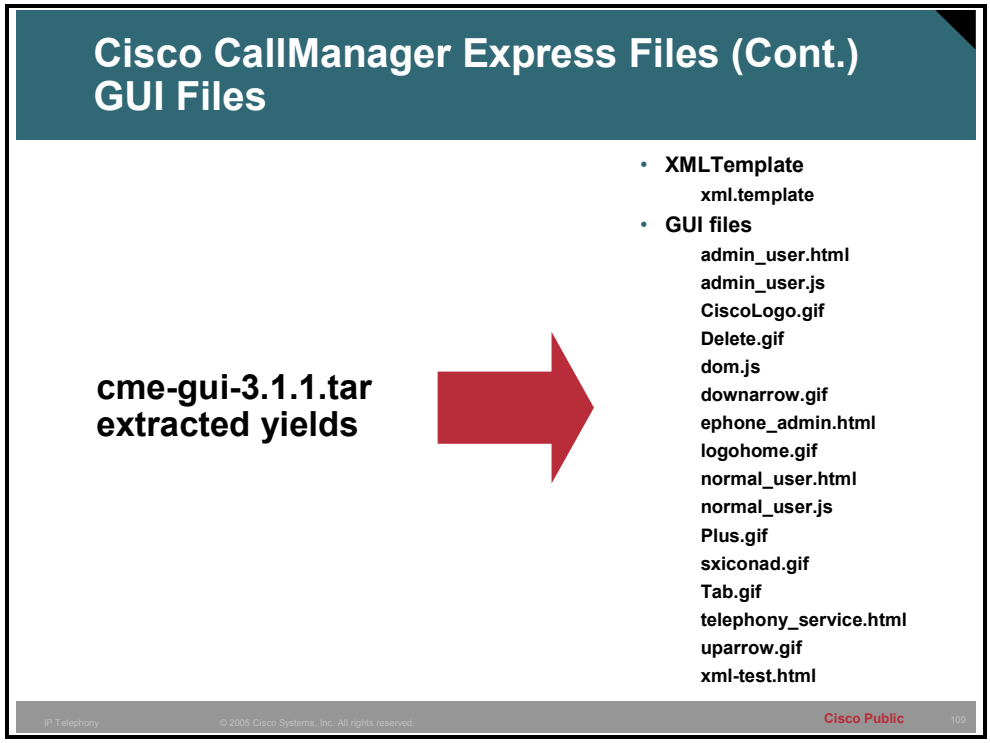
GUI Files

This topic identifies Cisco CME GUI files to enable Web access.



One of the individual files that can be downloaded is the tar that contains the GUI Web interface for Cisco CME. The Cisco Unity Express module GUI is also dependent on the CallManager GUI.

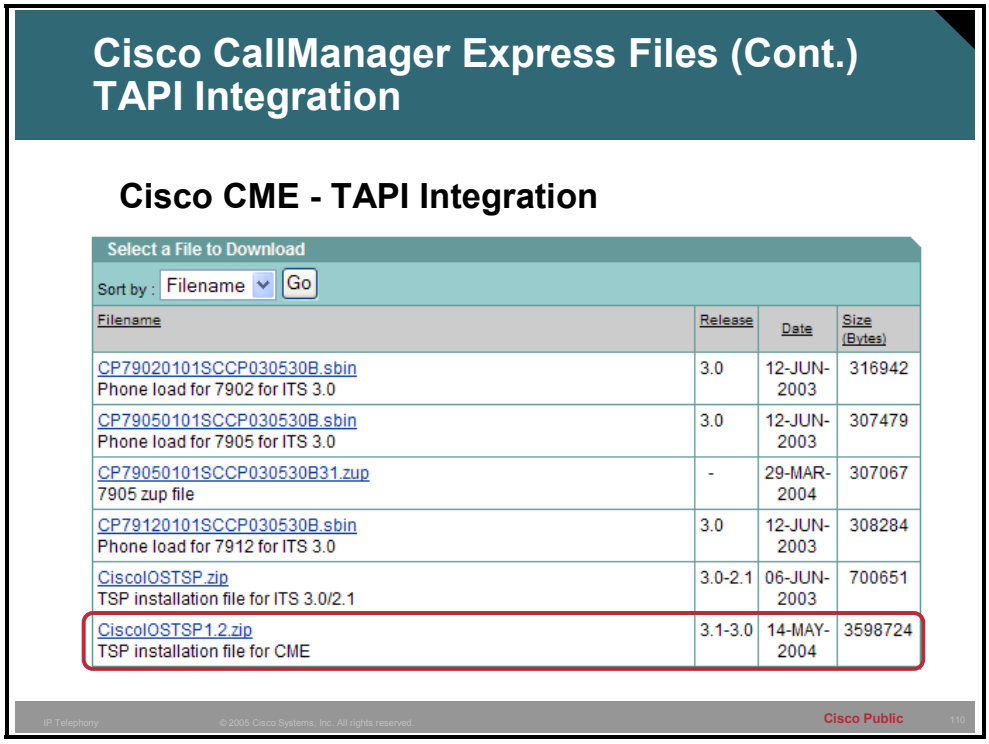
 Copyright © 2005, Cisco Systems, Inc.



The contents of the GUI Web interface tar file are shown above and these files will need to be present in the flash of the Cisco CME router. This will be covered in more detail in a later module.

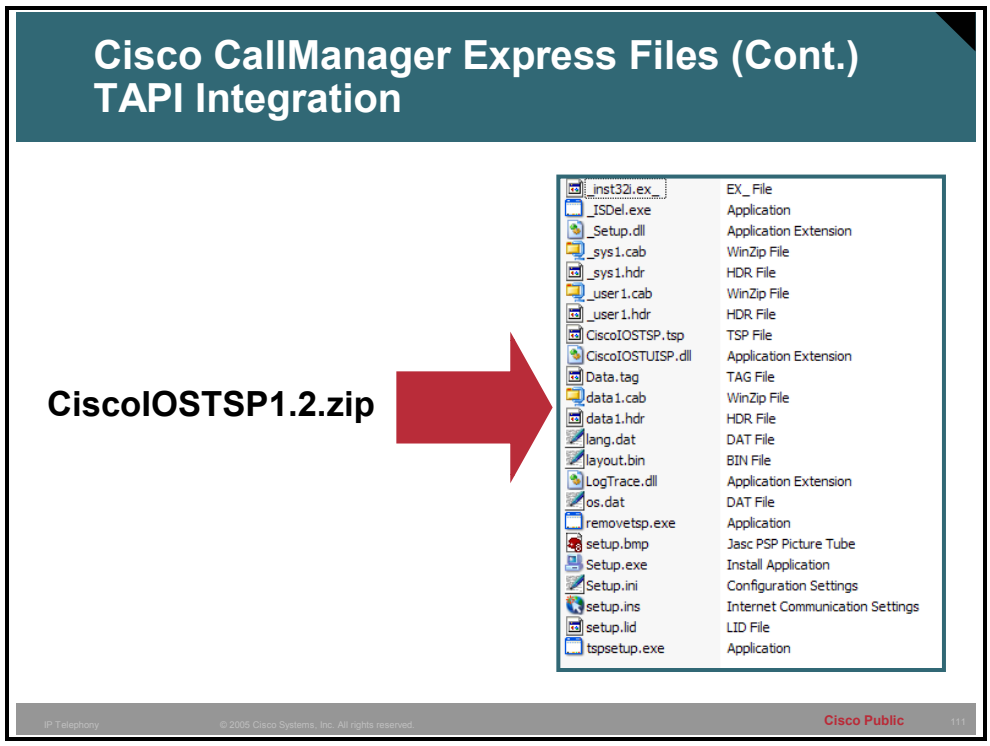
Cisco CME - TAPI Integration

This topic identifies TSP files for TAPI integration.



To allow a third-party piece of software to interact with the Cisco CME system through TAPI lite, the files in the IOS TSP file will need to be installed on the same Windows PC where the software will be installed. This will be covered in more detail in a later module.

 Copyright © 2005, Cisco Systems, Inc.

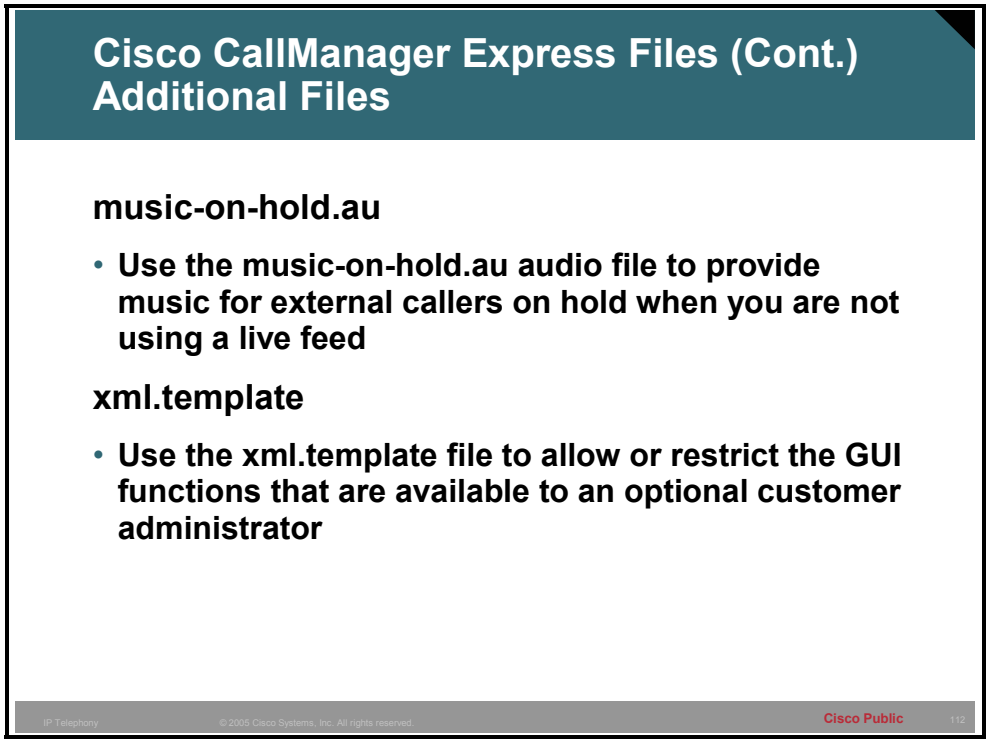


The content of the IOS TSP file are shown above. Run the setup.exe on the Windows PC where the TAPI integration is being performed. These files are version-specific and must be upgraded on the PC when Cisco CME is upgraded.

Note	This file does not need to reside in flash; it will be extracted and installed on a Windows PC.

Additional Files

This topic describes music-on-hold and xml.template files.



Other files that may be of interest include the file needed for music on hold (MoH). This file must reside in flash on the Cisco CME router and must be called music-on-hold.au. The file that comes in the bundle or was downloaded individually contains an audio file that will be used when a caller is placed on hold. This may be customized and this topic is covered in more detail in a later module.

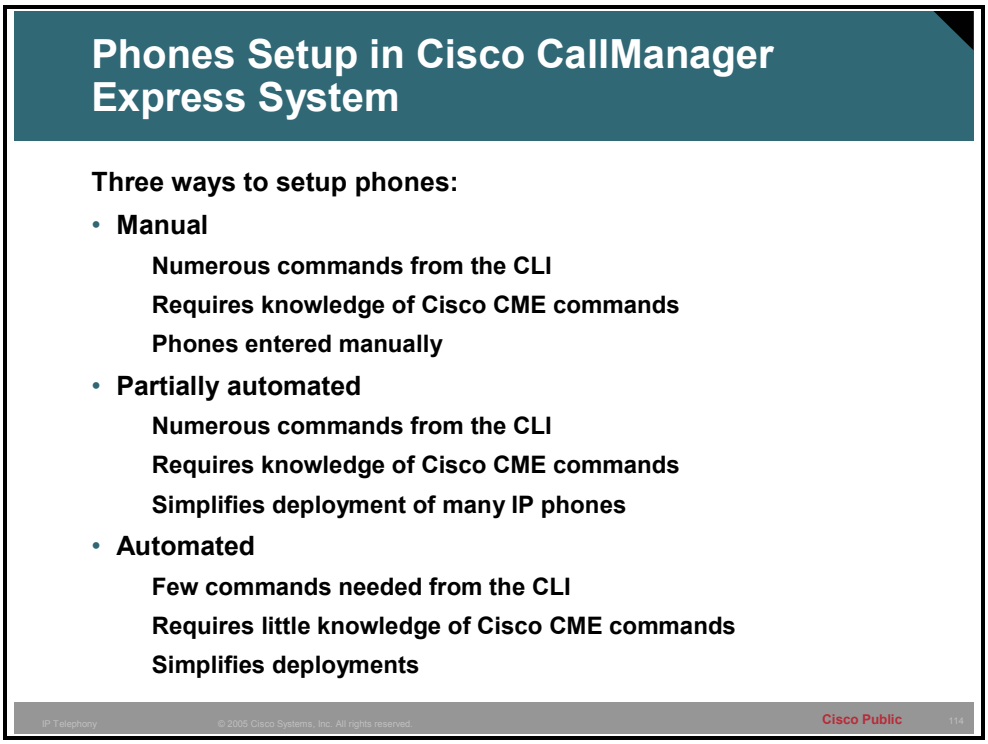
A sample file for creating a customer administrator with a limited subset of administrative privileges is included in the bundle or can be downloaded in an individual file that contains the basic files. This file can be customized and stored in flash memory for use. This topic is covered in more detail in a later module.

 Copyright © 2005, Cisco Systems, Inc.

Initial Phone Setup

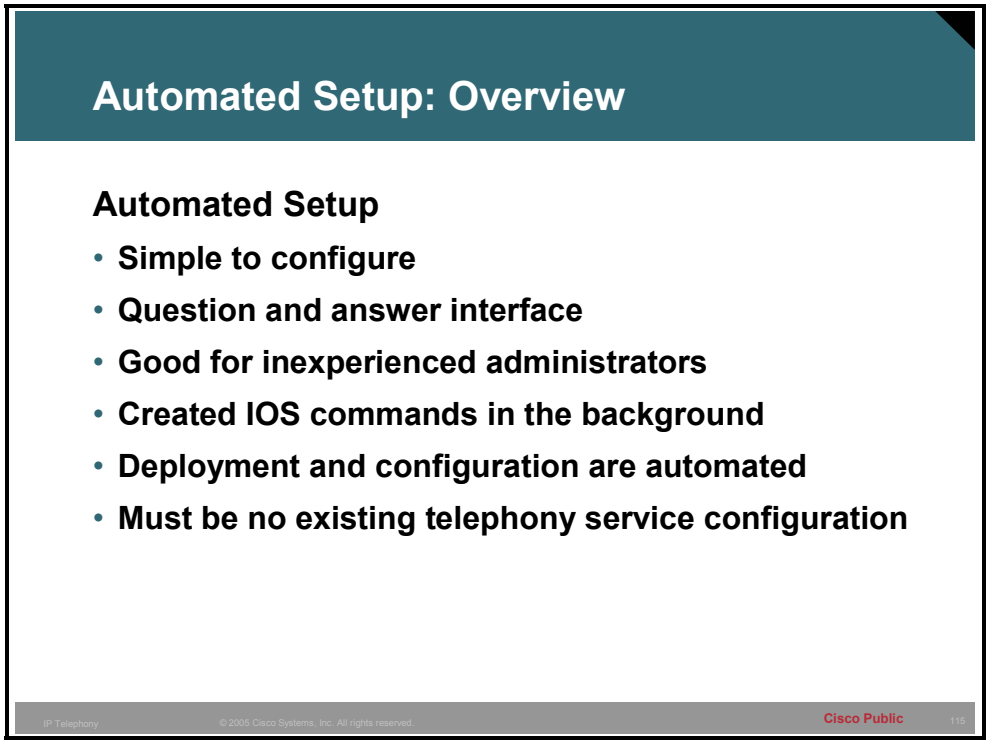
Setting Up Phones in a CME System

This topic describes the three ways to create an initial phone setup in a Cisco CME system.



Automated Phone Setup

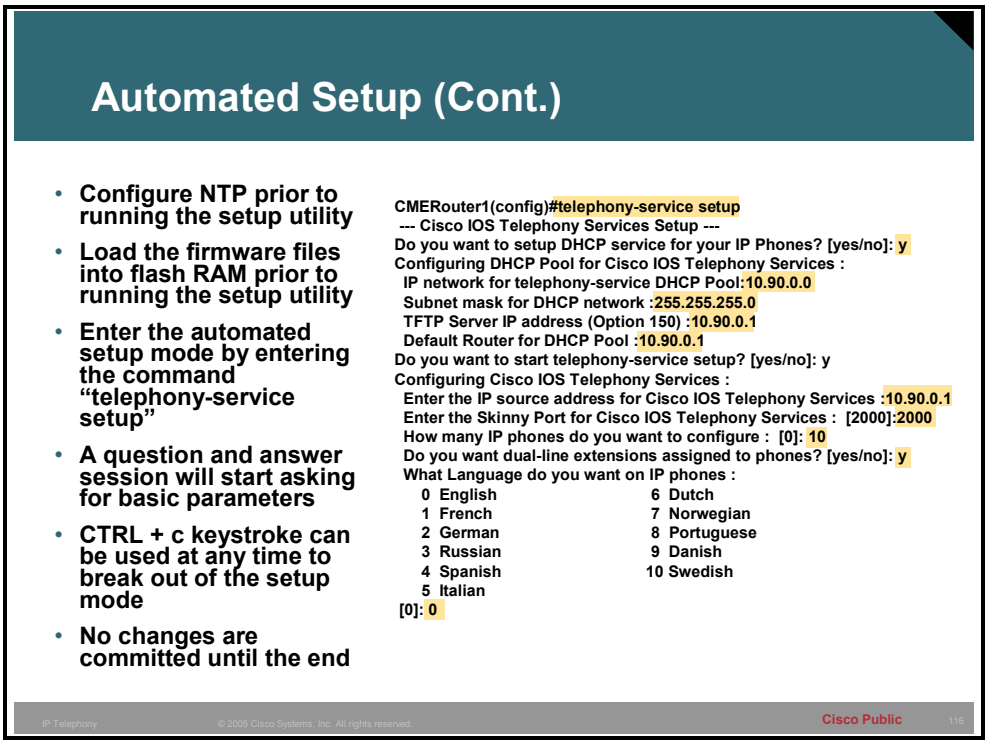
This topic describes how to perform ann automated phone setup in a Cisco CME system using the setup tool.



The automated setup is designed for the administrator that does not have a lot of experience with Cisco IOS and may not feel comfortable manually configuring the Cisco CME system. A question-and-answer interface will start and all the administrator does is answer the questions appropriately.

Note	Any existing configuration of the telephony-service in Cisco CME must be removed prior to starting the setup.

 Copyright © 2005, Cisco Systems, Inc.



The Cisco CME setup tool provides a question-and-answer interface that allows you to set up an entire Cisco CME system at one time. The Cisco CME setup tool is started using the **telephony-service setup** command. If you do not use the **setup** keyword, you can set up phones one at a time using router CLI. The **setup** keyword is not stored in the router NVRAM. When using the Cisco CME setup tool, you provide information in response to a series of questions.

Note	If you attempt to use the setup option for a system that has a nonempty telephony-service configuration, an error message advises you to remove the existing configuration first by using the **no telephony-service** command.

Prior to running the automated setup utility please configure the Cisco CME router with Network Time Protocol (NTP) and load the appropriate firmware files into flash RAM on the Cisco CME router.

The actual configuration is created only when the entire dialog has been completed. You can interrupt the process using **Control-c** at any point prior to the final question without having any configuration occur.

The first question asked by the automated setup deals with DHCP and whether the Cisco CME router is going to be providing this service. If "y" is entered the parameters of the DHCP scope need to be entered when the setup prompts ask. The name of the scope that will be created as a result of the setup is "ITS."

The second section of the automated setup configures the telephony service. The setup asks if the telephony service should be started and if "y" is selected the IP address and port that Cisco CME runs on will need to be entered when the setup prompts. The IP address entered should be

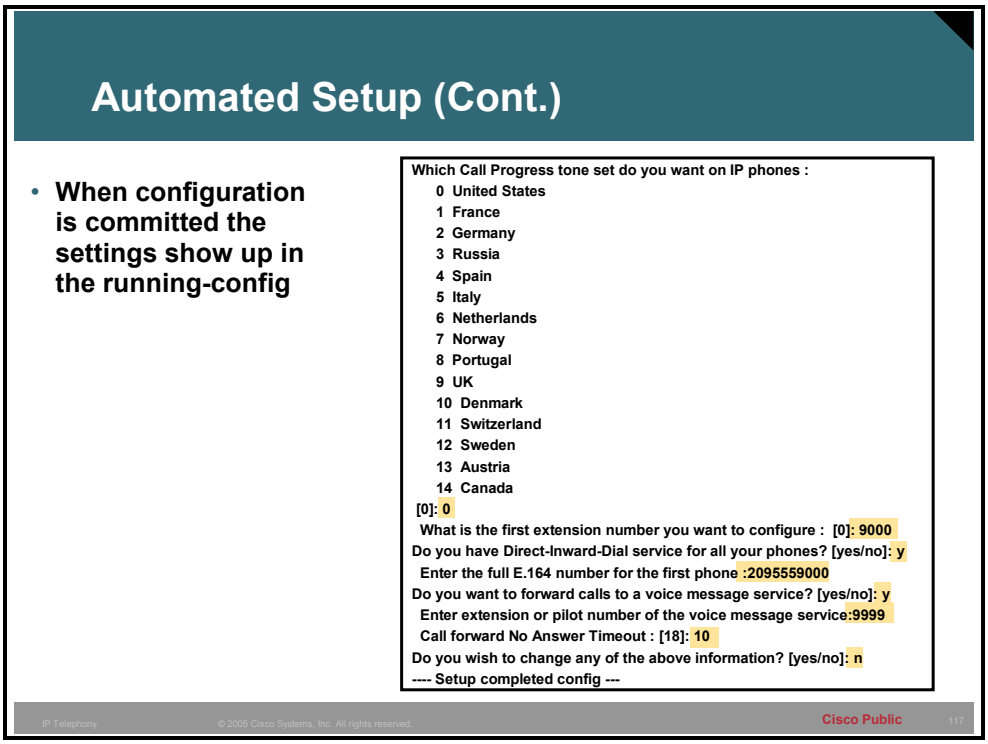
the address on the LAN that is local to the IP phones. This is the address that the phones will use to register to. The port should in most cases be left to the default port of 2000.

The next question is how many phones you want to configure. Select no more than the licensed amount. If a number is selected that is less than the licensed amount, more ephones can be added later manually.

The next question asks if dual lines are desired, if “y” is selected the phones will be configured like PBX phones, if “n” is selected the phones will be configured similar to a key switch phone.

The next question deals with the language of the phones and configures the locale that will be used on the IP phone display. This when the configuration is committed will configure the SCCP-dictionary.xml and the *phonemode*l-dictionary.xml files.

 Copyright © 2005, Cisco Systems, Inc.



The next part of the automated setup configures the call progress tones on the IP phones. The call progress tones are the sounds heard by a caller. These would include things like dial tone, busy signal, ringback and reorder signal. These call progress tones vary from country to country and should be set according to what the users are used to hearing.

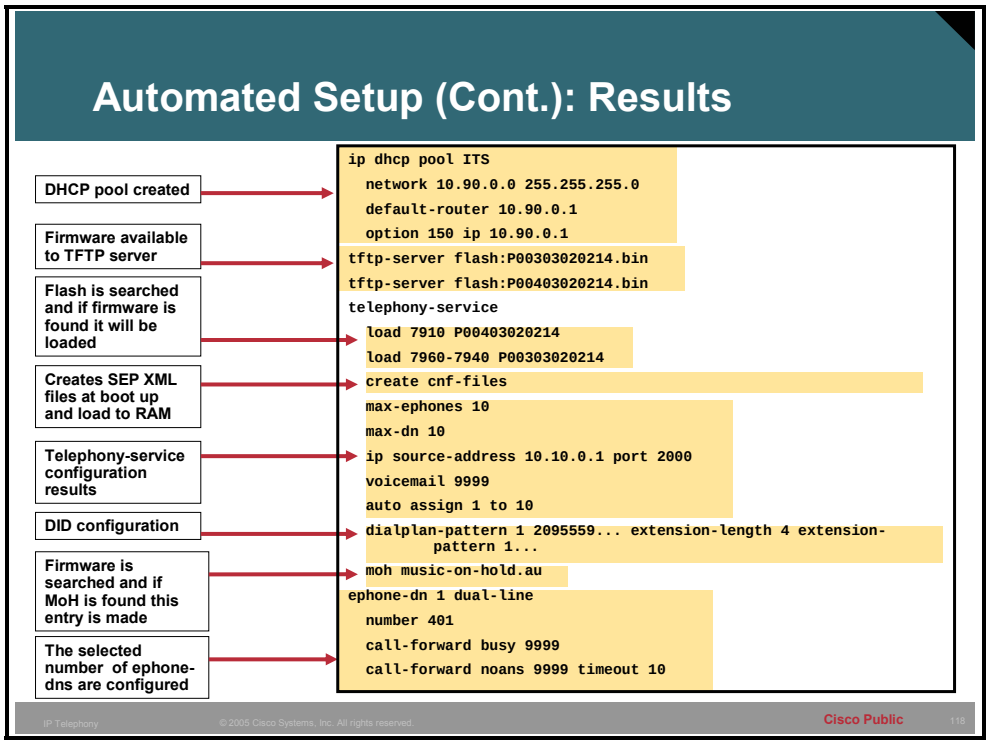
To continue the automated setup enter the Directory Number (DN) that will be the start of the DNs that will be assigned, they will be assigned in a sequential fashion.

If Direct Inward Dial (DID) needs to be setup enter “yes” when prompted. DIDs are used when the connection to the PSTN is able to pass the dialed number. In order for this to happen the connection will typically be an ISDN connection. If the connections are FXO then a Private Line Auto Ringdown (PLAR) on the analog trunk will need to be set up instead, this will have to be done manually and is not a part of the automated setup. Setting up DIDs can be very simple especially if there is relationship between the PSTN number and the internal DN. (Example 209-555-9009 maps to 1009). If there is no common relationship between the PSTN number and internal DN then manual settings will need to be made outside of the automated setup (Example 209-555-9009 maps to 7691).

The next question asks if the calls should be forwarded to a voice message service. Assuming that there is a voice mail system the pilot point number will need to be entered. This sets the “forward no answer” and the “forward busy” for all of the phones created to the pilot point number. The timeout value for the “forward no answer” will also need to be set, 18 seconds is the default. This value is in seconds not rings as rings may vary in length up to 2 seconds.

The final question asks if any of the information that was entered needs to be changed. If “y” is entered the setup starts over, if “n” is entered the changes are committed to the running-config.

After finishing the automated configuration the configuration has not been saved to the startup configuration. Use the **copy running-config startup-config** command to save the configuration.



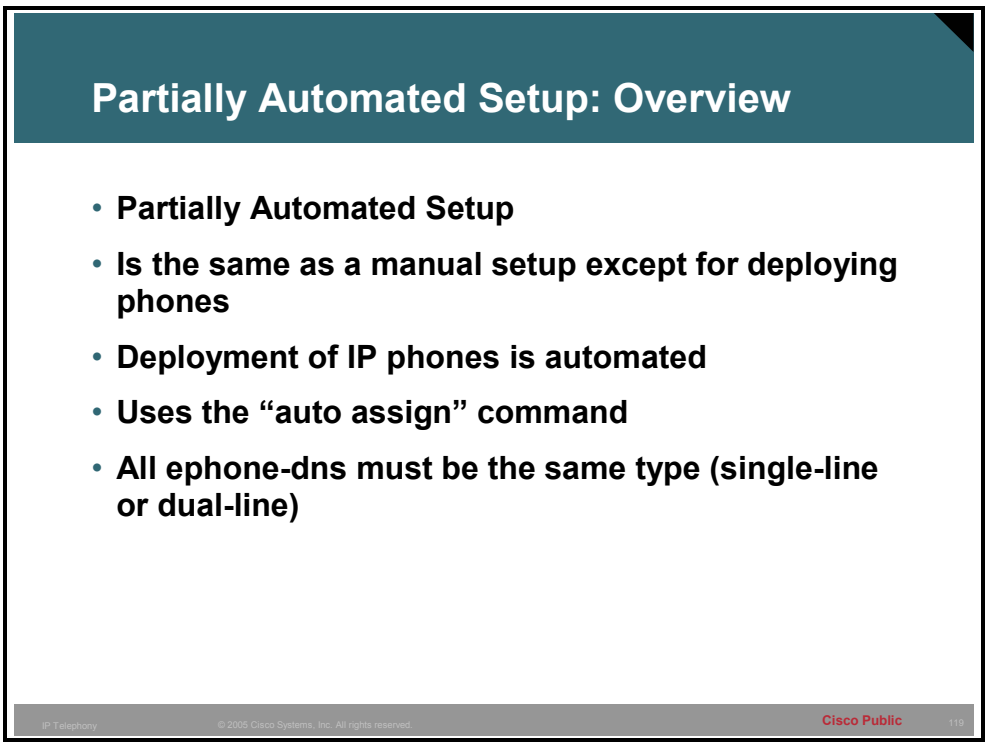
This shows the results of the automated setup.

Note	ITS is the initial name of what is now called Cisco CME, and still appears in some of the configuration that is created with the automated setup.

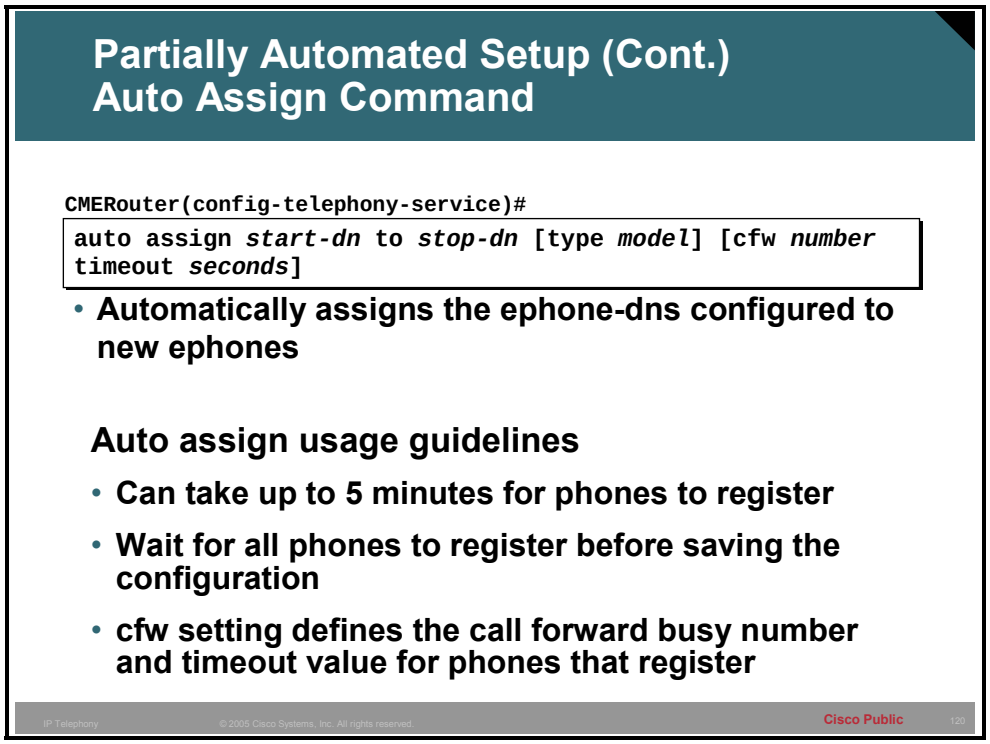
 Copyright © 2005, Cisco Systems, Inc.

Partially Automated Phone Setup

This topic describes how to perform a partially automated phone setup in a Cisco CME system using the router CLI.



The partially automated setup is exactly like a manual setup, without having to configure ephones. The ephones can be detected automatically and assigned an ephone-dn from a range of configured ephone-dns. This allows for the deployment of many phones without the work of configuring every phone manually. This automatic assignment is done through the use of the **auto assign** command.



To automatically assign ephone-dn tags to Cisco IP phones as they register for service with the Cisco CME router, use the **auto assign** command in telephony-service configuration mode.

This command lets you assign ranges of ephone-dn tags according to the physical phone type. Multiple **auto assign** commands can be used to provide discontinuous ranges and to support multiple types of IP phones. Overlapping ephone-dn ranges may be assigned so that they map to more than one type of phone. If no type is specified, the values in the range are assigned to phones of any type, but if a specific range is assigned for a phone type, the available ephone-dns in that range are used first. The **cfw** keyword sets the call forward busy number and timeout value on all phones that auto register.

The **auto assign** command cannot be used for the Cisco IP Phone 7914 Expansion Module. Phones with one or more expansion modules must be configured manually.

Automatically assigned ephone-dn tags must belong to normal ephone-dns and cannot belong to paging ephone-dns, intercom ephone-dns, music-on-hold (MOH) ephone-dns, or message-waiting-indication (MWI) ephone-dns. The ephone-dn tags that are automatically assigned must have at least a primary number defined.

All the ephone-dns in a single automatic assignment set must be of the same kind (either single-line or dual-line). Automatic assignment cannot create shared lines.

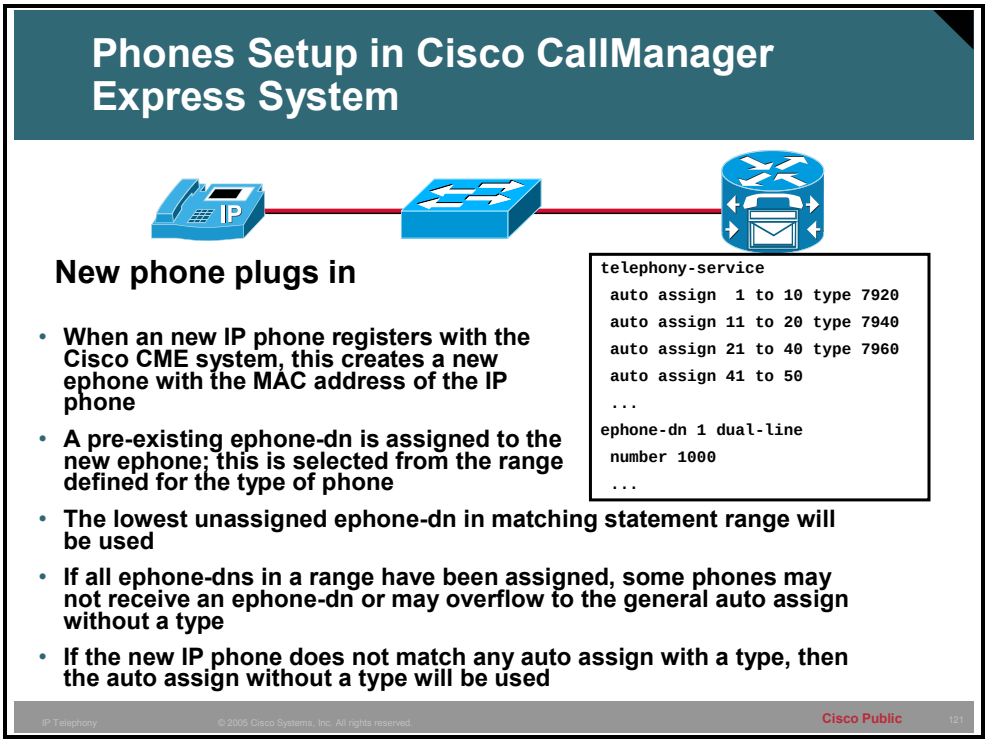
If an insufficient number of ephone-dns are available in the automatic assignment set, some phones will not receive ephone-dns.

Reversal or undoing of automatic assignment must be performed by manual command-line interface (CLI) entry. This command must be followed by a reboot of the phones that are assigned. If you use the **type** keyword with this command, use the **reset** command to reboot the phones. If you do not use the **type** keyword with this command, use the **restart** command to perform a quick reboot.

 Copyright © 2005, Cisco Systems, Inc.

Note	Care should be taken when using the **auto assign** command because this command grants telephony service to any IP phone that attempts to register. If you use the **auto assign** configuration option, make sure that your network is secure from unauthorized access by unknown IP phones.

Example: Phone Setup in Cisco CME System

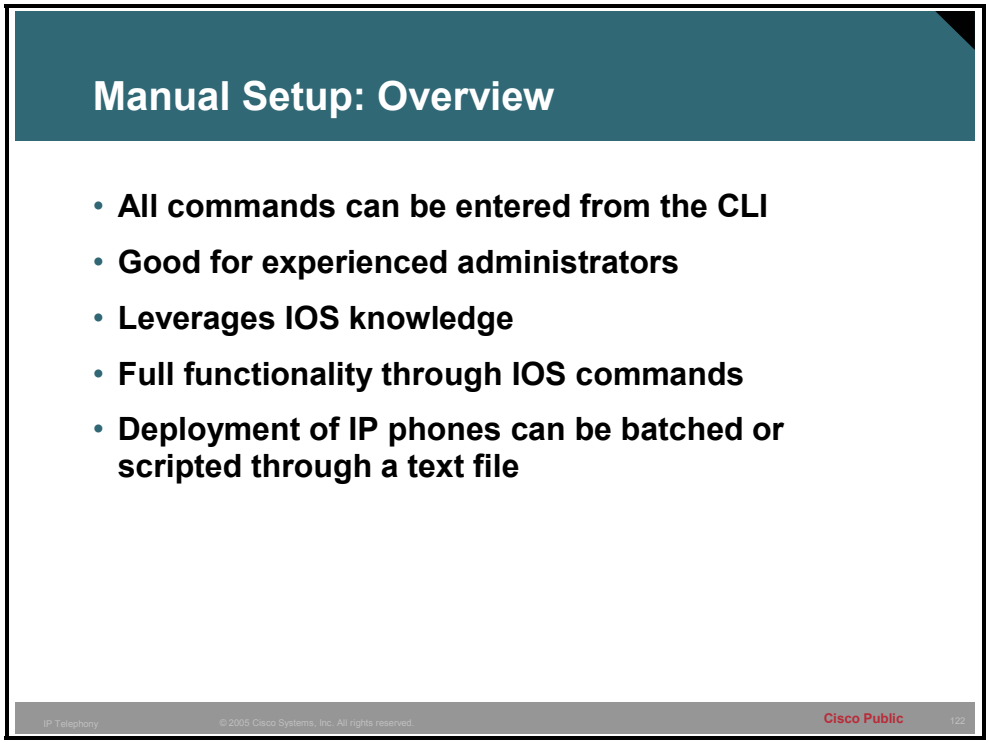


In this example there are four **auto assign** commands with different ephone-dn assigned to each. Any 7920 IP phones will be assigned the lowest unassigned ephone-dn between 1 and 10. 7940s will be assigned the lowest unassigned ephone-dn between 11 and 20. Any 7960s will be assigned the lowest unassigned ephone-dn between 21 and 40. Finally, the phone can get an ephone-dn assigned to it from the generic range 41 to 50 in this example if any 7920s, 7940s, or 7960s cannot be assigned an ephone-dn in their assigned range because they are all assigned. This generic range that is not tied to any type will also be used for any other non specified models of IP phones.

Note	When all desired IP phones are have been auto assigned make sure to save the configuration.

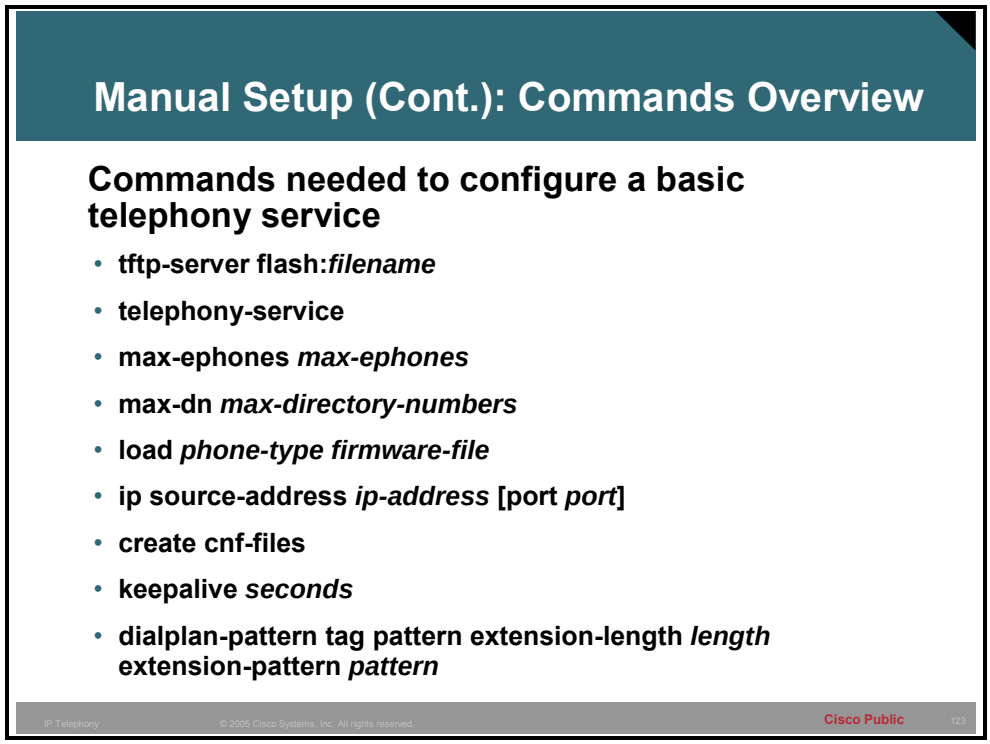
Manual Phone Setup

This topic describes how to perform a manual phone setup in a Cisco CME system using the router CLI.



The manual setup of the Cisco CME system involves using the CLI environment. This allows the administrator to leverage existing knowledge of IOS and implement any of the Cisco CME functions. The configuration can be viewed, backed up and restore through a simple text file. This can also be used for multiple site deployments allowing just the differences to be changed on a per site basis, there by saving time and effort.

 Copyright © 2005, Cisco Systems, Inc.



The following commands will need to be configured to deploy a Cisco CME system.

tftp-server flash:*filename*

telephony-service

max-ephones *max-ephones*

max-dn *max-directory-numbers*

load *phone-type firmware-file*

ip source-address *ip-address* [port *port*]

create cnf-files

keepalive *seconds*

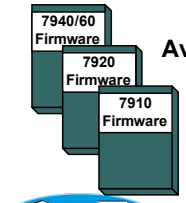
dialplan-pattern *tag pattern* extension-length *length* extension-pattern *pattern*

In the addition to these commands, ephones and ephone-dns will need to be manually configured. These topics were discussed in a previous lesson.

Manual Setup (Cont.): tftp-server Command

```
CMERouter(config)#
tftp-server flash:filename
```

- **Allows a file in flash to be downloadable with TFTP**



Available through TFTP

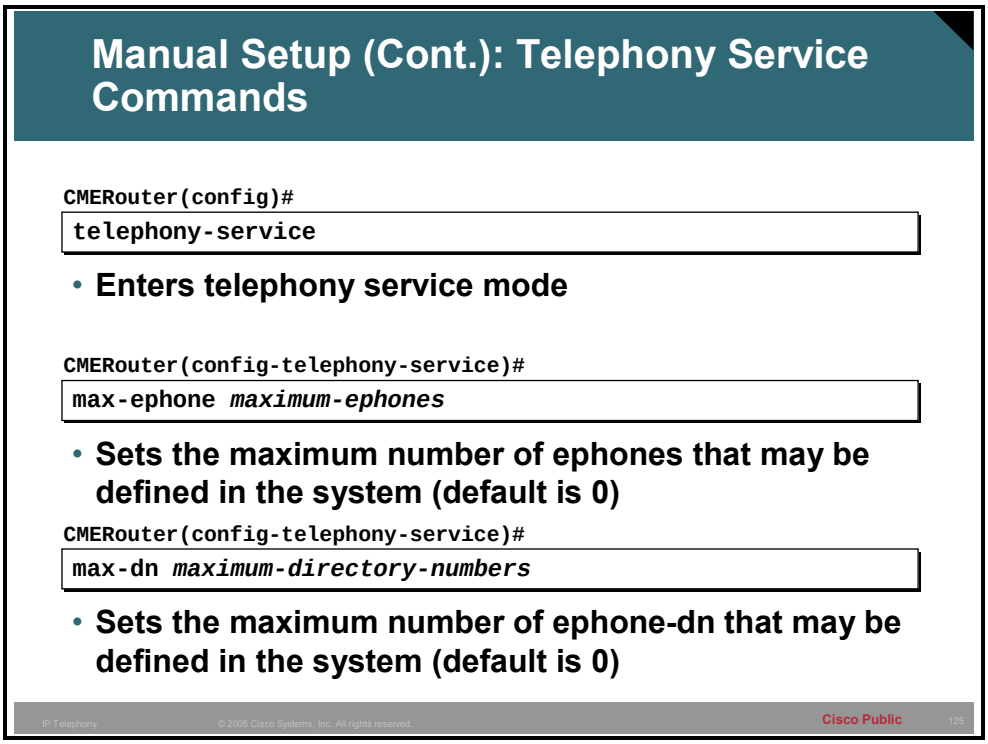


```
tftp-server flash:P00303020214.bin
tftp-server flash:cmterm_7920.3.3-01-06.bin
tftp-server flash:P00403020214.bin
```

IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 124

The command **tftp-server flash:*filename*** allows the file specified that resides in flash to be downloaded via TFTP. In Cisco CME the firmware files need to be configured to be available through TFTP. The example above shares firmware for the 7910, 7940-7960, and the 7920 IP phones.

 Copyright © 2005, Cisco Systems, Inc.



The command **telephony-service** enters the telephony service mode where much of the configuration of the Cisco CME system is entered. Two of the first commands that will want to be entered are the **max-dn** and **max-ephone**. Both of these commands are set to 0 which has the affect of not allowing any ephones or ephone-dns to be configured.

The number of ephones and ephone-dns is version and platform specific. The number displayed in the IOS help is not always accurate and may reflect an artificially high number. Consult the information provided with the CallManager router or cisco.com website.

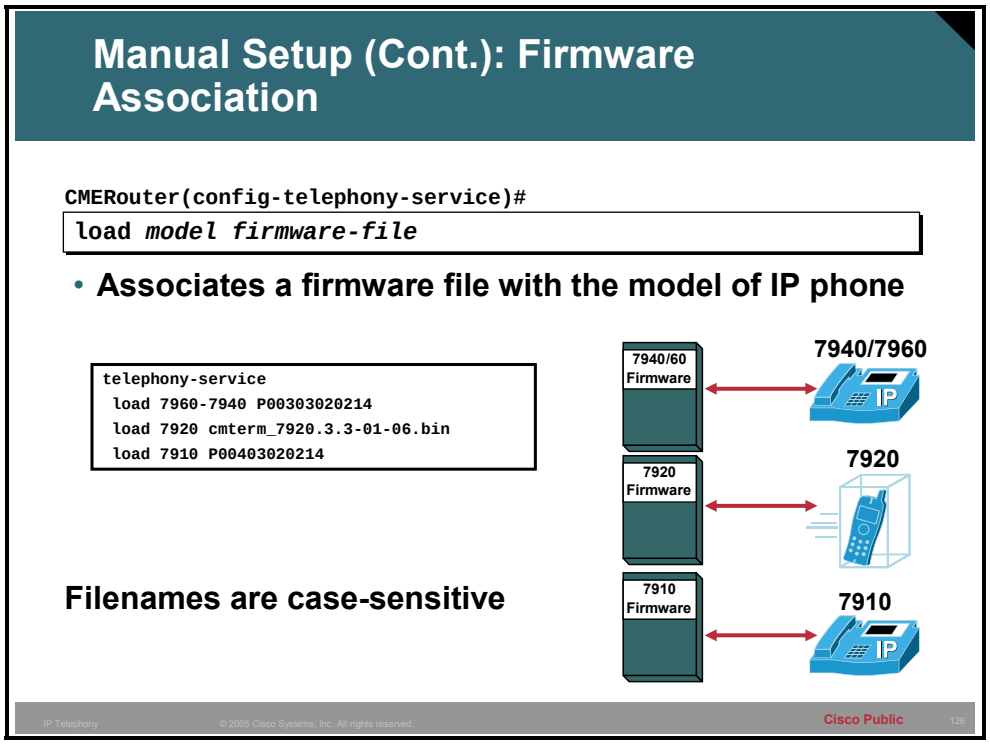
Example

CMERouter1(config-telephony)#**max-dn ?**

<1-288> Maximum directory numbers supported

CMERouter1(config-telephony)#**max-ephone ?**

<1-100> Maximum phones to support



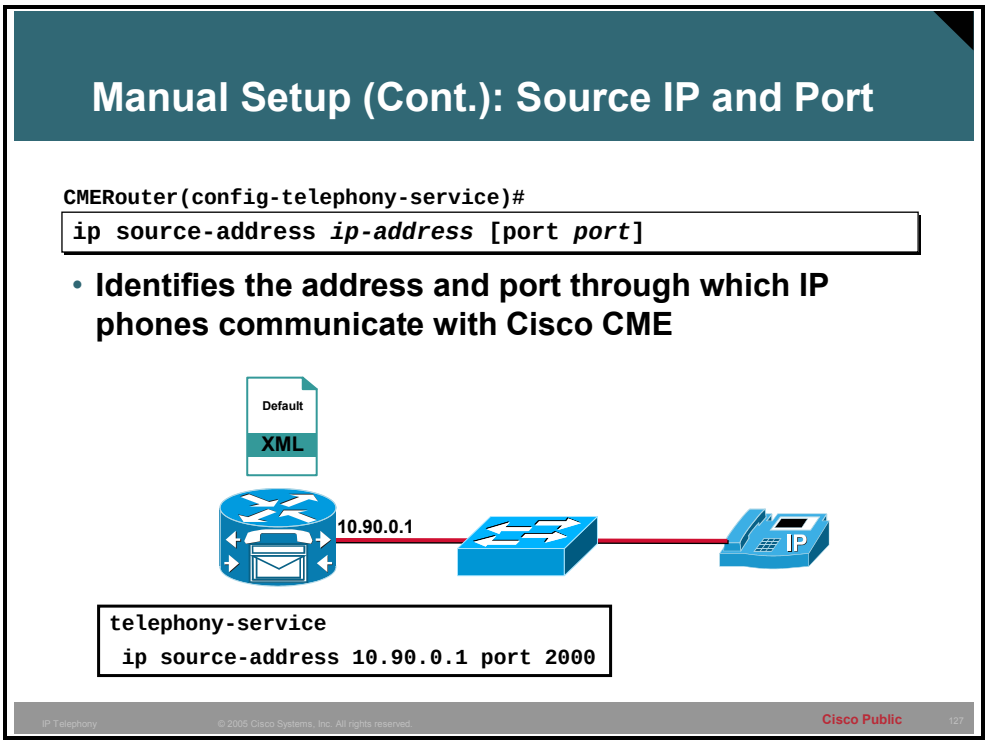
To associate a type of Cisco IP phone with a phone firmware file, use the **load *model firmware-file*** command in telephony-service configuration mode. The following show the supported models for which firmware can be loaded:

Note	No suffix should be used when using the load command for the 7910, 7940 and 7960 model IP phones.

CMERouter1(config-telephony)#**load ?**

7902	Select the firmware load file for 7902
7905	Select the firmware load file for 7905
7910	Select the IP phone firmware load file for Telecaster 7910 phones
7912	Select the firmware load file for 7912
7914	Select the IP phone firmware load file for sidecar 7914
7920	Select the firmware load file for 7920
7935	Select the IP phone firmware load file for 7935 Conference Station
7936	Select the firmware load file for 7936
7960-7940	Select the IP phone firmware load file for Telecaster 7960 & 7940 phones
ATA	Select the firmware load file for ATA

 Copyright © 2005, Cisco Systems, Inc.



The command **ip source *ip-address* [port *port*]** is used to configure the local IP address and TCP port where the Cisco CME system is expecting Skinny Client Control Protocol (SCCP) messages from the IP phones concerning registrations and call control. The port by default is set to 2000, while this may be changed it is unusual to do so.

Example

This is an example of the XMLDefault.cnf.xml file. Note the IP address, port and firmware files.

<Default>

<callManagerGroup>

<members>

<member priority="0">

<callManager>

<ports>

<ethernetPhonePort>2000</ethernetPhonePort>

</ports>

<processNodeName>10.90.0.1</processNodeName>

</callManager>

</member>

</members>

</callManagerGroup>

<loadInformation6 model="IP Phone 7910">P00403020214</loadInformation6>

<loadInformation124 model="Addon 7914"></loadInformation124>

<loadInformation9 model="IP Phone 7935"></loadInformation9>

<loadInformation8 model="IP Phone 7940">P00303020214</loadInformation8>

<loadInformation7 model="IP Phone 7960">P00303020214</loadInformation7>

<loadInformation20000 model="IP Phone 7905"></loadInformation20000>

<loadInformation30008 model="IP Phone 7902"></loadInformation30008>

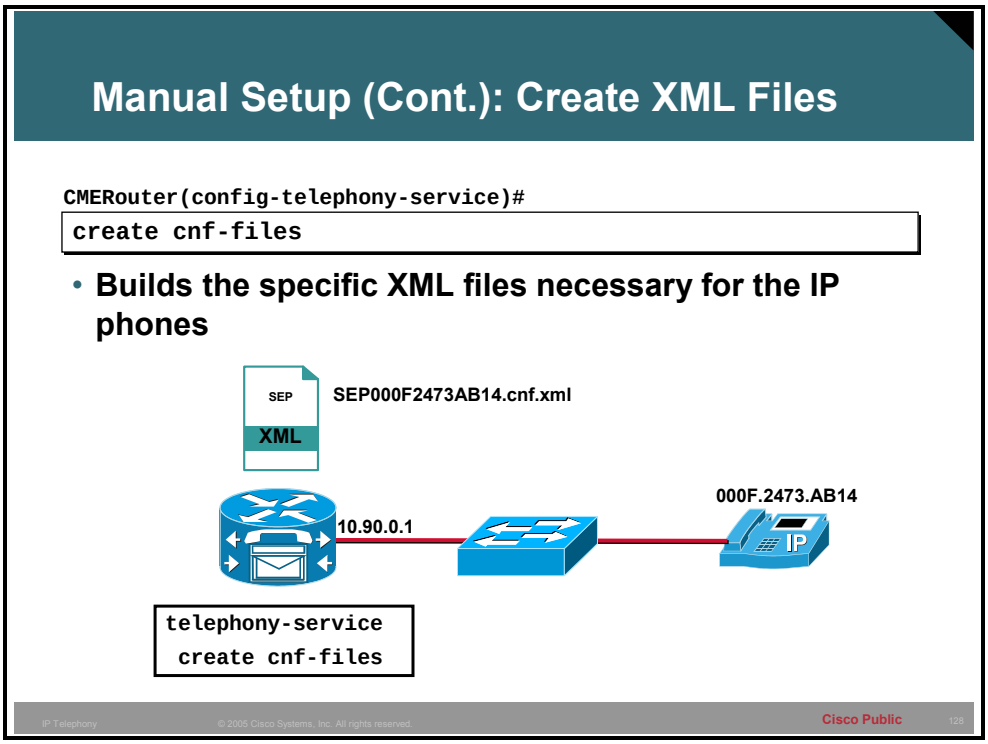
<loadInformation30002 model="IP Phone 7920">cmterm_7920.3.3-01-06.bin</loadInformation30002>

<loadInformation30019 model="IP Phone 7936"></loadInformation30019>

<loadInformation30007 model="IP Phone 7912"></loadInformation30007>

</Default>

 Copyright © 2005, Cisco Systems, Inc.



To build the XML configuration files that are required for IP phones used with Cisco CME 3.1, or later versions, use the **create cnf-files** command in telephony-service configuration mode.

When this command is entered the file XMLDefault.cnf.xml is generated with that appropriate settings including the firmware defined by the **load** command, the IP address for new IP phones to register to and the TCP port those messages will arrive on.

Example

This is an example of SEP000F2473AB14.cnf.xml. Note the IP address, port, locale information and firmware required.

<device>

<devicePool>

<callManagerGroup>

<members>

<member priority="0">

<callManager>

<ports>

<ethernetPhonePort>2000</ethernetPhonePort>

</ports>

<processNodeName>10.90.0.1</processNodeName>

</callManager>

</member>

</members>

</callManagerGroup>

</devicePool>

<versionStamp>{Jan 01 2002 00:00:00}</versionStamp>

<loadInformation>P00303020214</loadInformation>

- <userLocale>

<name>English_United_States</name>

<langCode>en</langCode>

</userLocale>

<networkLocale>United_States</networkLocale>

<idleTimeout>0</idleTimeout>

<authenticationURL />

<directoryURL>http://10.90.0.1/localdirectory</directoryURL>

<idleURL />

<informationURL />

<messagesURL />

<proxyServerURL />

<servicesURL />

</device>

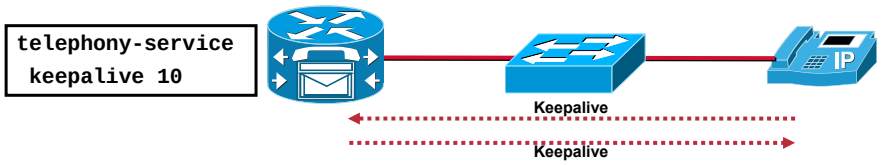
 Copyright © 2005, Cisco Systems, Inc.

Manual Setup (Cont.)
Keepalive

Cisco.com

```
CMERouter(config-telephony-service)#
keepalive seconds
```

- **Sets the length of the time interval between keepalive message from the IP phones to Cisco CME**



- **Default is 30 seconds, range is 10 – 65535 seconds**
- **If 3 keepalives are missed in a row, the device will have to register again**

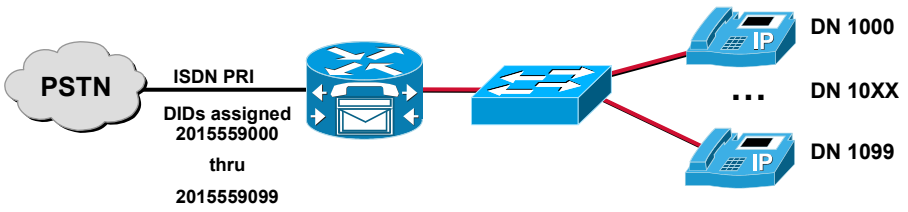
© 2004 Cisco Systems, Inc. All rights reserved.

To set the length of the time interval between successive keepalive messages from the Cisco CME router to IP phones, use the **keepalive** command in telephony-service configuration mode. The default setting for the keepalives is 30 seconds and if the router fails to receive three successive keepalive messages, it considers the phone to be out of service until the phone reregisters.

Manual Setup (Cont.): DID Configuration Commands

```
CMERouter(config-telephony-service)#
dialplan-pattern tag pattern extension-length length
extension-pattern pattern [no-reg]
```

- **Sets a dial plan pattern which can expand extension numbers to E.164 numbers that can be used for DIDs**




```
telephony-service
 dialplay-pattern 1 20155590.. extension-length 4 extension pattern 10..
```

IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 131

To create a global prefix that can be used to expand abbreviated extension numbers in a Cisco CME system into fully qualified E.164 numbers, use the **dialplan-pattern** command in telephony-service configuration mode.

Directory numbers for the Cisco IP phones are entered in extension-number format. The **dialplan-pattern** command creates a global prefix that can be used to expand the abbreviated extension numbers into fully qualified E.164 numbers. The dial-plan pattern is also required in order to register Cisco IP phone lines with a gatekeeper. The **dialplan-pattern** command can resolve an incoming call with a full E.164 number to a Cisco IP phone extension number.

The **extension-length** keyword enables the system to convert a full E.164 telephone number back into an extension number for the purposes of caller ID display and received-call and missed-call lists. For example, a company uses extension number range 100 to 199 across several sites, with only the extensions from 1000 to 1099 present on the local router. An incoming call from 1044 arrives from the company's internal VoIP H.323 network, and this call includes the calling number as 4085550144 in its full E.164 format.

By default the numbers matching the **dialplan-pattern** command will be registered to a H.323 Gatekeeper if a gatekeeper is configured. The use of the **no-reg** keyword will change this default behavior and prevent the numbers matching the pattern from registering with the Gatekeeper.

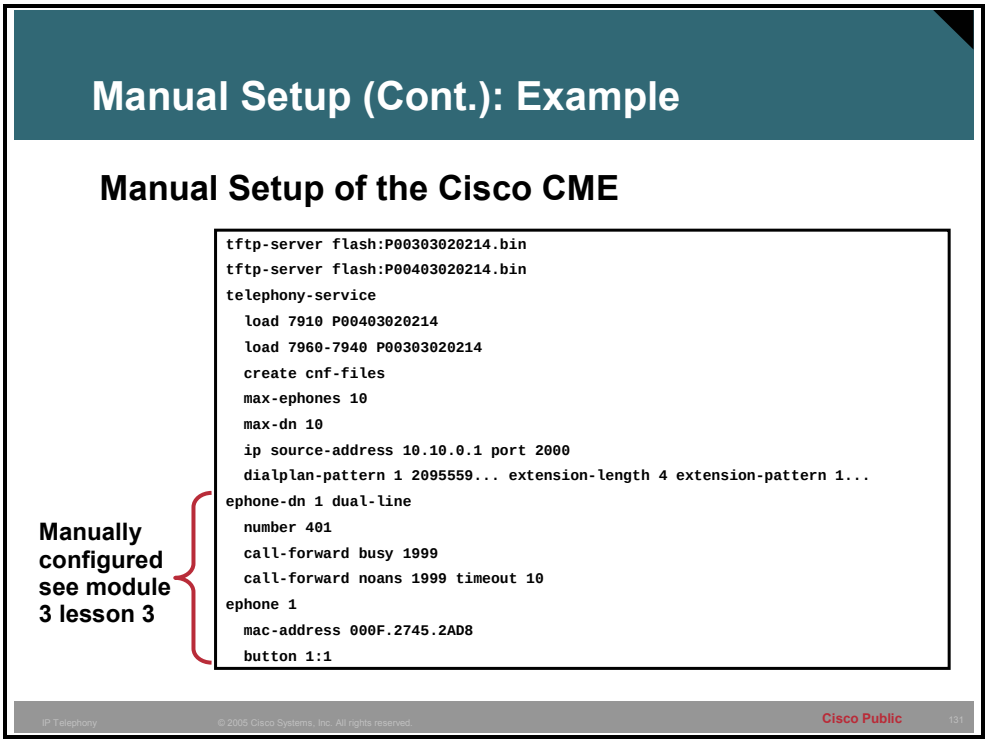
When the called number matches the dial-plan pattern, the call is considered a local call and has a distinctive ring that identifies the call as internal. Any call that does not match the dial-plan pattern is considered an external call and has a ring different from the internal ring. The valid dial-plan pattern with the lowest dial-plan-tag number is used as a prefix to all local Cisco IP phones.

The number of *extension-pattern* characters must match the extension length that is specified in this command.

 Copyright © 2005, Cisco Systems, Inc.

Note	This command can be a replacement for configuring secondary numbers on ephone-dns.

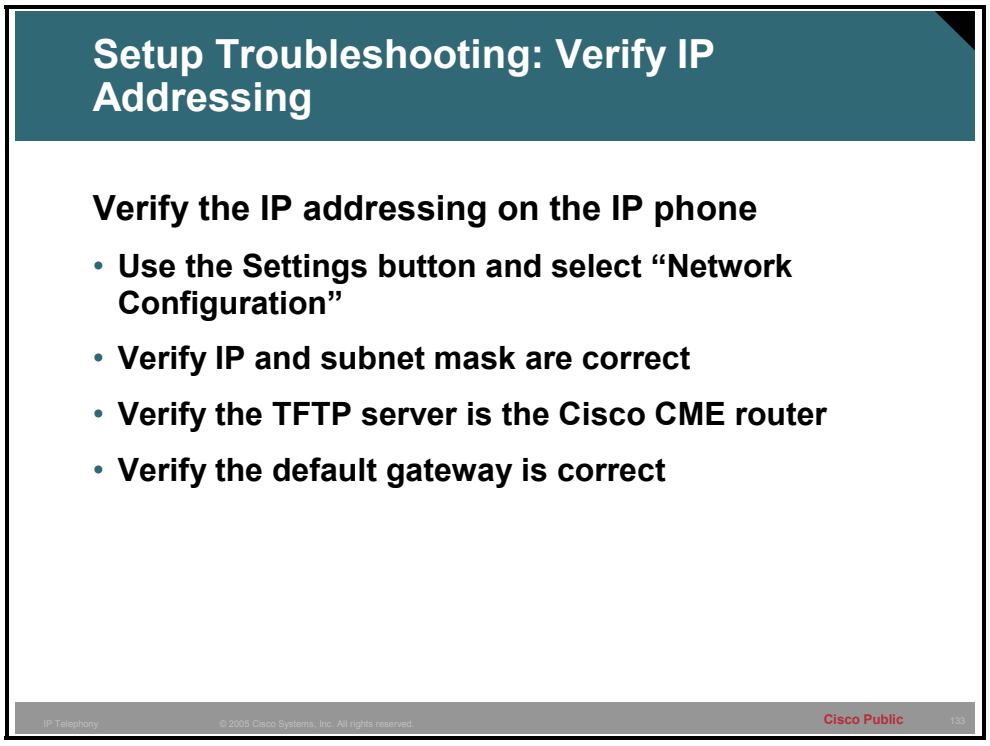
Example



This shows a sample basic Cisco CME system that has been configured.

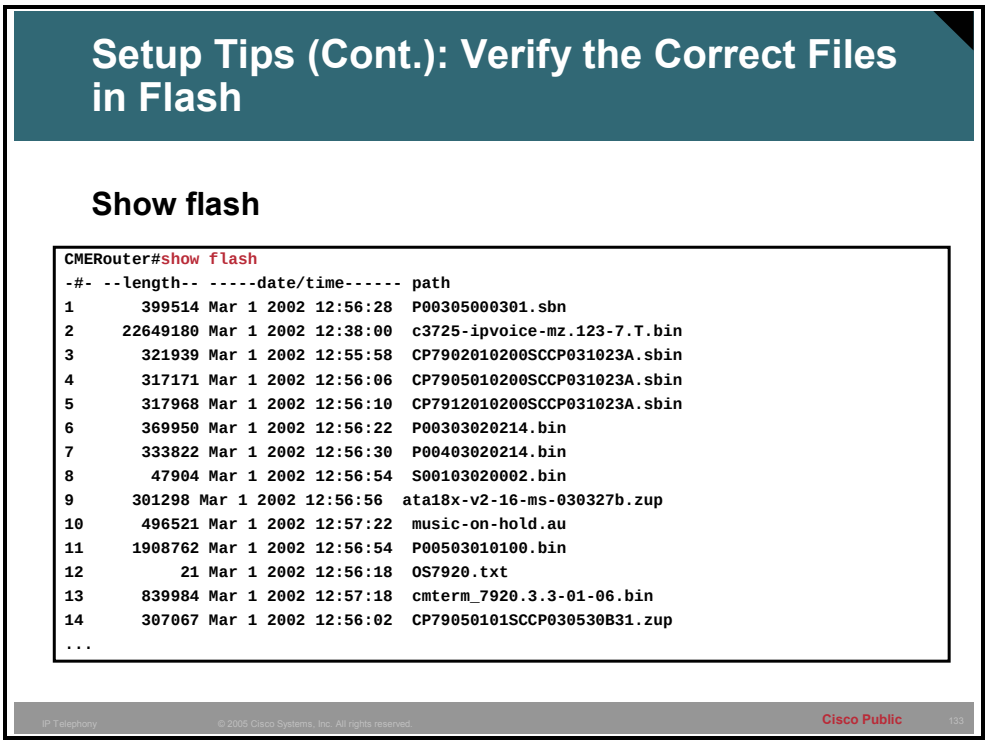
Setup Tips

This topic identifies IP phone setup troubleshooting tips.



To verify that the DHCP server is handing out the correct information to the IP phones use the “Settings” button and from the menu that appears select the “Network Configuration” settings. Scroll through the settings and verify the IP address, subnet mask, default gateway and the location of the defined TFTP server. The TFTP server needs to be the Cisco CME router.

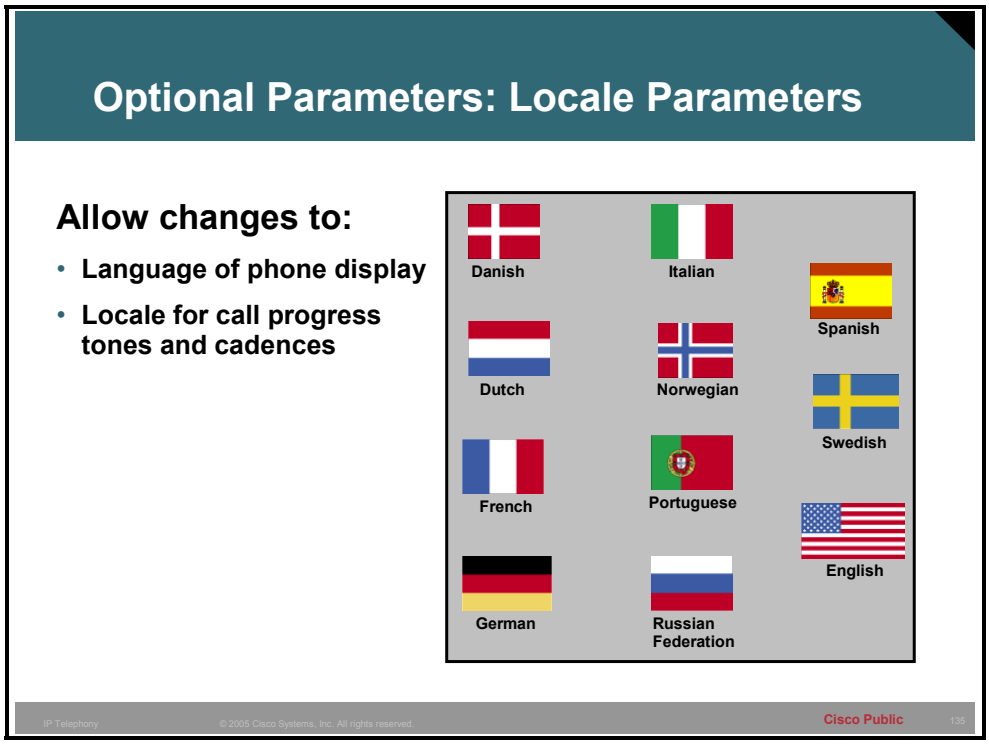
 Copyright © 2005, Cisco Systems, Inc.



The command **show flash** displays the contents of flash RAM. This needs to contain the firmware file necessary for the models of IP phones that are deployed. There may be many other files here depending on other configurations.

Optional Parameters

This topic identifies optional IP phone parameters.



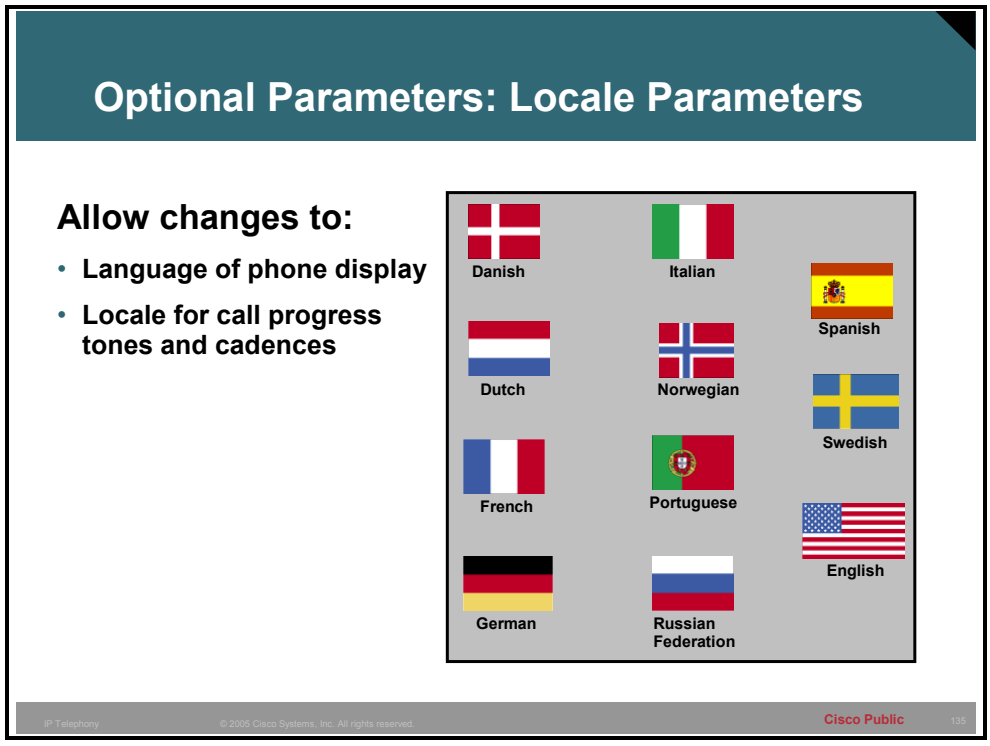
The Cisco CME system can be customized to some degree with a localized language on the IP phone, call progress indicators and cadence. This allows the user to hear and interact with the system with the language and audible queues that they are familiar with.

The format that the phone displays the date and time in can be modified to the format that is usual for the location of the installation.

 Copyright © 2005, Cisco Systems, Inc.

Router Configuration: Two Commands

This topic identifies a router configuration.

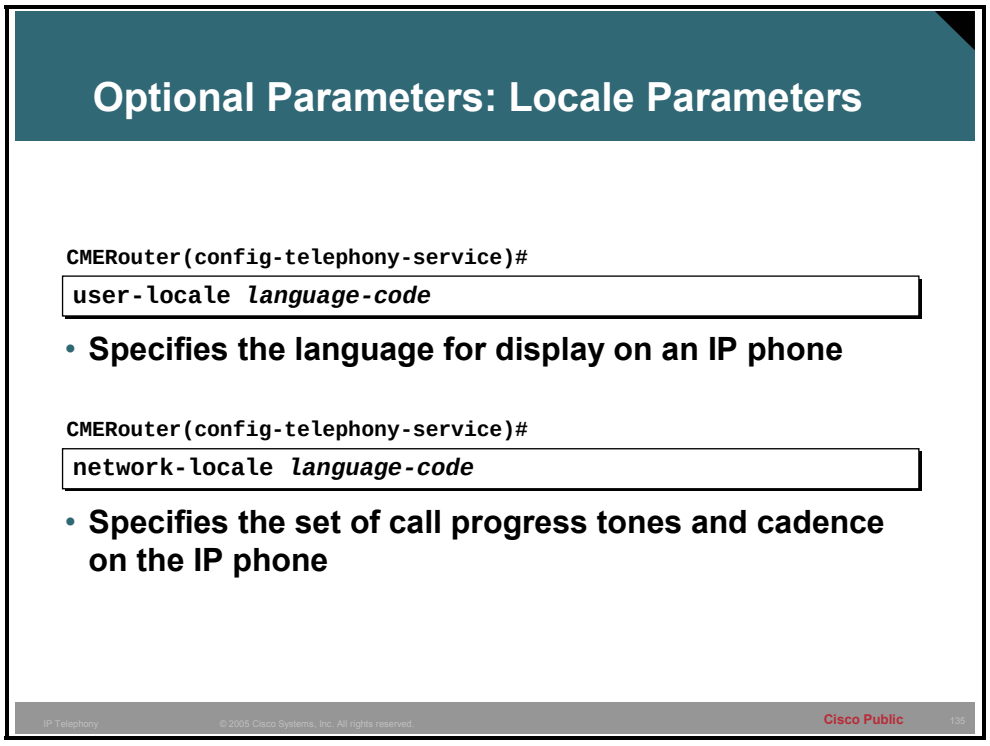


The CallManager Express system can be customized to some degree with a localized language on the IP phone, call progress indicators and cadence. This allows the user to hear and interact with the system with the language and audible queues that they are familiar with.

The format that the phone displays the date and time can be modified to the format that is usual for the location of the installation.

Optional Parameters – Locale Parameters

This topic identifies a router configuration.



On the Cisco IP Phone 7940 and Cisco IP Phone 7960, the language displayed on the phone and the locale for call progress tones and cadences can be set to one of several ISO-3166 codes that indicate specific languages and geographic regions.

Note	The 7920 IP phone supports English, French, German, and Spanish and this setting is made on the handset. The **user-locale** and **network-locale** have no effect on the 7920 IP phone.

CMERouter1(config-telephony)#**user-locale ?**

DE Germany

DK Denmark

ES Spain

FR France

IT Italy

NL Netherlands

NO Norway

PT Portugal

 Copyright © 2005, Cisco Systems, Inc.

RU Russian Federation

SE Sweden

US United States

CMERouter1(config-telephony)#**network-locale ?**

AT Austria

CA Canada

CH Switzerland

DE Germany

DK Denmark

ES Spain

FR France

GB United Kingdom

IT Italy

NL Netherlands

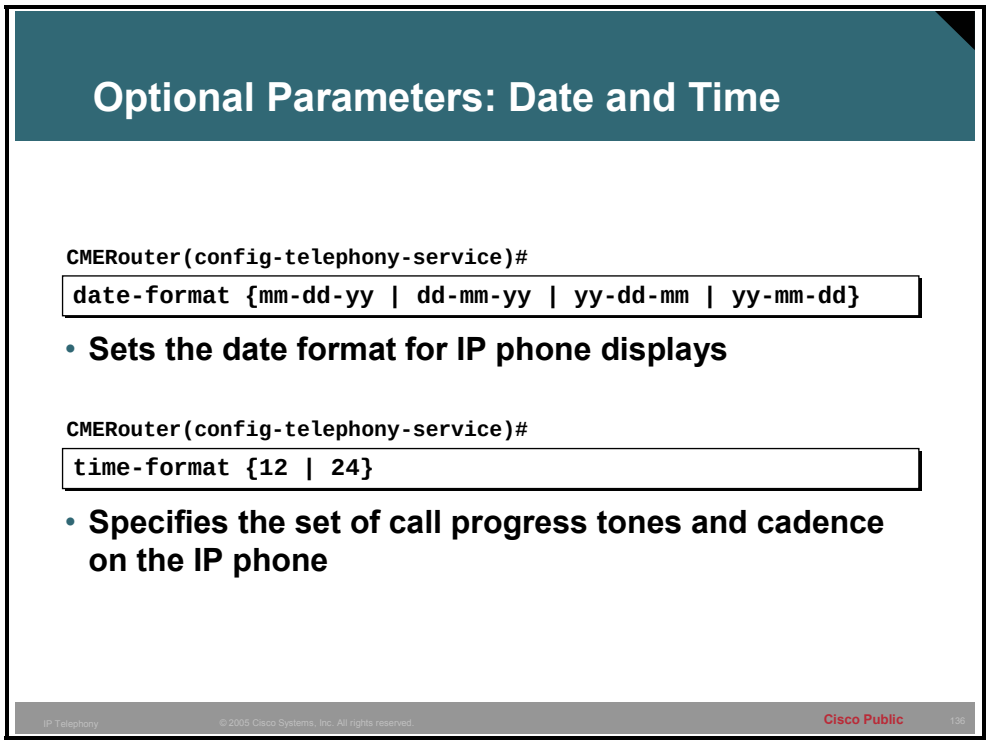
NO Norway

PT Portugal

RU Russian Federation

SE Sweden

US United States



On the Cisco IP Phone 7940 and Cisco IP Phone 7960, the date and time format can be set on a system wide basis for all IP phones.

CMERouter1(config-telephony)#**date-format ?**

dd-mm-yy Set date to dd-mm-yy format

mm-dd-yy Set date to mm-dd-yy format

yy-dd-mm Set date to yy-dd-mm format

yy-mm-dd Set date to yy-mm-dd format

CMERouter1(config-telephony)#**time-format ?**

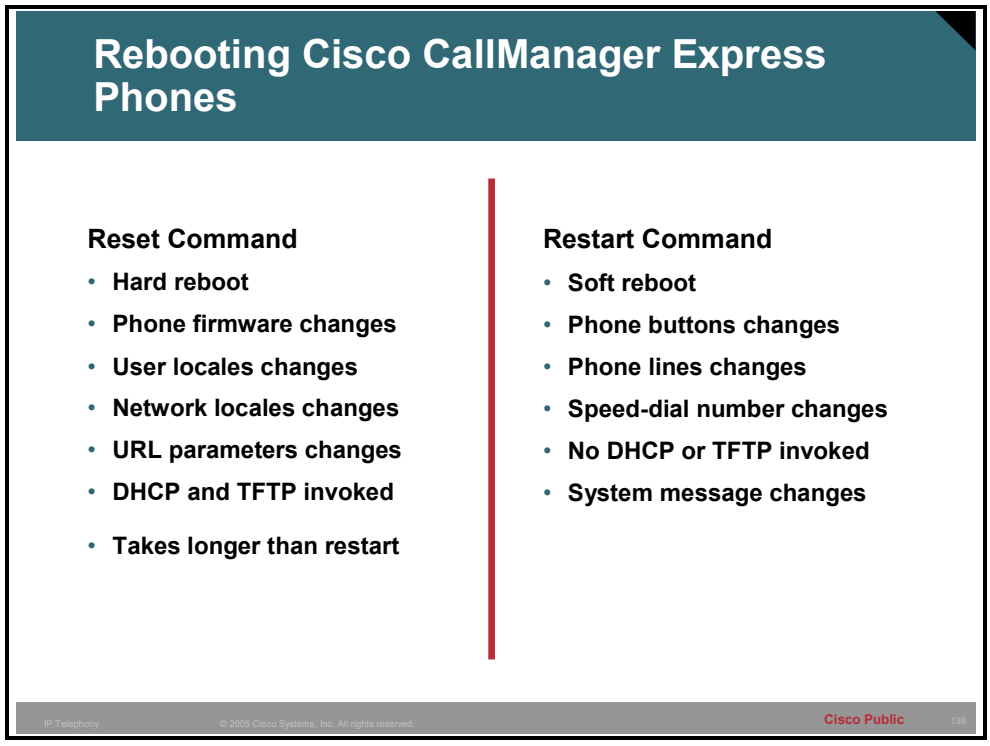
12 Set time to 12Hrs(AM/PM) format

24 Set time to 24Hrs format

 Copyright © 2005, Cisco Systems, Inc.

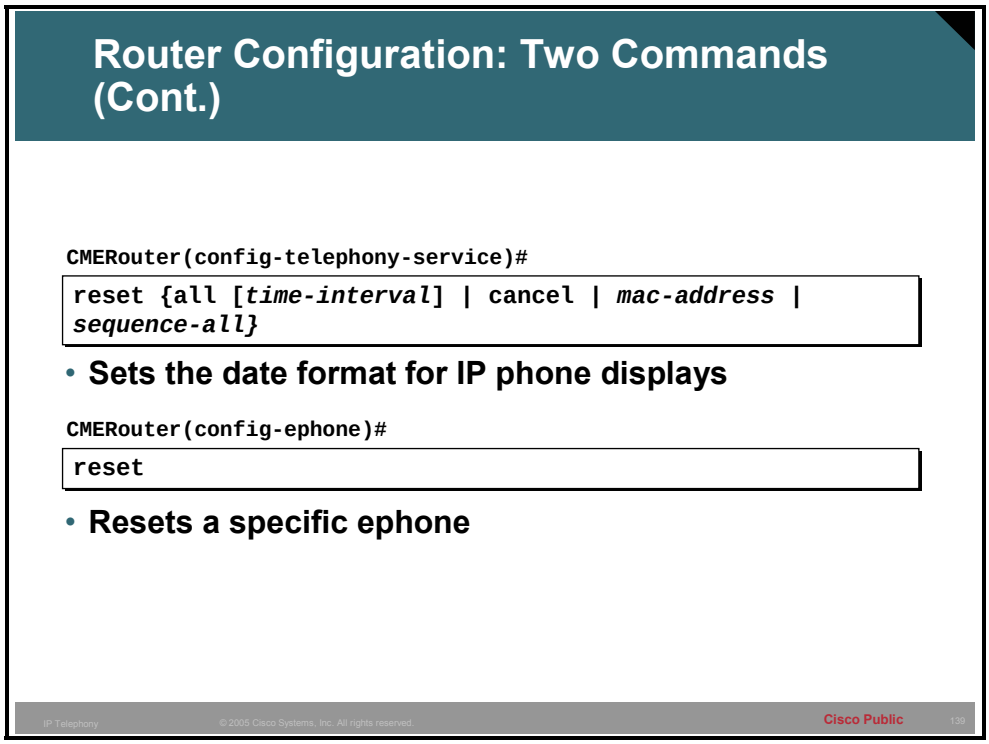
Rebooting Cisco CallManager Express Phones

This topic discusses rebooting IP phones.



After you update information for one or more phones associated with a Cisco CME router, the phone or phones must be rebooted. There are two commands to reboot the phones: **reset** and **restart**. The **reset** command performs a "hard" reboot similar to a power-off-power-on sequence. It reboots the phone and contacts the DHCP server and TFTP server to update from their information as well. The **restart** command performs a "soft" reboot by simply rebooting the phone without contacting the DHCP and TFTP servers. The **reset** command takes significantly longer to process than the **restart** command when you are updating multiple phones, but it must be used after updating phone firmware, user locale, network locale, or URL parameters. For simple button, line, or speed-dial changes, you can use the **restart** command.

Use the **reset** (ephone) command to perform a complete reboot of an IP phone when you are in ephone configuration mode. This command has the same effect as a **reset** (telephony-service) command that is used to reset a single phone.



To perform a complete reboot of one or all phones associated with a Cisco CME router, use the **reset** command in telephony-service configuration mode.

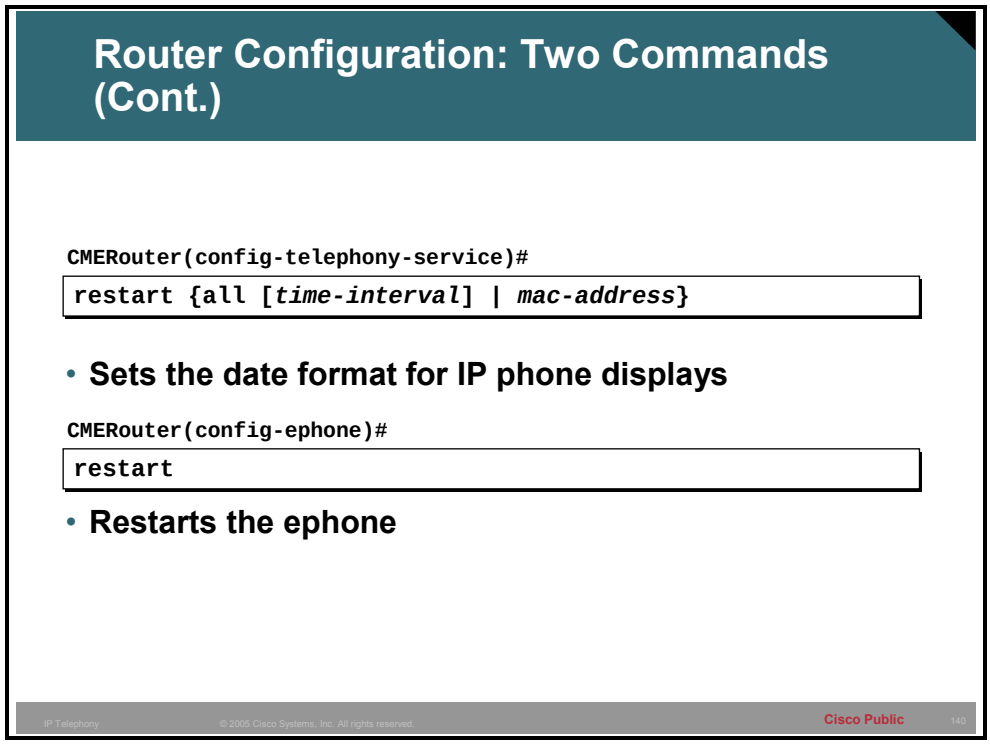
When using the **reset** command from telephony service mode, the default time interval of 15 seconds is recommended for an 8- to 10-phone office so that all the phones do not attempt to access TFTP server resources simultaneously. This value should be increased for larger networks.

When you use the **reset sequence-all** command, the router waits for one phone to complete its reset and reregister before starting to reset the next phone. The delay provided by this command prevents multiple phones from attempting to access the TFTP server simultaneously and therefore failing to reset properly. Each reset operation can take several minutes when you use this command. There is a reset timeout of 4 minutes, after which the router stops waiting for the currently registering phone to complete registration and starts to reset the next phone.

If the router configuration is changed so that the XML configuration files for the phones are modified (changes are made to user locale, network locale, or phone firmware), then whenever you use the **reset all** or **restart all** command, the router automatically executes the **reset sequence-all** command instead. The **reset sequence-all** command resets phones one at a time in order to prevent multiple phones trying to contact the TFTP server simultaneously. This one-at-a-time sequencing can take a long time if there are many phones. To avoid this automatic behavior, use the **reset all** *time-interval* command or the **restart all** *time-interval* command with an explicit argument that is not equal to the default 15-second time interval; for example, set a time interval of 14 seconds. If a **reset sequence-all** command has been started in error, use the **reset cancel** command to interrupt and cancel the sequence of resets.

To perform a complete reboot of a single phone associated with a Cisco CallManager Express router, use the **reset** command in ephone configuration mode.

 Copyright © 2005, Cisco Systems, Inc.



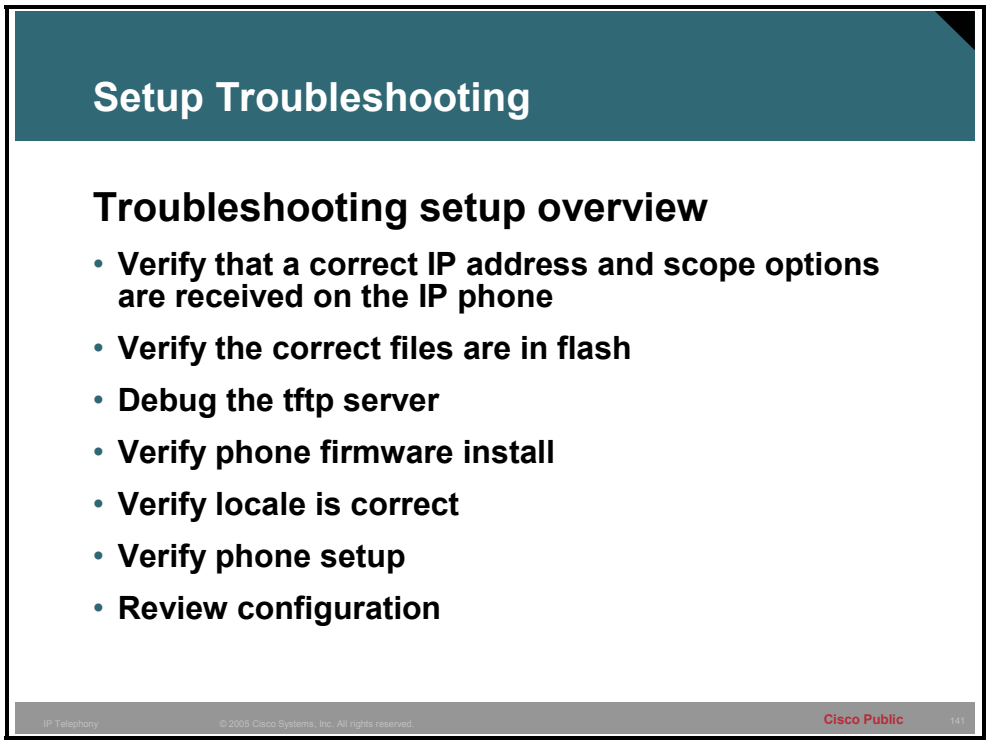
This command causes the system to perform a fast phone reset in which only the button template, lines, and speed-dial numbers are updated on the phone. For updates related to phone firmware, user locale, network locale, or URL parameters, use the **reset** command.

Use the **restart** command to reboot IP phones after quick changes to buttons, lines, and speed-dial numbers. This command is much faster than the **reset** command because the phone does not access the DHCP or TFTP server.

To restart a single phone, use the **restart** command with the *mac-address* argument or use the **restart** command in ephone configuration mode.

Setup Troubleshooting

This topic identifies IP phone setup troubleshooting tips.



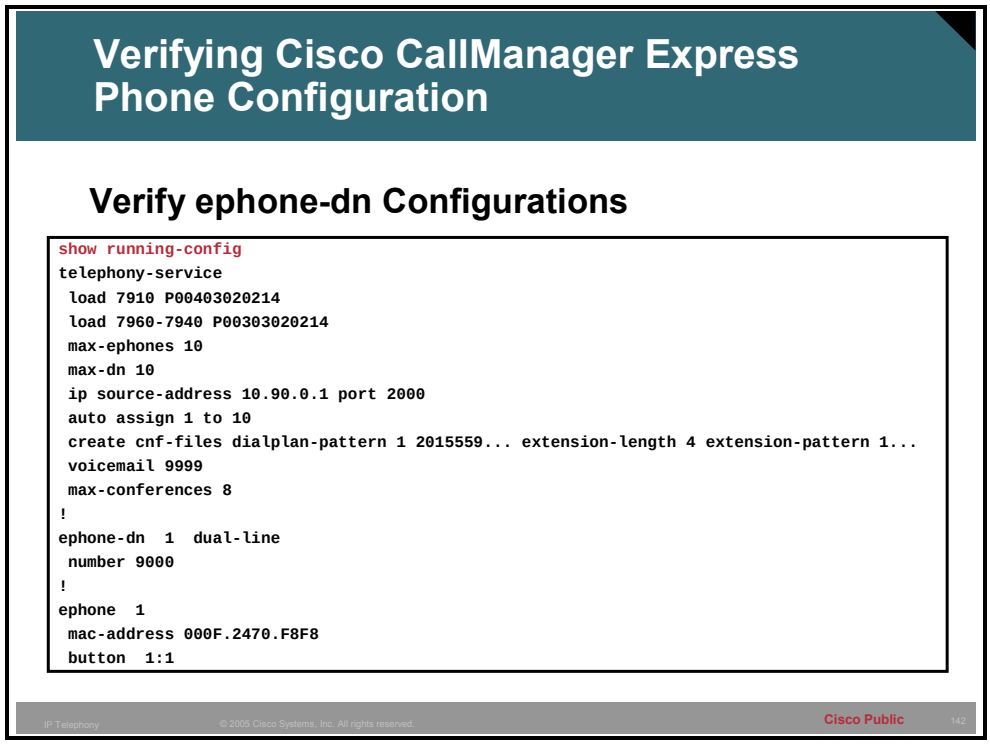
When using the automated setup if problems are encountered there are a many places to check, some of the more useful places and tools to use include:

- **Verify IP addressing** - checking the configuration on the IP phone through the "Settings" button
- **Verify the files in flash** – Check and verify that the correct firmware files are present in flash
- **Debug the TFTP server** – Make sure the firmware and xml files are being served correctly
- **Verify the phone firmware install –** Use the debug ephone register command to verify which firmware is being installed.
- **Verify locale is correct -** Use the telephony-service tftp-bindings command to view the files being served up by the tftp server
- **Verify phone setup –** Use the show ephone command to view the status of ephone and whether they are registered correctly
- **Review the configuration -** Use the show running-config command to verify the ephone-dn configuration

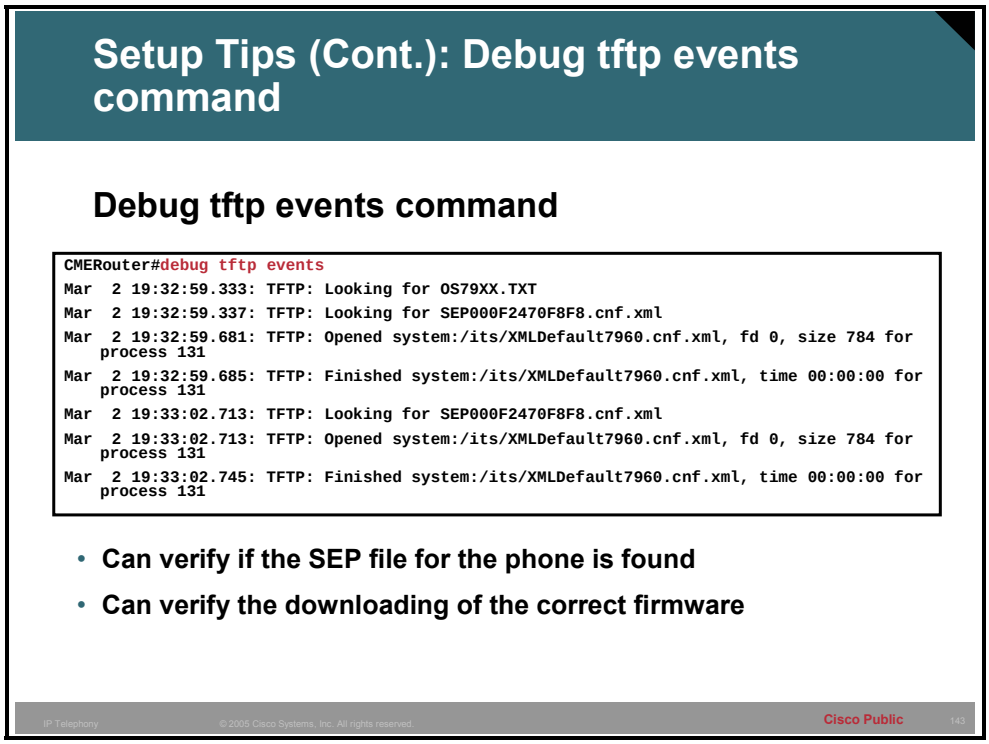
 Copyright © 2005, Cisco Systems, Inc.

Verifying Cisco CallManager Express Phone Configuration

This topic identifies the steps to verify the Cisco CME configuration.



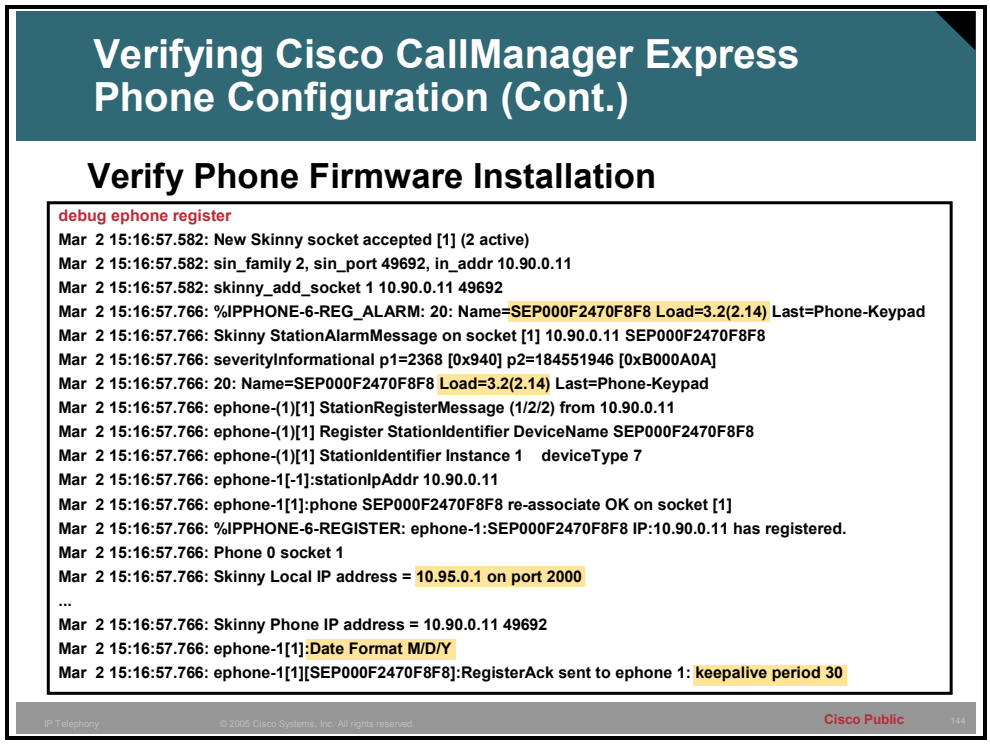
To verify the configuration the command **show running-config** may be used. The primary area of interest for Cisco CME functionality will be the telephony-service section, the tftp configuration, the ephones, and the ephone-dns.



The debugging command **debug tftp events** allows the administrator to view output regarding files that are served up by the tftp server. Cisco CME specific files include firmware if version are out of date or different than the supported versions, XML files for configured IP phones, XML files for new IP phones, and locale files.

If the firmware ends with a .bin extension then the file is unsigned. The .sbin firmware files are signed and if used the IP phone will permanently require signed load and can no longer use unsigned firmware loads.

 Copyright © 2005, Cisco Systems, Inc.



Verify the correct phone firmware installation by setting registration debugging with the **debug ephone register** command. Then, reset the phones and look at the StationAlarmMessage displayed during phone re-registration. The Load= parameter should appear in the display, followed by an abbreviated version name corresponding to the correct phone firmware file name.

Verifying Cisco CallManager Express Phone Configuration (Cont.)

Verify Locale-Specific Files

```
CMERouter1#show telephony-service tftp-bindings
tftp-server system:/its/SEPDEFAULT.cnf
tftp-server system:/its/SEPDEFAULT.cnf alias SEPDefault.cnf
tftp-server system:/its/XMLDefault.cnf.xml alias XMLDefault.cnf.xml
tftp-server system:/its/ATADefault.cnf.xml
tftp-server system:/its/united_states/7960-tones.xml alias United_States/7960-tones.xml
tftp-server system:/its/united_states/7960-font.xml alias English_United_States/7960-font.xml
tftp-server system:/its/united_states/7960-dictionary.xml alias English_United_States/7960-
dictionary.xml
tftp-server system:/its/united_states/7960-kate.xml alias English_United_States/7960-kate.xml
tftp-server system:/its/united_states/SCCP-dictionary.xml alias English_United_States/SCCP-
dictionary.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEP000F2470F8F8.cnf.xml
tftp-server system:/its/XMLDefault7960.cnf.xml alias SEP000F23FC9CF0.cnf.xml
```

IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 145

Use the show telephony-service tftp-bindings command to ensure that the locale-specific files are correct.

Verifying Cisco CallManager Express Phone Configuration (Cont.)

Verify Cisco IP Phone Setup

```
CMERouter1#show ephone
ephone-1 Mac:000F.2470.F8F8 TCP socket:[1] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:1
IP:10.10.0.11 49692 Telecaster 7960  keepalive 29 max_line 6
button 1: dn 1  number 1000 CH1   IDLE         CH2   IDLE

ephone-2 Mac:000F.23FC.9CF0 TCP socket:[2] activeLine:0 REGISTERED
mediaActive:0 offhook:0 ringing:0 reset:0 reset_sent:0 paging 0 debug:1
IP:10.10.0.13 52633 Telecaster 7960  keepalive 135 max_line 6
button 1: dn 2  number 1001 CH1   IDLE         CH2   IDLE
```

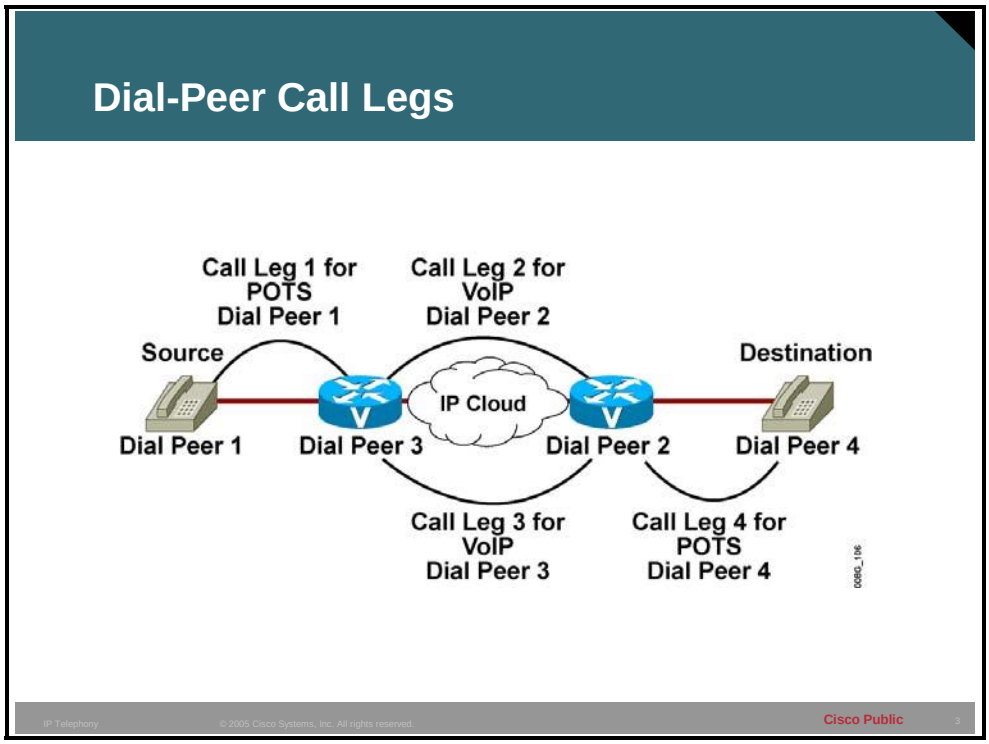
IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 146

Enter the show ephone command to verify Cisco IP phone setup after phones have registered with the Cisco CME router.

Call Establishment Principles

What Are Call Legs?

This topic describes call legs and their relationship to other components.



Call legs are logical connections between any two telephony devices, such as gateways, routers, Cisco CallManagers, or telephony endpoint devices.

Call legs are router-centric. When an inbound call arrives, it is processed separately until the destination is determined. Then a second outbound call leg is established, and the inbound call leg is switched to the outbound voice port.

Example: Call Legs Defined

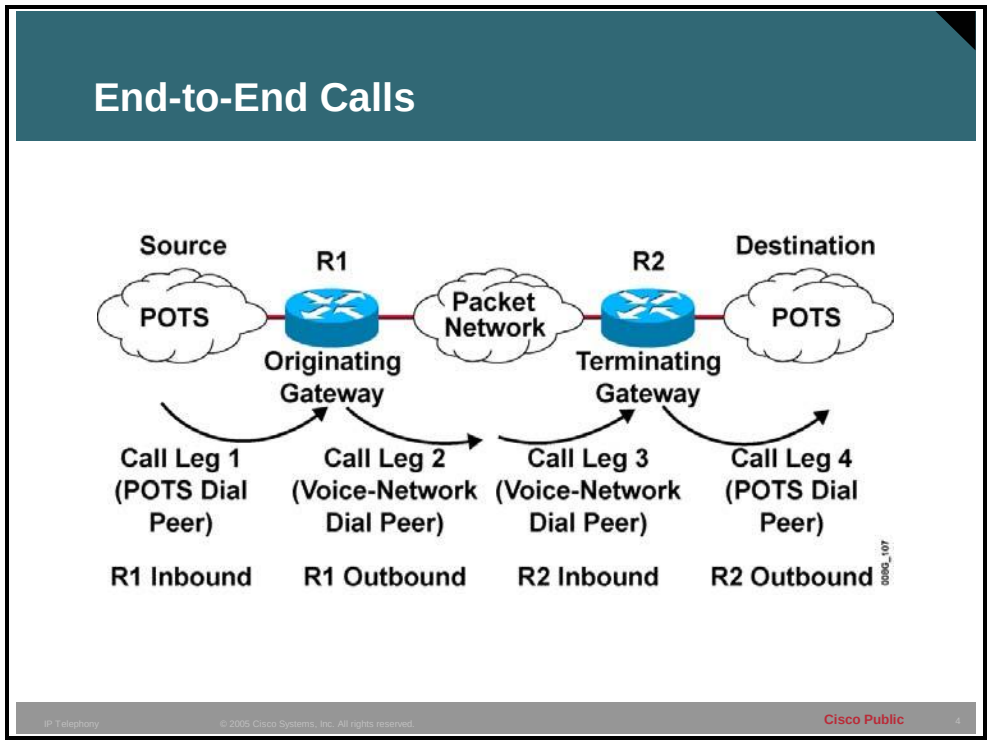
The connections are made when you configure dial peers on each interface. An end-to-end call consists of four call legs: two from the source router perspective (as shown in the figure), and two from the destination router perspective. To complete an end-to-end call from either side and send voice packets back and forth, you must configure all four dial peers.

Dial peers are used only to set up calls. When the call is established, dial peers are no longer used.

 Copyright © 2005, Cisco Systems, Inc.

End-to-End Calls

This topic explains how routers interpret call legs to establish end-to-end calls.



An end-to-end voice call consists of four call legs: two from the originating router (R1) or gateway perspective, and two from the terminating router (R2) or gateway perspective. An inbound call leg originates when an incoming call comes *into* the router or gateway. An outbound call leg originates when a call is placed *from* the router or gateway.

A call is segmented into call legs and a dial peer is associated with each call leg. The process for call setup is listed below:

1. The plain old telephone service (POTS) call arrives at R1 and an inbound POTS dial peer is matched.
2. After associating the incoming call to an inbound POTS dial peer, R1 creates an inbound POTS call leg and assigns it a Call ID (call leg 1).
3. R1 uses the dialed string to match an outbound voice network dial peer.
4. After associating the dialed string to an outbound voice network dial peer, R1 creates an outbound voice network call leg and assigns it a Call ID (call leg 2).
5. The voice network call request arrives at R2 and an inbound voice network dial peer is matched.
6. After R2 associates the incoming call to an inbound voice network dial peer, R2 creates the inbound voice network call leg and assigns it a Call ID (call leg 3). At this point, both R1 and R2 negotiate voice network capabilities and applications, if required.

When the originating router or gateway requests nondefault capabilities or applications, the terminating router or gateway must match an inbound voice network dial peer that is configured for such capabilities or applications.

7. R2 uses the dialed string to match an outbound POTS dial peer.

8. After associating the incoming call setup with an outbound POTS dial peer, R2 creates an outbound POTS call leg, assigns it a Call ID, and completes the call (call leg 4).

 Copyright © 2005, Cisco Systems, Inc.

Steps to Configure Class of Restriction

This topic presents the steps to configure Class of Restriction (COR).

Steps to Configure Class of Restriction

- **Step 1 – Configure the Class of Restriction names**
- **Step 2 – Configure the Class of Restriction lists and members**
- **Step 3 – Assign the COR list to the dial peers**
- **Step 4 - Assign the COR to the ephone-dns**

© 2005 Cisco Systems, Inc. All rights reserved.

Steps to Configure Class of Restriction

Step 1 – Configure the Class of Restriction names

```
CMERouter(config)#
dial-peer cor custom
```

- **Enters COR config mode where classes of restrictions are specified**

```
CMERouter(config-dp-cor)#
name class-name
```

- **Used to specify a class of restriction**

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc.

Step 1 **Define the name of the COR**

Before relating a COR to a dial peer, it needs to be named. This is important because the COR list needs to refer to these names to apply the COR to dial peers or ephone-dns. Multiple names can be added to represent various COR criteria. The ‘dial-peer cor custom’ and ‘name’ commands define the COR functionality. Possible names: call1900, call527, call9. Up to 64 COR names can be defined under a dial peer cor custom. This means that a configuration cannot have more than 64 COR names and A COR list would have a limitation of 64 members.

Example: COR naming and list

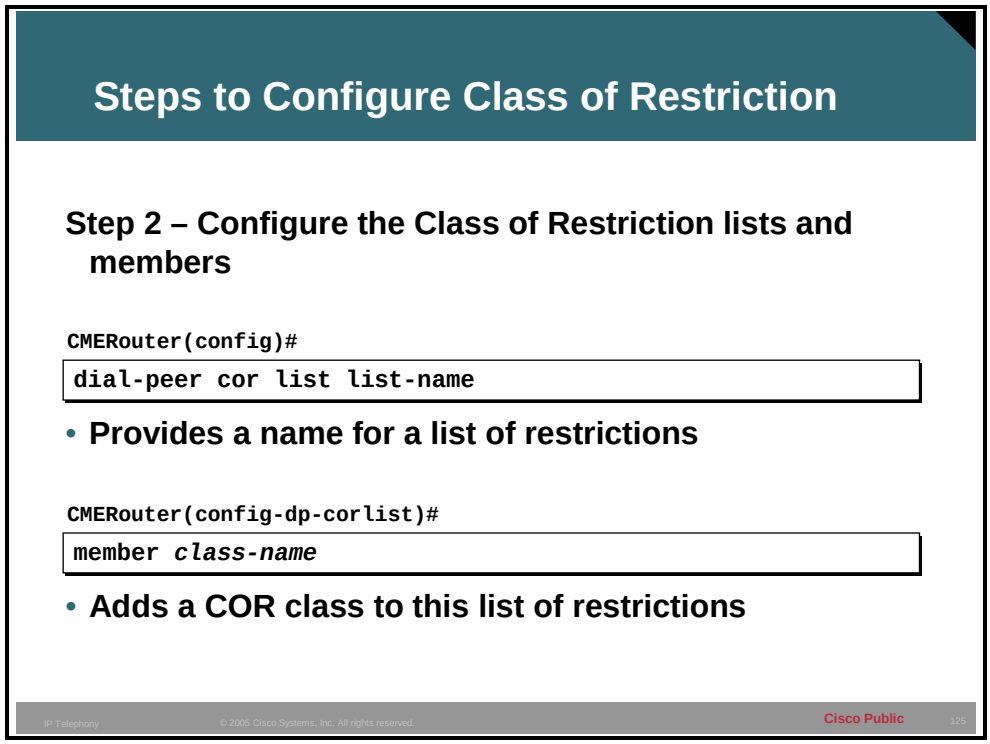
CMERouter(config)#dial-peer cor custom

CMERouter(config-dp-cor)#name local_call

CMERouter(config-dp-cor)#name 911

CMERouter(config-dp-cor)#name 1800

CMERouter(config-dp-cor)#name 1900



Step 2 Dial peer COR list and member commands set the capabilities of a COR list. COR list is used in dial peers to indicate the restriction that a dial peer has as an outgoing dial peer. The order of entering the members is not important and the list can be appended or made shorter by removing the members.

Example: Define the COR lists

CMERouter(config)#dial-peer list callLocal

CMERouter(config-dp-corlist)member local_call

CMERouter(config)#dial-peer list call911

CMERouter(config-dp-corlist)member 911

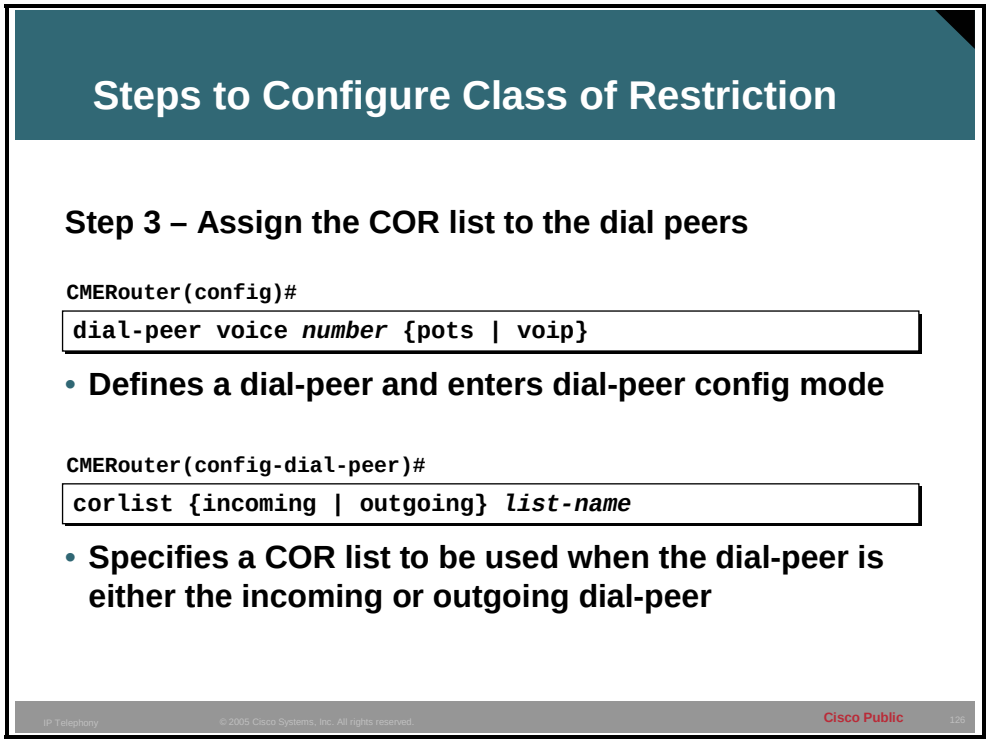
CMERouter(config)#dial-peer list call1800

CMERouter(config-dp-corlist)member 1800

CMERouter(config)#dial-peer list call1900

CMERouter(config-dp-corlist)member 1900

This is the third step to configure Class of Restriction (COR).



 Copyright © 2005, Cisco Systems, Inc.

Step 3 Apply the incoming or outgoing COR list to the dial peer. The incoming COR list specifies the capacity of dial-peer to initiate a certain series or Class of Calls. The outgoing COR list specifies the restriction on dial peers able to place calls to a given number range or port.

Example: Apply the COR to the dial peer

CMERouter(config)#dial-peer voice 1 pots

CMERouter(config-dial-peer)#destination-pattern 1500

CMERouter(config-dial-peer)#port 1/0/0

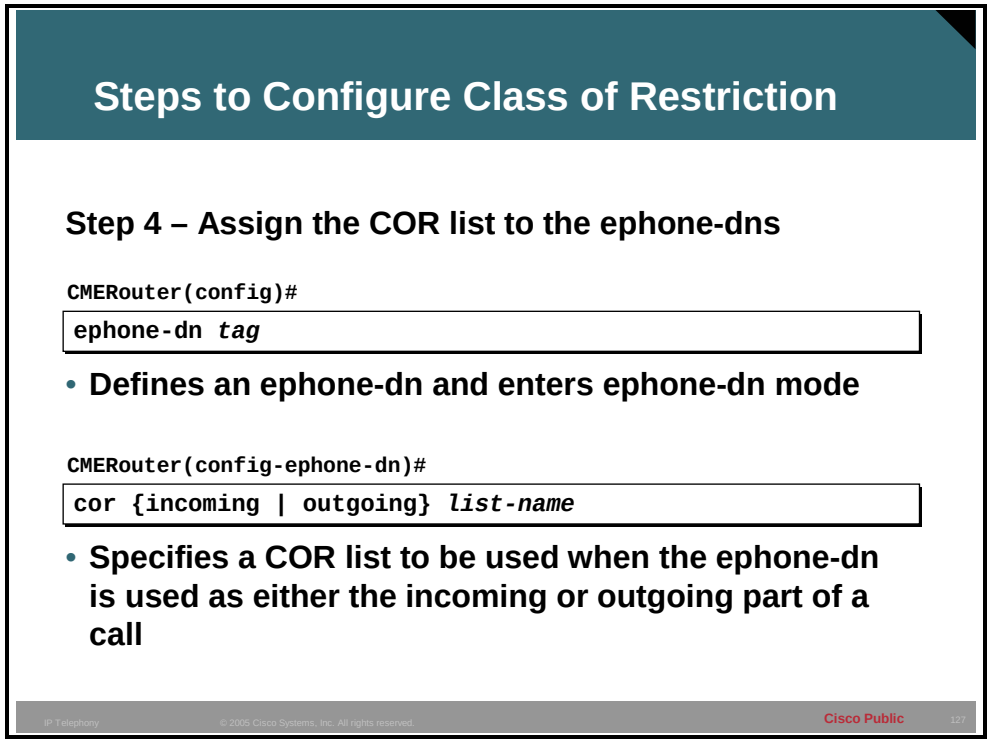
CMERouter(config-dial-peer)#corlist incoming call911

CMERouter(config)#dial-peer voice 2pots

CMERouter(config-dial-peer)#destination-pattern 1800.....

CMERouter(config-dial-peer)#port 2//1

CMERouter(config-dial-peer)#corlist outgoing call1800



Step 4 Apply the incoming or outgoing COR list to an ephone-dn. The Incoming COR list specifies the capacity of ephone-dn to initiate a certain series or Class of Calls. The outgoing COR list specifies the restriction on the ephone-dn to be able to place calls to a given number range or port.

Example: Apply the COR to ephone-dns

```
CMERouter(config)#ephone-dn 1

CMERouter(config-ephone-dn)#number 1000

CMERouter(config-ephone-dn)#description LobbyPhone

CMERouter(config-ephone-dn)#cor incoming call911

CMERouter(config)#ephone-dn 2

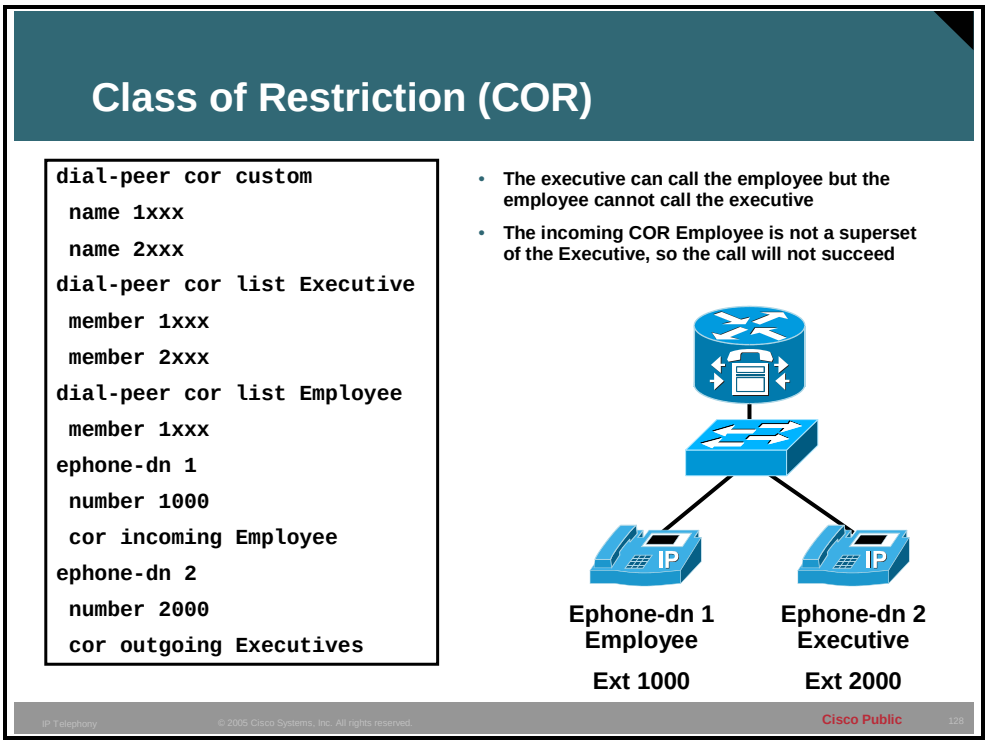
CMERouter(config-ephone-dn)#number 1001

CMERouter(config-ephone-dn)#description ConfRoomPhone

CMERouter(config-ephone-dn)#cor incoming callLocal
```

 Copyright © 2005, Cisco Systems, Inc.

This is an example of Class of Restriction (COR).



Example: COR used to restrict access internally within Cisco CME

COR can be used to regulate internal calls and whether they are allowed or not. This example shows two IP phones with an employee and an executive. In this company, the executive should be able to call anyone but employees should not be able to call the executive. Notice that to accomplish the required results, both an incoming COR on the employee must be configured as well as an outgoing COR on the executive. There is no outgoing COR on the employee and as a result anyone can call the employee phone regardless if the phone calling has an incoming COR set or not. The lack of an incoming COR on the executive will allow the executive to call any phone regardless of the outgoing COR setting on the phone called.

This topic describes Class of Restriction case study.

Class of Restriction – Case Study

Class of Restriction Case Study – XYZ company

- **The XYZ company wishes to prevent toll fraud by restricting the destinations on the PSTN that IP phones and analog phones attached to FXS port can call.**
- **There should be no restrictions internally; everyone internal should be able to call anyone else internal**
- **All phones MUST be able to call 911**
- **Within the XYZ company there are Lobby phones, Employee phones, Sales, and Executive phones**
- **The Lobby phone should be able to call only 911 on the PSTN**
- **The Employee phones should be able to call 911 and local calls on the PSTN**
- **The Sales phones should be able to call 911, local calls, and domestic long distance on the PSTN**
- **The executives should be able to call 911, local call, domestic long distance, and international on the PSTN**
- **No one should be able to call 900 numbers**

© 2005 Cisco Systems, Inc. All rights reserved.

Case Study of the XYZ Company.

Class of Restriction – Case Study

```
dial-peer cor custom
 name 911
 name local
 name long_distance
 name international
 name 900
```



911



local



long_distance



international



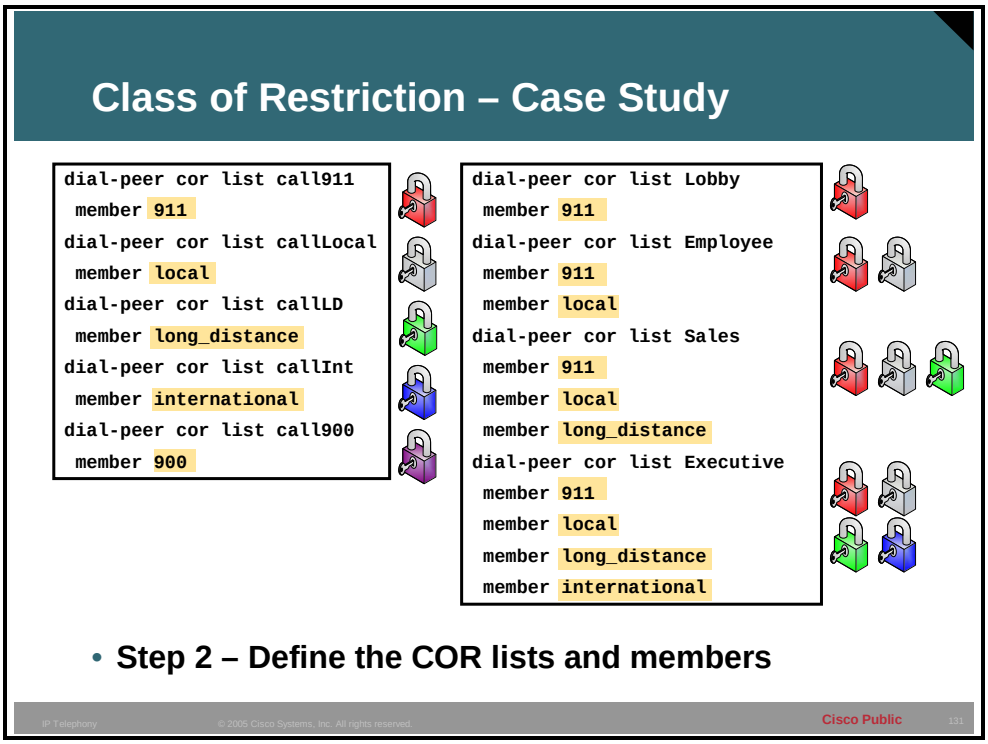
900

- **Step 1 - Define the classes of restriction**

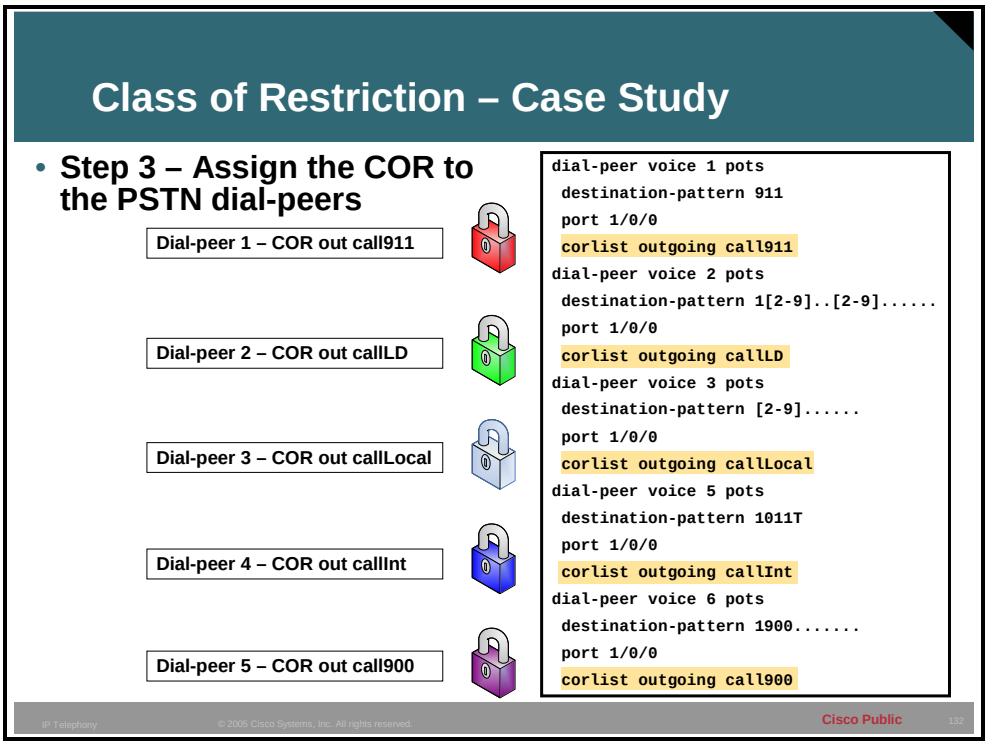
© 2005 Cisco Systems, Inc. All rights reserved.

Step 1 The first step will be to define the COR names.

Copyright © 2005, Cisco Systems, Inc.

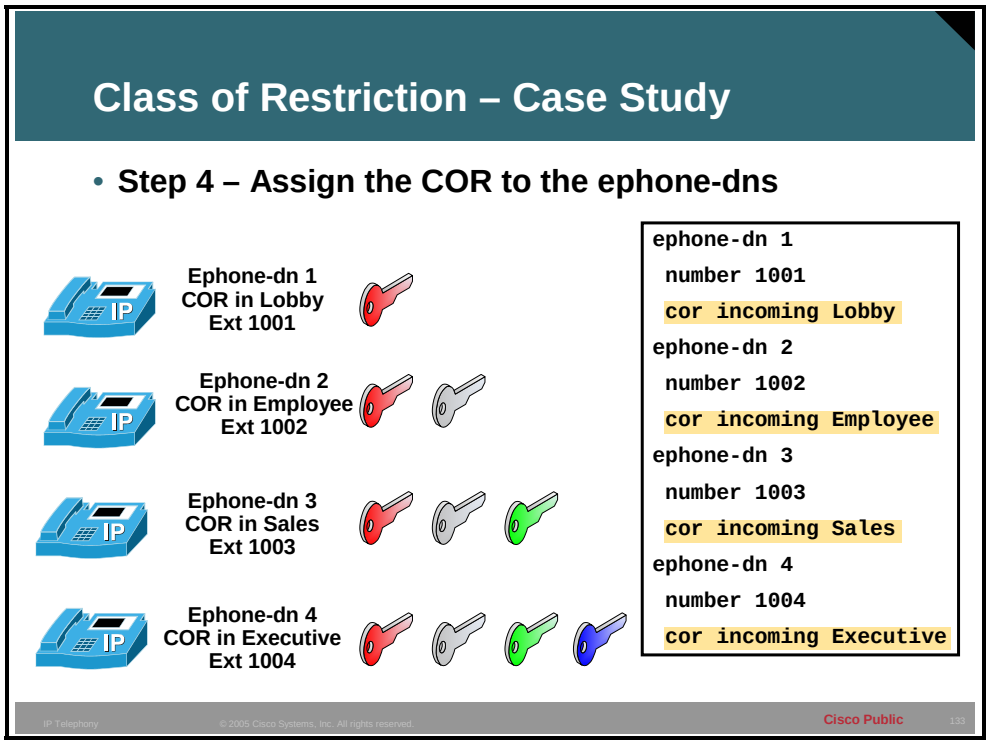


Step 2 The second step will be to define the COR list and its member or members. Notice that none of the COR lists contain the member 900.



Step 3 Assign the COR to the dial peers that govern PSTN access. To restrict calls to the PSTN destinations, the outbound COR setting will be defined.

Note Although not shown here, the inbound COR can be set to regulate where calls arriving from the PSTN will be allowed to connect internally.



Step 4 Assign the incoming COR to the Lobby, Employee, Sales, and Executive ephone-dns. Notice that no ephone-dn has the ability to call 900 numbers.

 Copyright © 2005, Cisco Systems, Inc.

Class of Restriction – Case Study

Results:

- **The Lobby ephone-dn can only call 911 on the PSTN**
- **The Employee ephone-dn can call 911 and local calls on the PSTN**
- **The Sales ephone-dn can call 911, local calls, and long distance on the PSTN**
- **The Executive ephone-dn can call 911, local calls, long distance, and international on the PSTN**
- **No one can call 900 numbers**



Ephone-dn 1
COR in Lobby
Ext 1001



Ephone-dn 2
COR in Employee
Ext 1002



Ephone-dn 3
COR in Sales
Ext 1003



Ephone-dn 4
COR in Executive
Ext 1004

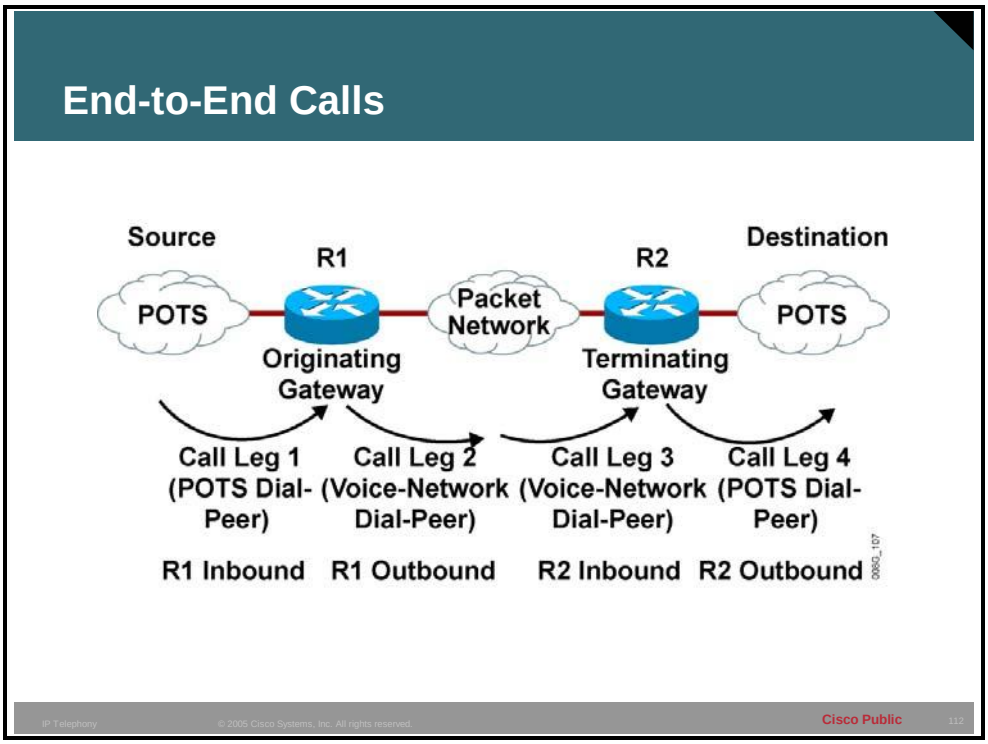
IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 134

The result of the configuration is shown.

Call Setup and Digit Manipulation

End-to-End Calls

This topic explains how routers interpret call legs to establish end-to-end calls.



An end-to-end voice call consists of four call legs: two from the originating router (R1) or gateway perspective and two from the terminating router (R2) or gateway perspective. An inbound call leg originates when an incoming call comes *into* the router or gateway. An outbound call leg originates when a call is placed *from* the router or gateway.

A call is segmented into call legs and a dial peer is associated with each call leg. The process for call setup is listed below:

1. The plain old telephone service (POTS) call arrives at R1 and an inbound POTS dial peer is matched.
2. After associating the incoming call to an inbound POTS dial peer, R1 creates an inbound POTS call leg and assigns it a Call ID (Call Leg 1).
3. R1 uses the dialed string to match an outbound voice network dial peer.
4. After associating the dialed string to an outbound voice network dial peer, R1 creates an outbound voice network call leg and assigns it a Call ID (Call Leg 2).
5. The voice network call request arrives at Router 2 (R2) and an inbound voice network dial peer is matched.

6. After R2 associates the incoming call to an inbound voice network dial peer, R2 creates the inbound voice network call leg and assigns it a Call ID (Call Leg 3). At this point, both R1 and R2 negotiate voice network capabilities and applications, if required.

When the originating router or gateway requests non-default capabilities or applications, the terminating router or gateway must match an inbound voice network dial peer that is configured for such capabilities or applications.

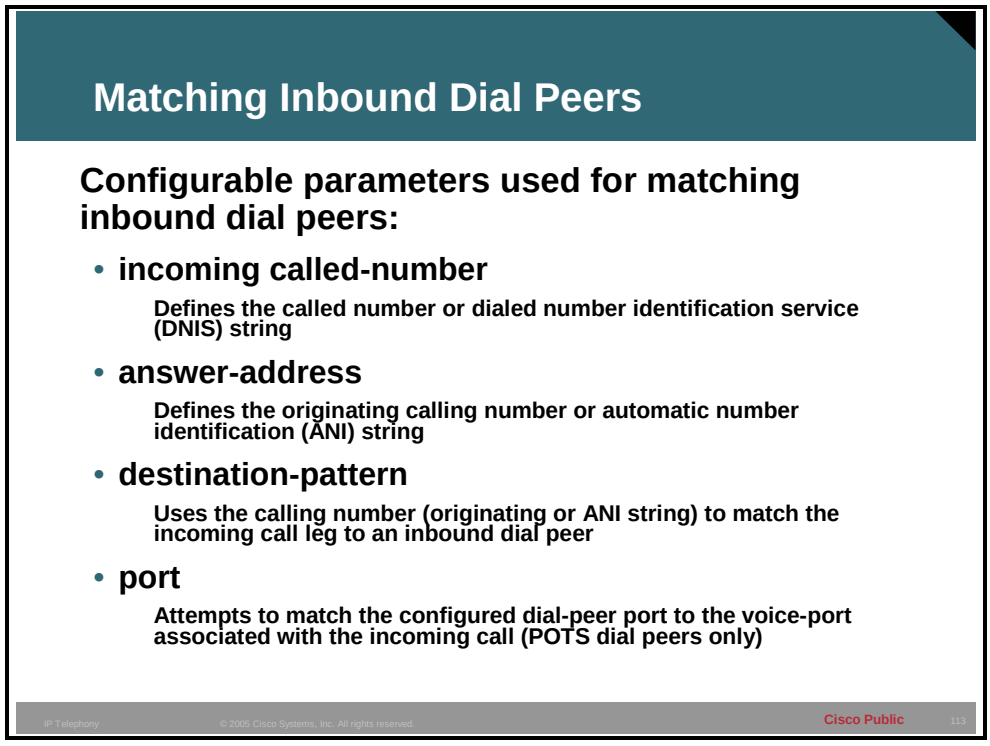
7. R2 uses the dialed string to match an outbound POTS dial peer.

8. After associating the incoming call setup with an outbound POTS dial peer, R2 creates an outbound POTS call leg, assigns it a Call ID, and completes the call (Call Leg 4).

 Copyright © 2005, Cisco Systems, Inc.

Matching Inbound Dial Peers

This topic describes how the router matches inbound dial peers.



When determining how inbound dial peers are matched on a router, it is important to note whether the inbound call leg is matched to a POTS or VoIP dial peer. Matching occurs in the following manner:

- Inbound POTS dial peers are associated to the incoming POTS call legs of the originating router or gateway.
- Inbound VoIP dial peers are associated to the incoming VoIP call legs of the terminating router or gateway.

Three information elements sent in the call setup message are matched against four configurable dial-peer command attributes.

The three call setup information elements that are known about calls arriving at the gateway are:

Call Setup Information Elements

Call Setup Element	Description
Called number Dialed Number Identification Service (DNIS)	This is the call-destination dial string, and it is derived from the ISDN setup message or channel associated signaling (CAS) DNIS.
Calling Number Automatic Number Identification (ANI)	This is a number string that represents the origin, and it is derived from the ISDN setup message or CAS ANI. The ANI is also referred to as the Calling Line ID (CLID).
Voice Port	This represents the POTS physical voice port.

When the Cisco IOS router or gateway receives a call setup request, it makes a dial peer match for the incoming call. This is not digit-by-digit matching; instead, the router uses the full digit string received in the setup request for matching against the configured dial peers.

The router or gateway matches call setup element parameters in the following order:

How the Router or Gateway Matches Inbound Dial Peers

Step	Action
1	The router or gateway attempts to match the called number of the call setup request with the configured **incoming called-number** of each dial peer
2	If a match is not found, the router or gateway attempts to match the calling number of the call setup request with **answer-address** of each dial peer
3	If a match is not found, the router or gateway attempts to match the calling number of the call setup request to the **destination-pattern** of each dial peer
4	The voice port uses the voice port number associated with the incoming call setup request to match the inbound call leg to the configured dial peer **port** parameter
5	If multiple dial peers have the same port configured, then the router or gateway matches the first dial peer added to the configuration
6	If a match is not found in the previous steps, then the default is dial-peer 0

Because call setups always include DNIS information, it is recommended that you use the **incoming called-number** command for inbound dial-peer matching. Configuring **incoming called-number** is useful for a company that has a central call center providing support for a number of different products. Purchasers of each product get a unique 1-800 number to call for support. All support calls are routed to the same trunk group destined for the call center. When a call comes in, the computer telephony system uses the DNIS to flash the appropriate message on the computer screen of the agent to whom the call is routed. The agent will then know how to customize the greeting when answering the call.

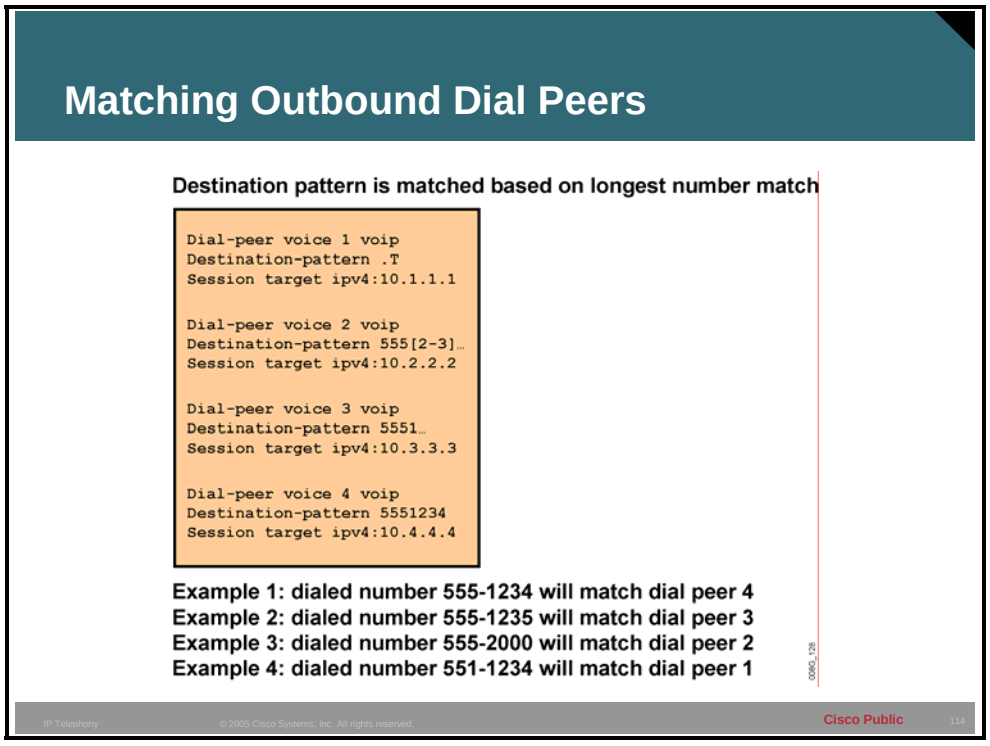
The calling number ANI with **answer address** is useful when you want to match calls based on the originating calling number. For example, when a company has international customers who require foreign-language-speaking agents to answer the call, the call can be routed to the appropriate agent based on the country of call origin.

 Copyright © 2005, Cisco Systems, Inc.

You must use the calling number ANI with **destination pattern** when the dial peers are set up for two-way calling. In a corporate environment, the head office and the remote sites must be connected. As long as each site has a VoIP dial peer configured to point to each site, inbound calls from the remote site will match against that dial peer.

Matching Outbound Dial Peers

This topic describes how the router matches outbound dial peers.



Outbound dial-peer matching is completed on a digit-by-digit basis. Therefore, the router or gateway checks for dial peer matches after receiving each digit, and then routes the call when a full match is made.

The router or gateway matches outbound dial peers in the following order:

How the Router or Gateway Matches Outbound Dial Peers

Step	Action
1	The router or gateway uses the dial peer **destination-pattern** command to determine how to route the call
2	The **destination-pattern** command routes the call in the following manner: ■ On POTS dial peers, the **port** command forwards the call ■ On VoIP dial peers, the **session target** command forwards the call
3	Use the **show dialplan number *string*** command to determine which dial peer is matched to a specific dialed string. This command displays all matching dial peers in the order that they are used.

Example

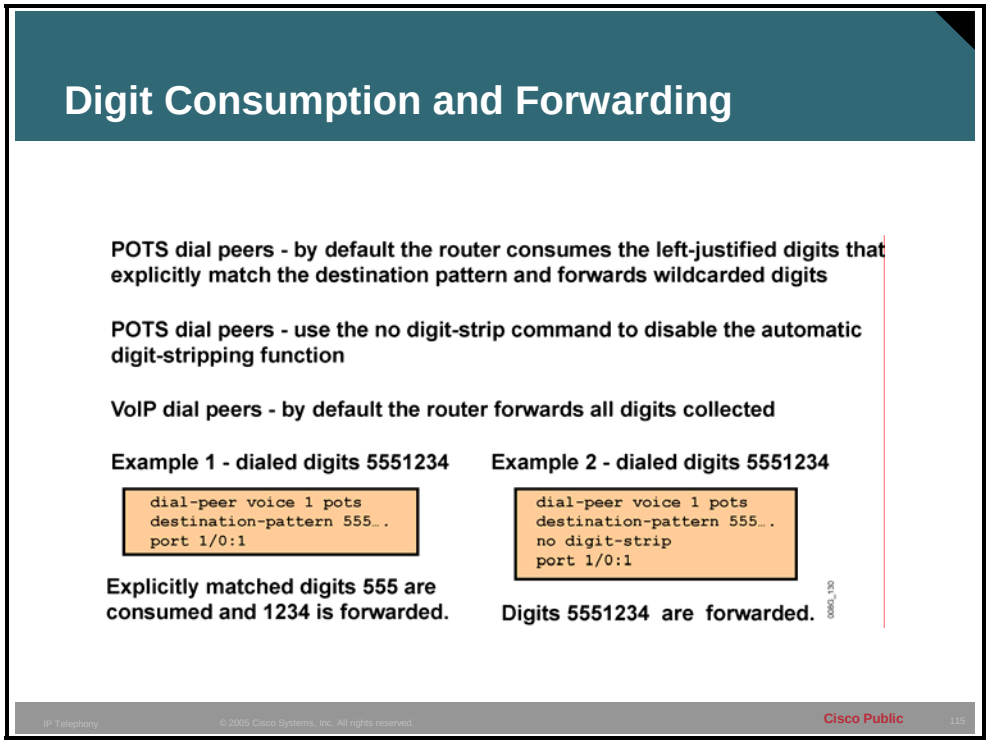
In the figure, dial-peer 1 matches any digit string that has not matched other dial peers more specifically. Dial-peer 2 matches any seven-digit number in the 2000 and 3000 range of numbers starting with 555. Dial-peer 3 matches any seven-digit number in the 1000 range of numbers starting with 555. Dial-peer 4 matches the specific number 5551234 only. When the

 Copyright © 2005, Cisco Systems, Inc.

number 5551234 is dialed, dial-peers 1, 3, and 4 all match that number, but dial-peer 4 places that call because it has the most specific destination pattern.

Digit Collection and Consumption

This topic describes how the router collects and consumes digits and applies them to the dial peer statements.



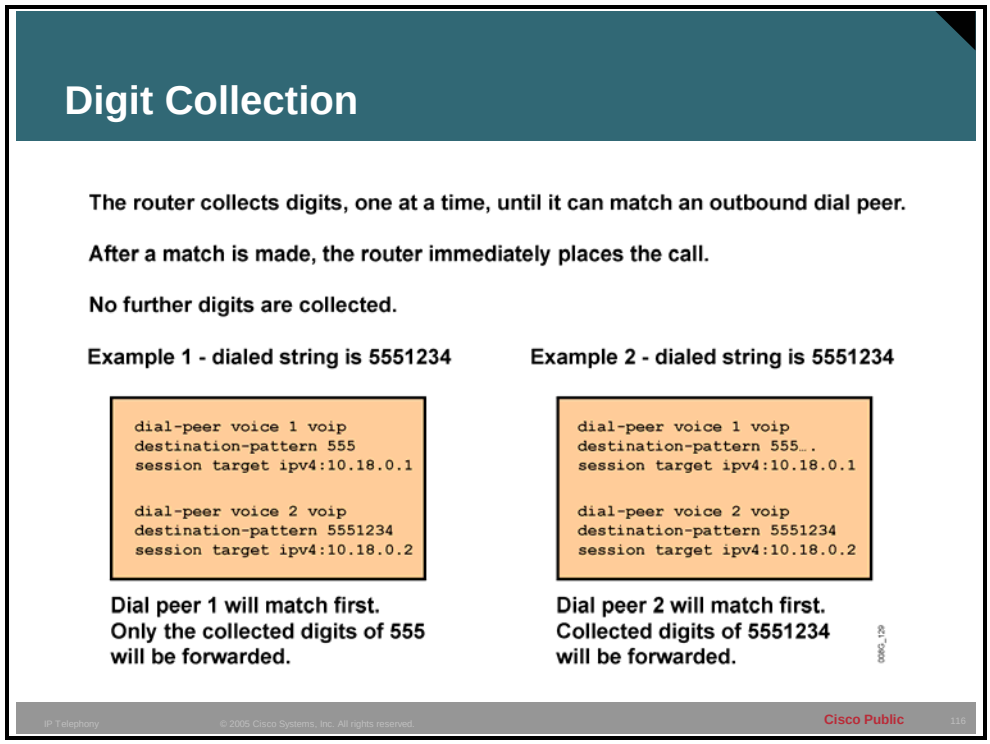
Use the **no digit-strip** command to disable the automatic digit-stripping function. This allows the router to match digits and pass them to the telephony interface.

By default, when the terminating router matches a dial string to an outbound POTS dial peer, the router strips off the left-justified digits that explicitly match the destination pattern. The remaining digits, or *wildcard digits,* are forwarded to the telephony interface, which connects devices such as a PBX or the PSTN.

Digit stripping is the desired action in some situations. There is no need to forward digits out of a POTS dial peer if it is pointing to an FXS port that connects a telephone or fax machine. If digit stripping is turned off on this type of port, the user may hear tones after answering the call because any unconsumed and unmatched digits are passed through the voice path after the call is answered.

In other situations, where a PBX or the PSTN is connected through the POTS dial peer, digit stripping is not desired because these devices need additional digits to further direct the call. In this situation, the administrator must assess the number of digits that need to be forwarded for the remote device to correctly process the call. With a VoIP dial peer, all digits are passed across the network to the terminating voice-enabled router.

 Copyright © 2005, Cisco Systems, Inc.



When a voice call enters the network:

How the Router Collects Digits

Step	Action
1	The originating router collects dialed digits until it matches an outbound dial peer
2	The router immediately places the call and forwards the associated dial string
3	The router collects no additional dialed digits

Example

The figure demonstrates the impact that overlapping destination patterns have on the call-routing decision. In example 1, the destination pattern in dial-peer 1 is a subset of the destination pattern in dial-peer 2. Because the router matches one digit at a time against available dial peers, an exact match will always occur on dial-peer 1, and dial-peer 2 will never be matched.

In example 2, the length of the destination patterns in both dial peers is the same. Dial-peer 2 has a more specific value than dial-peer 1, so it will be matched first. If the path to IP address 10.18.0.2 is unavailable, dial-peer 1 will be used.

Matching Destination Patterns

Dialed Digits	Destination Pattern	Dialed Digits Collected
5551234	5……	5551234
5551234	555….	5551234
5551234	555	555
5551234	555T	5551234

In the first row of the table, the destination pattern specifies a seven-digit string. The first digit must be a five, and the remaining six digits can be any valid digits. All seven digits must be entered before the destination pattern is matched.

In the second row, the destination pattern specifies a seven-digit string. The first three digits must be 555, and the remaining four digits can be any valid digits. All seven digits must be entered before the destination pattern is matched.

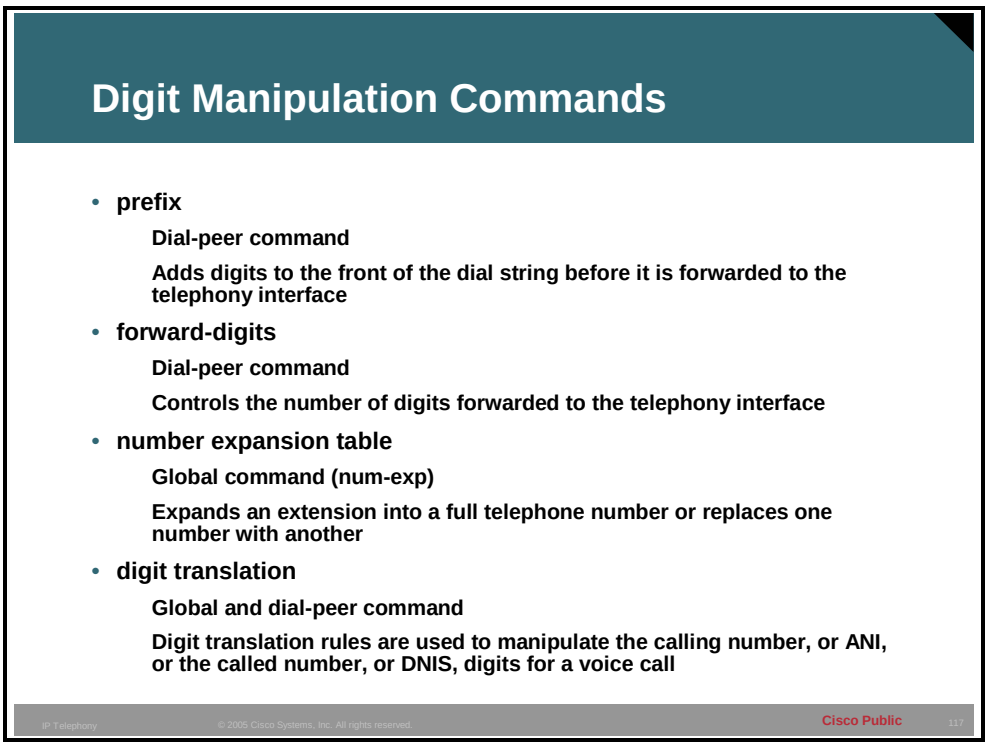
In the third row, the destination pattern specifies a three-digit string. The dialed digits must be exactly 555. When the user begins to dial the seven-digit number, the destination pattern matches after the first three digits are entered. The router then stops collecting digits and places the call. If the call is set up quickly, the answering party at the other end may hear the remaining four digits as the user finishes dialing the string. After a call is set up, any dual-tone multifrequency (DTMF) tones are sent through the voice path and played out at the other end.

In the last row, the destination pattern specifies a variable-length digit string that is at least three digits long. The first three digits must be exactly 555, and the remaining digits can be any valid digits. The ‘T’ tells the router to continue collecting digits until the interdigit timer expires. The router stops collecting digits when the timer expires, or when the user presses the pound (#) key.

 Copyright © 2005, Cisco Systems, Inc.

What Is Digit Manipulation?

This topic describes digit manipulation and the commands that are used to connect to a specified destination.



Digit manipulation is the task of adding or subtracting digits from the original dialed number to accommodate user-dialing habits or gateway needs. The digits can be manipulated before matching an inbound or outbound dial peer. The following is a list of digit manipulation commands and their uses:

- **prefix:** This dial-peer command adds digits to the front of the dial string before it is forwarded to the telephony interface. This occurs after the outbound dial peer is matched, but before digits get sent out of the telephony interface. Use the **prefix** command when the dialed digits leaving the router must be changed from the dialed digits that had originally matched the dial peer; for example, a call is dialed using a four-digit extension such as 1234, but the call needs to be routed to the PSTN, which requires ten digit dialing. If the four-digit extension matches the last four digits of the actual PSTN telephone number, then you can use the **prefix** command, **prefix 902555**, to prepend the six additional digits needed for the PSTN to route the call to 902-555-1234. After the POTS dial peer is matched with the destination pattern of 1234, the **prefix** command prepends the additional digits, and the string 9025551234 is sent out of the voice port to the PSTN.

- **forward-digits:** This dial-peer command specifies the number of digits that must be forwarded to the telephony interface, regardless of whether they are explicitly matched or wildcard matched. This command occurs after the outbound dial peer is matched, but before the digits are sent out of the telephony interface. When a specific number of digits are configured for forwarding, the count is right justified. For example, if the POTS dial peer has a destination pattern configured to match all extensions in the 1000 range (destination-pattern 1…), by default, only the last three digits are forwarded to the PBX that is connected to the specified voice port. If the PBX needs all four digits to route the call, you must use the command **forward-digits 4**, or **forward-digits all**, so that the appropriate number of digits are forwarded.

Note	To restore the **forward-digits** command to its default setting, use the **default forward-digits** command. Using the **no forward-digits** command specifies that no digits are to be forwarded.

- **number expansion table** (num-exp)**:** This global command expands an extension into a full telephone number or replaces one number with another. The number expansion table manipulates the called number. This command occurs before the outbound dial peer is matched; therefore, you must configure a dial peer with the expanded number in the destination pattern for the call to go through. The number expansion table is useful, for example, where the PSTN changes the dialing requirements from seven-digit dialing to ten-digit dialing. In this scenario, you can do one of the following:

  — Make all the users dial all ten digits to match the new POTS dial peer that is pointing to the PSTN

  — Allow the users to continue dialing the seven-digit number as they have before, but expand the number to include the area code before the ten-digit outbound dial peer is matched.

Note	You must use the **show num-exp** command to view the configured number-expansion table. You must use the **show dialplan number *number*** command to confirm the presence off a valid dial peer to match the newly expanded number.

- **digit translation**: Digit translation is a two-step configuration process. First, the translation rule is defined at the global level. Then, the rule is applied at the dial-peer level either as inbound or outbound translation on either the called or calling number. Translation rules manipulate the ANI or DNIS digits for a voice call. Translation rules convert a telephone number into a different number before the call is matched to an inbound dial peer, or before the outbound dial-peer forwards the call. For example, an employee may dial a five-digit extension to reach another employee of the same company at another site. If the call is routed through the PSTN to reach the other site, the originating gateway may use

 Copyright © 2005, Cisco Systems, Inc.

translation rules to convert the five-digit extension into the ten-digit format that is recognized by the central office (CO) switch.

You can also use translation rules to change the numbering type for a call. For example, some gateways may tag a number with more than 11 digits as an international number, even when the user must dial 9 to reach an outside line. In this case, the number that is tagged as an international number needs to be translated into a national number—without the 9—before it is sent to the PSTN.

As illustrated in this topic, there are numerous ways to manipulate digits at various stages of call completion. In many cases, several of these tools will provide a workable solution. The administrator needs to determine which command will be most suitable and the requirements that are necessary for manipulation.

Note	To test configured translation rules, you must use the test **translation** command.

Example

The following is a sample configuration using the **prefix** command:

dial-peer voice 1 pots

destination-pattern 555….

prefix 555

port 1/0/0

In the sample configuration using the **prefix** command, the device attached to port 1/0/0 needs all seven digits to process the call. On a POTS dial peer, only wildcard-matched digits are forwarded by default. Use the **prefix** command to send the prefix numbers of 555 before forwarding the four wildcard-matched digits.

The following is a sample configuration using the **forward-digits** command:

dial-peer voice 1 pots

destination-pattern 555….

forward-digits 7

port 1/0/0

In the sample configuration using the forward-digits command, the device attached to port 1/0/0 needs all seven digits to process the call. On a POTS dial peer, only wildcard-matched digits are forwarded by default. The **forward-digits** command allows the user to specify the total number of digits to forward.

The following is a sample configuration using the **number expansion table** command:

num-exp 2… 5552…

dial-peer voice 1 pots

destination-pattern 5552…

port 1/1/0

In the sample configuration using the **number expansion table** command, the extension number of 2… is expanded to 5552… before an outbound dial peer is matched. For example, the user dials 2401, but the outbound dial-peer 1 is configured to match 5552401.

The following is a sample configuration using the **digit translation** command:

translation-rule 5

rule 1 2401 5552401

dial-peer voice 1 pots

translate-outgoing called-number 5

In the sample configuration using the **translation-rule** command, the rule is defined to translate 2401 into 5552401. The dial peer **translate-outgoing called-number 5** command notifies the router to use the globally defined translation rule 5 to translate the number before sending the string out the port. It is applied as an outbound translation from the POTS dial peer.

The following example shows a translation rule that converts any called number that starts with 91 and is tagged as an international number into a national number without the 9 before sending it to the PSTN.

translation-rule 20

rule 1 91 1 international national

!

!

dial-peer voice 10 pots

destination-pattern 91.....

translate-outgoing called 20

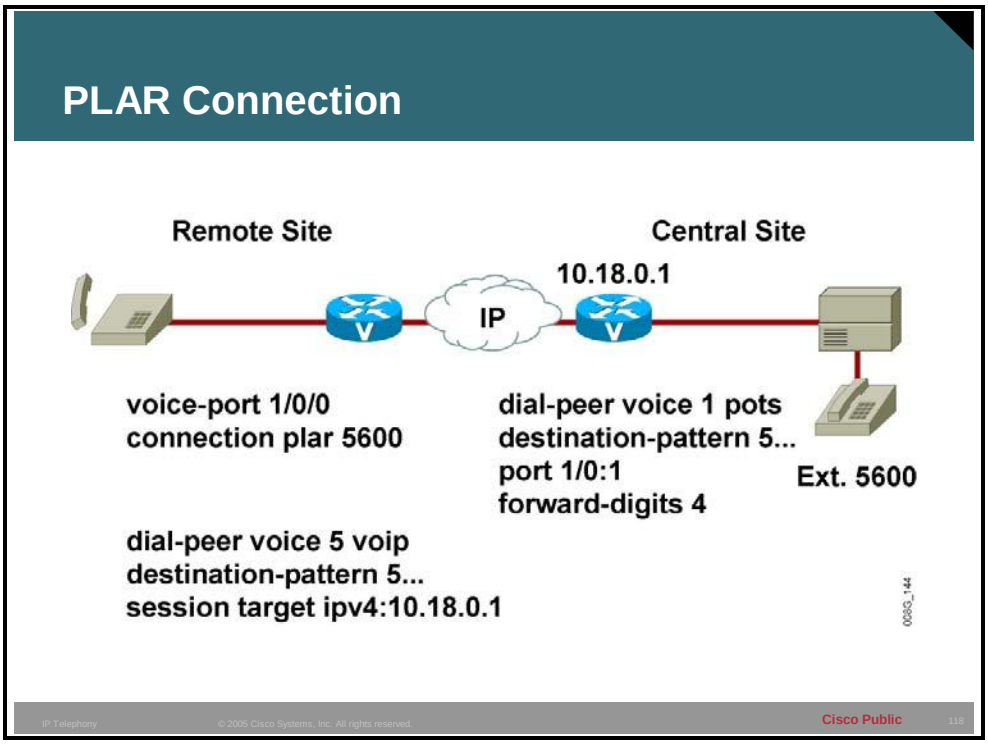
port 1/1:5

forward-digits all

 Copyright © 2005, Cisco Systems, Inc.

PLAR

This topic describes the use of PLAR connections



Private line, automatic ringdown (PLAR) is an autodialing mechanism that permanently associates a voice port with a far-end voice port, allowing call completion to a specific telephone number or PBX. When the calling telephone goes off hook, a predefined network dial peer is automatically matched, which sets up a call to the destination telephone or PBX. The caller does not hear a dial tone and does not have to dial a number. PLAR connections are widely used in the business world. One common use is to connect stockbrokers with trading floors. Timing is critical when dealing with stock transactions; the amount of time it may take to dial a number and get a connection can be costly in some cases. Another common use is in the travel sector, directly connecting travelers with services. Often, at places like airports, the traveler will see display boards advertising taxi companies, car rental companies and local hotels. These displays often have telephones that will connect the traveler directly with the service of choice; the device is preconfigured with the telephone number of the desired service. One obvious difference between these telephones and a normal telephone is that they do not have a dial pad.

As demonstrated in the figure, the following actions must occur to establish a PLAR connection:

1. A user at the remote site lifts the handset.
2. A voice port at the remote site router automatically generates digits 5600 for a dial-peer lookup.

3. The router at the remote site matches digits 5600 to Voice over IP (VoIP) dial peer 5 and sends the setup message with the digits 5600 to IP address 10.18.0.1 as designated in the session target statement.

4. The router at the central site matches received digits 5600 to plain old telephone service (POTS) dial peer 1 and forwards digits 5600 out voice port 1/0:1. At the same time, it sends a call-complete setup message to the router at the remote site because both the inbound and outbound call legs on the central site router were processed correctly.

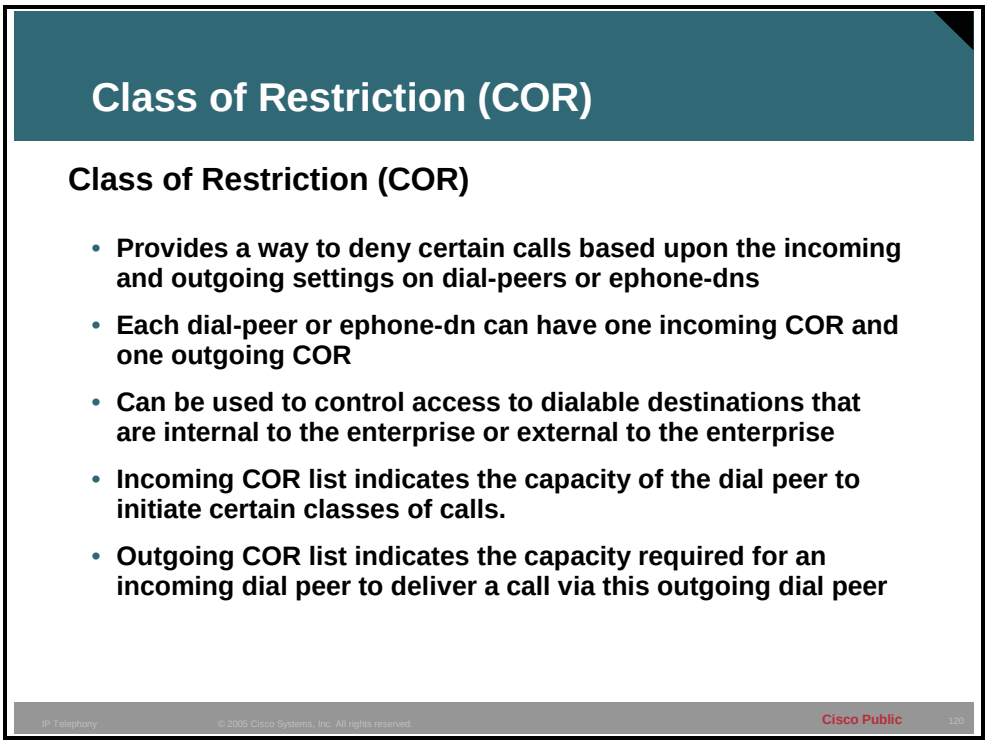
5. The PBX receives digits 5600 and rings the appropriate telephone.

 Copyright © 2005, Cisco Systems, Inc.

Class of Restriction

Class of Restriction (COR)

This topic describes Class of Restriction (COR).



The Class of Restrictions (COR) feature provides the ability to deny certain call attempts based on the incoming and outgoing CORs provisioned on the dial peers.

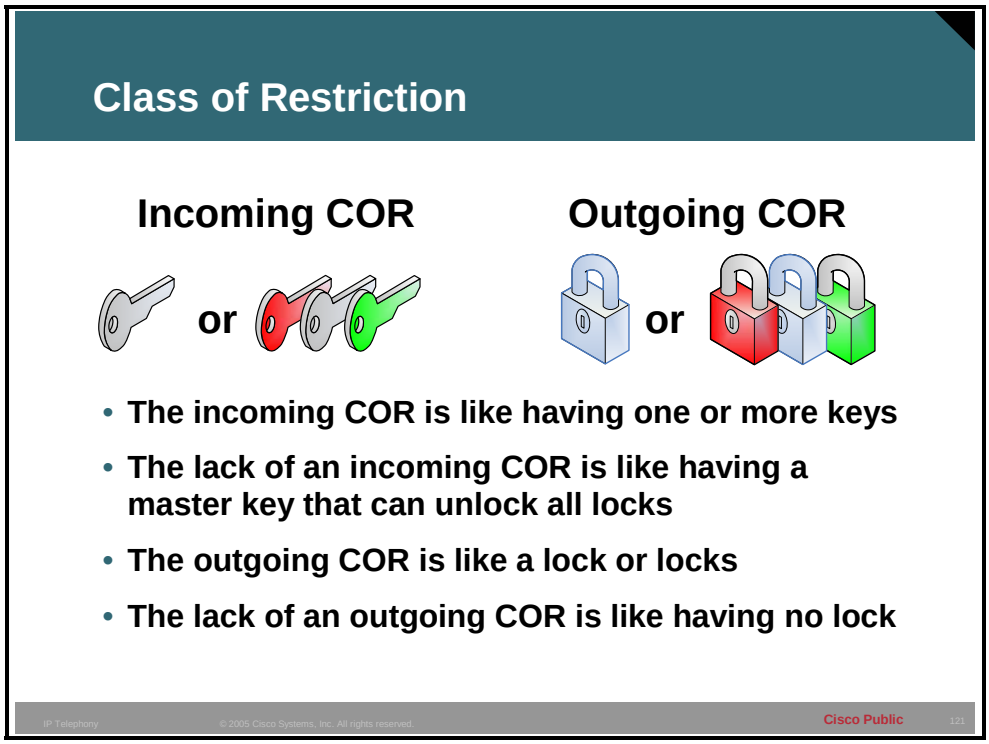
COR is used to specify which incoming dial peer can use which outgoing dial peer to make a call. Each dial peer can be provisioned with an incoming and an outgoing COR list. The COR command sets the dial peer COR parameter for dial peers and the directory numbers that are created for Cisco IP phones associated with the Cisco CME router. COR functionality provides the ability to deny certain call attempts on the basis of the incoming and outgoing class of restrictions that are provisioned on the dial peers. This functionality provides flexibility in network design, allows users to block calls (for example, calls to 900 numbers), and applies different restrictions to call attempts from different originators.

If the COR applied on an incoming dial peer (for incoming calls) is a superset or equal to the COR applied to the outgoing dial peer (for outgoing calls), the call will go through. Incoming and outgoing are with respect to the "voice ports."

Example: Incoming and Outgoing COR example

For example, if a phone is attached to one of the Foreign Exchange Station (FXS) ports of the router and an attempt is made to place a call from that phone, it is an incoming call and uses the

incoming COR for the router/voice-port. Similarly, if you make a call to that FXS phone, then it is an outgoing call and will use the outgoing COR for the voice-port.



When the incoming COR list is applied to an ephone-dn or dial-peer, the members of the COR list will be similar to keys. These keys will be used to unlock the outgoing COR list that is applied to the ephone-dn or dial peer that matches the digits of the destination pattern. The outgoing COR list is similar to having a lock or locks on it. In order to use the dial peer or ephone-dn with an outgoing COR list, the incoming COR list must have all the members (keys) that the outgoing COR list has.

The lack of an incoming COR list allows that ephone-dn or dial peer to call any other ephone-dn or dial peer regardless of the outgoing COR list. This is like having a master key for all locks. The lack of an outgoing COR list allows any ephone-dn or dial peer to complete calls to this ephone-dn or dial peer regardless of the incoming COR setting.

 Copyright © 2005, Cisco Systems, Inc.

Class of Restriction

COR List on Incoming dial-peer or ephone-dn	COR List on Outgoing dial-peer or ephone-dn	Result	Reason
No COR	No COR	Call Succeeds	COR not applied
No COR	Outgoing COR applied	Call Succeeds	The no (null) incoming COR condition has the highest COR priority
Incoming COR applied	No COR	Call Succeeds	The incoming COR list is a superset of the no (null) outgoing COR list
Incoming COR applied is a superset of outgoing COR	Outgoing COR applied	Call Succeeds	The incoming COR list is a superset of the outgoing COR list
Incoming COR applied not a superset of outgoing COR	Outgoing COR applied	Call cannot be completed	The incoming COR list is NOT a superset of the outgoing COR list

IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 122

By default, an incoming call leg has the highest COR priority and the outgoing COR list has the lowest COR priority. This means that if there is no COR configuration for incoming calls on a dial peer, then you can make a call from this dial peer (a phone attached to this dial peer) going out of any other dial peer, irrespective of the COR configuration on that dial peer.

Steps to Configure Class of Restriction

This topic presents the steps to configure Class of Restriction (COR).

Steps to Configure Class of Restriction

- **Step 1 – Configure the Class of Restriction names**
- **Step 2 – Configure the Class of Restriction lists and members**
- **Step 3 – Assign the COR list to the dial peers**
- **Step 4 - Assign the COR to the ephone-dns**

© 2005 Cisco Systems, Inc. All rights reserved.

Steps to Configure Class of Restriction

Step 1 – Configure the Class of Restriction names

```
CMERouter(config)#
dial-peer cor custom
```

- **Enters COR config mode where classes of restrictions are specified**

```
CMERouter(config-dp-cor)#
name class-name
```

- **Used to specify a class of restriction**

© 2005 Cisco Systems, Inc. All rights reserved.

Copyright © 2005, Cisco Systems, Inc.

Step 1 **Define the name of the COR**

Before relating a COR to a dial peer, it needs to be named. This is important because the COR list needs to refer to these names to apply the COR to dial peers or ephone-dns. Multiple names can be added to represent various COR criteria. The ‘dial-peer cor custom’ and ‘name’ commands define the COR functionality. Possible names: call1900, call527, call9. Up to 64 COR names can be defined under a dial peer cor custom. This means that a configuration cannot have more than 64 COR names and A COR list would have a limitation of 64 members.

Example: COR naming and list

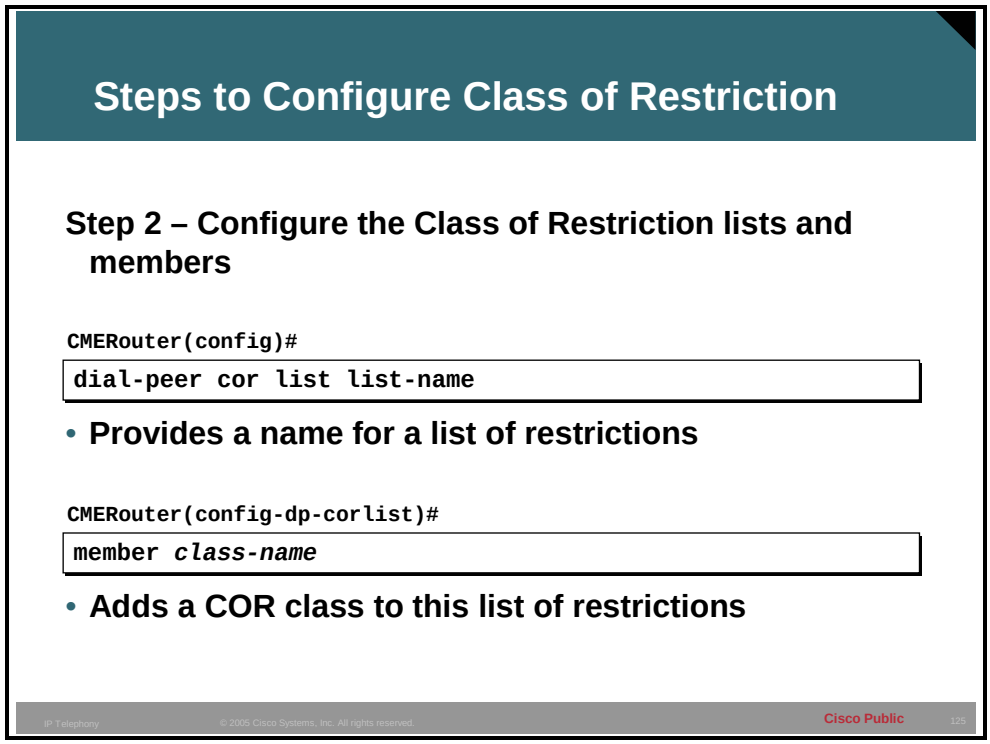
CMERouter(config)#dial-peer cor custom

CMERouter(config-dp-cor)#name local_call

CMERouter(config-dp-cor)#name 911

CMERouter(config-dp-cor)#name 1800

CMERouter(config-dp-cor)#name 1900



Step 2 Dial peer COR list and member commands set the capabilities of a COR list. COR list is used in dial peers to indicate the restriction that a dial peer has as an outgoing dial peer. The order of entering the members is not important and the list can be appended or made shorter by removing the members.

Example: Define the COR lists

CMERouter(config)#dial-peer list callLocal

CMERouter(config-dp-corlist)member local_call

CMERouter(config)#dial-peer list call911

CMERouter(config-dp-corlist)member 911

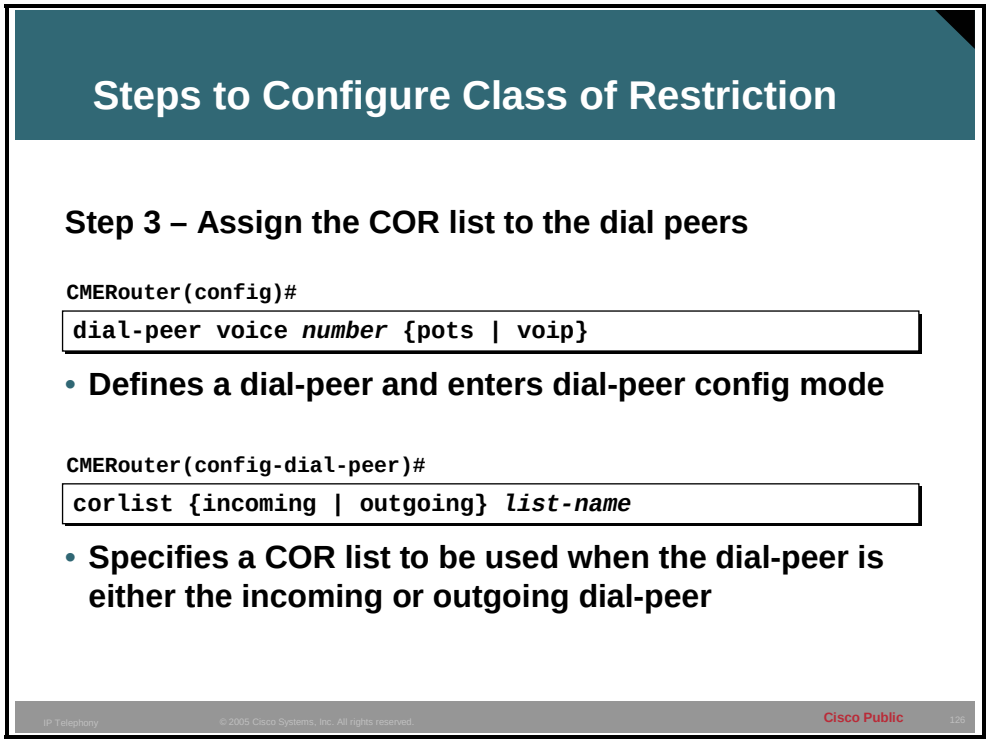
CMERouter(config)#dial-peer list call1800

CMERouter(config-dp-corlist)member 1800

CMERouter(config)#dial-peer list call1900

CMERouter(config-dp-corlist)member 1900

This is the third step to configure Class of Restriction (COR).



 Copyright © 2005, Cisco Systems, Inc.

Step 3 Apply the incoming or outgoing COR list to the dial peer. The incoming COR list specifies the capacity of dial-peer to initiate a certain series or Class of Calls. The outgoing COR list specifies the restriction on dial peers able to place calls to a given number range or port.

Example: Apply the COR to the dial peer

CMERouter(config)#dial-peer voice 1 pots

CMERouter(config-dial-peer)#destination-pattern 1500

CMERouter(config-dial-peer)#port 1/0/0

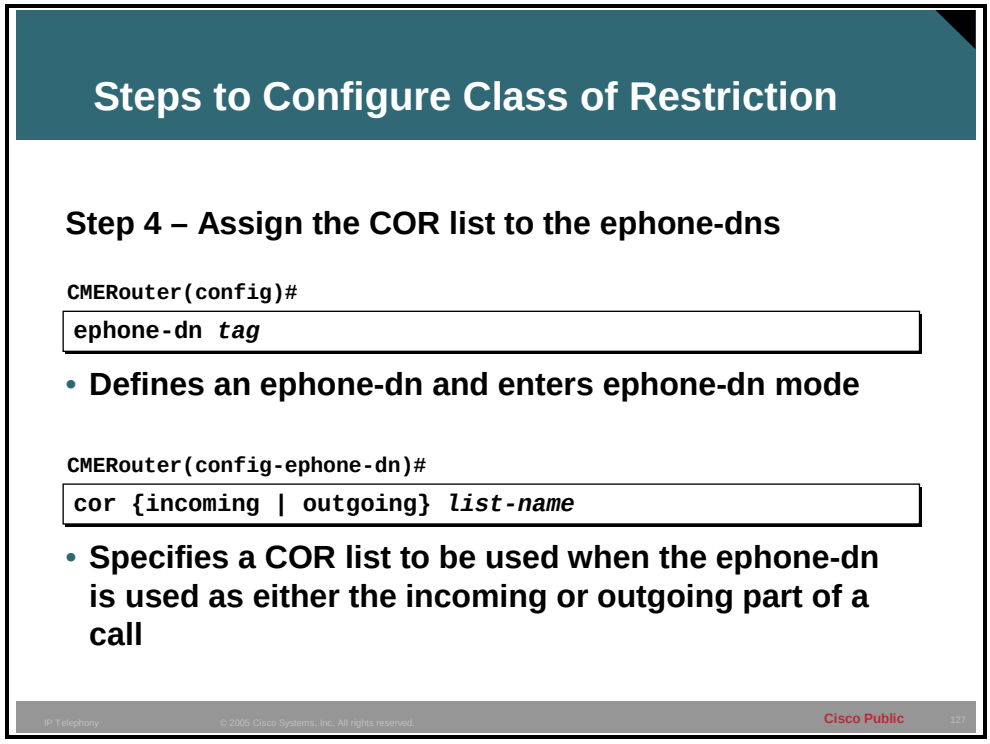
CMERouter(config-dial-peer)#corlist incoming call911

CMERouter(config)#dial-peer voice 2pots

CMERouter(config-dial-peer)#destination-pattern 1800.....

CMERouter(config-dial-peer)#port 2//1

CMERouter(config-dial-peer)#corlist outgoing call1800



Step 4 Apply the incoming or outgoing COR list to an ephone-dn. The Incoming COR list specifies the capacity of ephone-dn to initiate a certain series or Class of Calls. The outgoing COR list specifies the restriction on the ephone-dn to be able to place calls to a given number range or port.

Example: Apply the COR to ephone-dns

```
CMERouter(config)#ephone-dn 1

CMERouter(config-ephone-dn)#number 1000

CMERouter(config-ephone-dn)#description LobbyPhone

CMERouter(config-ephone-dn)#cor incoming call911

CMERouter(config)#ephone-dn 2

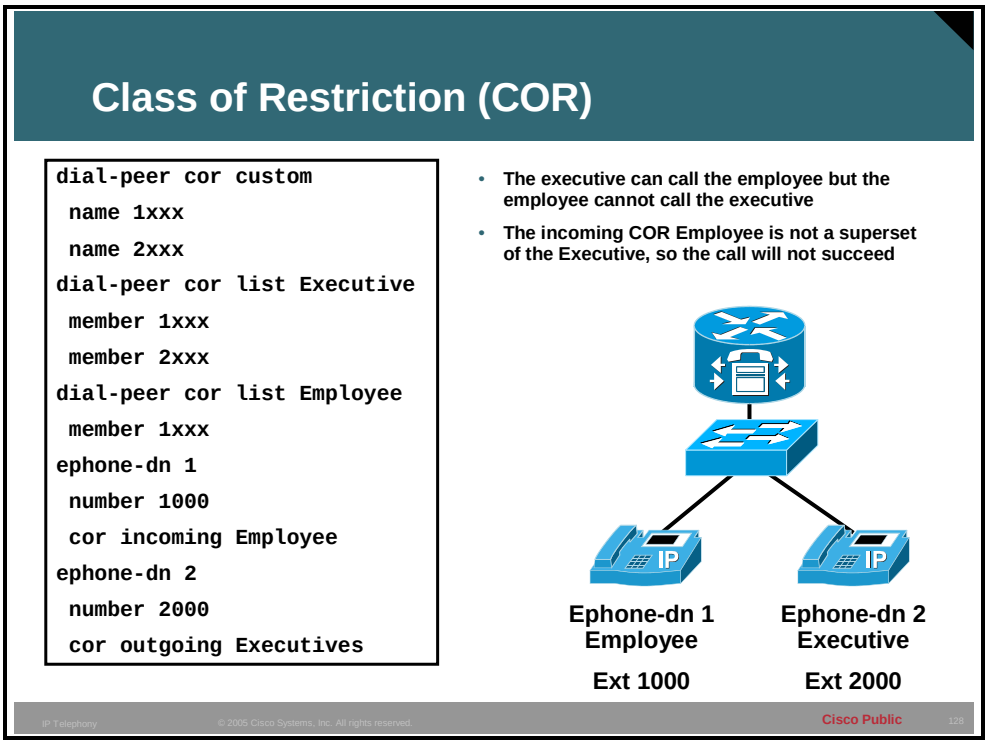
CMERouter(config-ephone-dn)#number 1001

CMERouter(config-ephone-dn)#description ConfRoomPhone

CMERouter(config-ephone-dn)#cor incoming callLocal
```

 Copyright © 2005, Cisco Systems, Inc.

This is an example of Class of Restriction (COR).



Example: COR used to restrict access internally within Cisco CME

COR can be used to regulate internal calls and whether they are allowed or not. This example shows two IP phones with an employee and an executive. In this company, the executive should be able to call anyone but employees should not be able to call the executive. Notice that to accomplish the required results, both an incoming COR on the employee must be configured as well as an outgoing COR on the executive. There is no outgoing COR on the employee and as a result anyone can call the employee phone regardless if the phone calling has an incoming COR set or not. The lack of an incoming COR on the executive will allow the executive to call any phone regardless of the outgoing COR setting on the phone called.

This topic describes Class of Restriction case study.

Class of Restriction – Case Study

Class of Restriction Case Study – XYZ company

- **The XYZ company wishes to prevent toll fraud by restricting the destinations on the PSTN that IP phones and analog phones attached to FXS port can call.**
- **There should be no restrictions internally; everyone internal should be able to call anyone else internal**
- **All phones MUST be able to call 911**
- **Within the XYZ company there are Lobby phones, Employee phones, Sales, and Executive phones**
- **The Lobby phone should be able to call only 911 on the PSTN**
- **The Employee phones should be able to call 911 and local calls on the PSTN**
- **The Sales phones should be able to call 911, local calls, and domestic long distance on the PSTN**
- **The executives should be able to call 911, local call, domestic long distance, and international on the PSTN**
- **No one should be able to call 900 numbers**

© 2005 Cisco Systems, Inc. All rights reserved.

Case Study of the XYZ Company.

Class of Restriction – Case Study

```
dial-peer cor custom
 name 911
 name local
 name long_distance
 name international
 name 900
```



911



local



long_distance



international



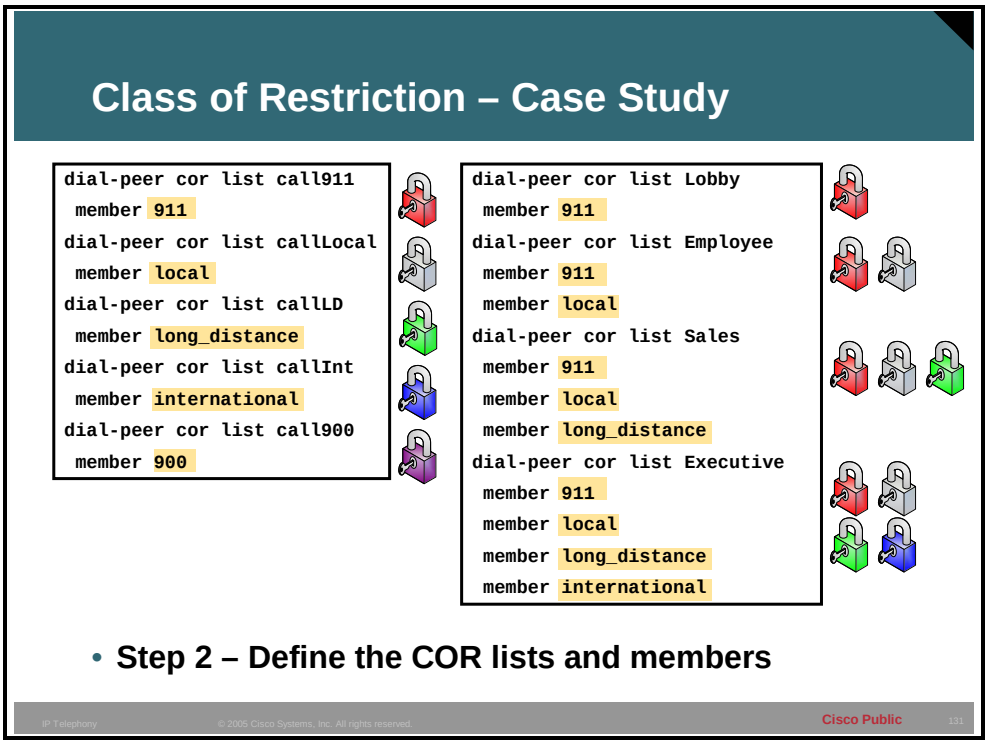
900

- **Step 1 - Define the classes of restriction**

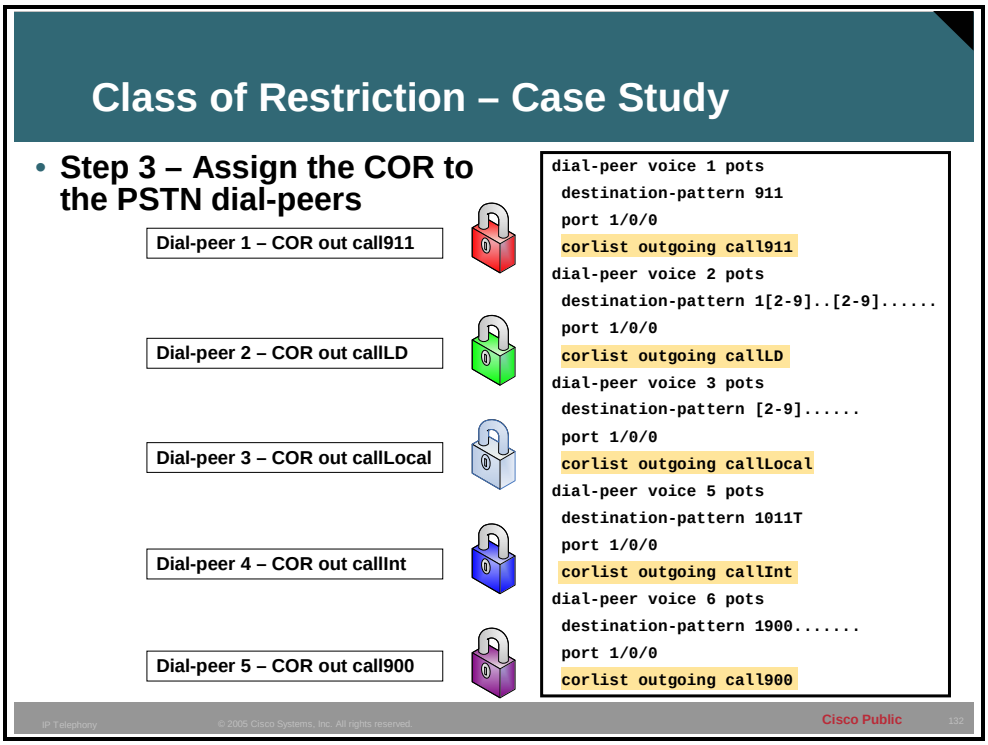
© 2005 Cisco Systems, Inc. All rights reserved.

Step 1 The first step will be to define the COR names.

Copyright © 2005, Cisco Systems, Inc.

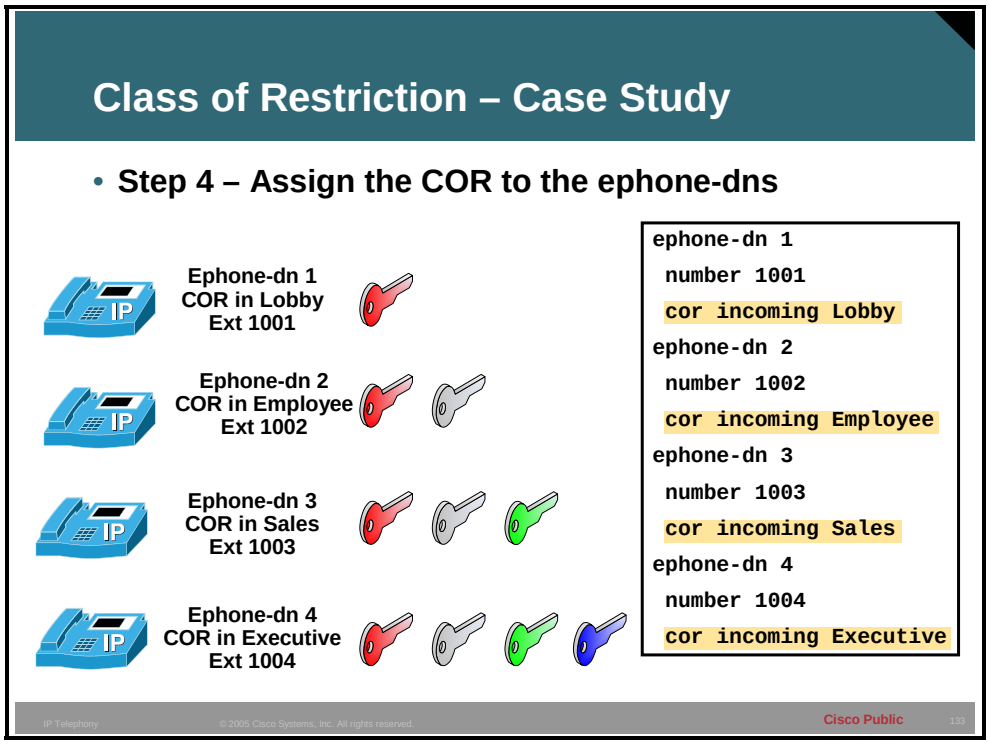


Step 2 The second step will be to define the COR list and its member or members. Notice that none of the COR lists contain the member 900.



Step 3 Assign the COR to the dial peers that govern PSTN access. To restrict calls to the PSTN destinations, the outbound COR setting will be defined.

Note Although not shown here, the inbound COR can be set to regulate where calls arriving from the PSTN will be allowed to connect internally.



Step 4 Assign the incoming COR to the Lobby, Employee, Sales, and Executive ephone-dns. Notice that no ephone-dn has the ability to call 900 numbers.

 Copyright © 2005, Cisco Systems, Inc.

Class of Restriction – Case Study

Results:

- **The Lobby ephone-dn can only call 911 on the PSTN**
- **The Employee ephone-dn can call 911 and local calls on the PSTN**
- **The Sales ephone-dn can call 911, local calls, and long distance on the PSTN**
- **The Executive ephone-dn can call 911, local calls, long distance, and international on the PSTN**
- **No one can call 900 numbers**



Ephone-dn 1
COR in Lobby
Ext 1001



Ephone-dn 2
COR in Employee
Ext 1002



Ephone-dn 3
COR in Sales
Ext 1003



Ephone-dn 4
COR in Executive
Ext 1004

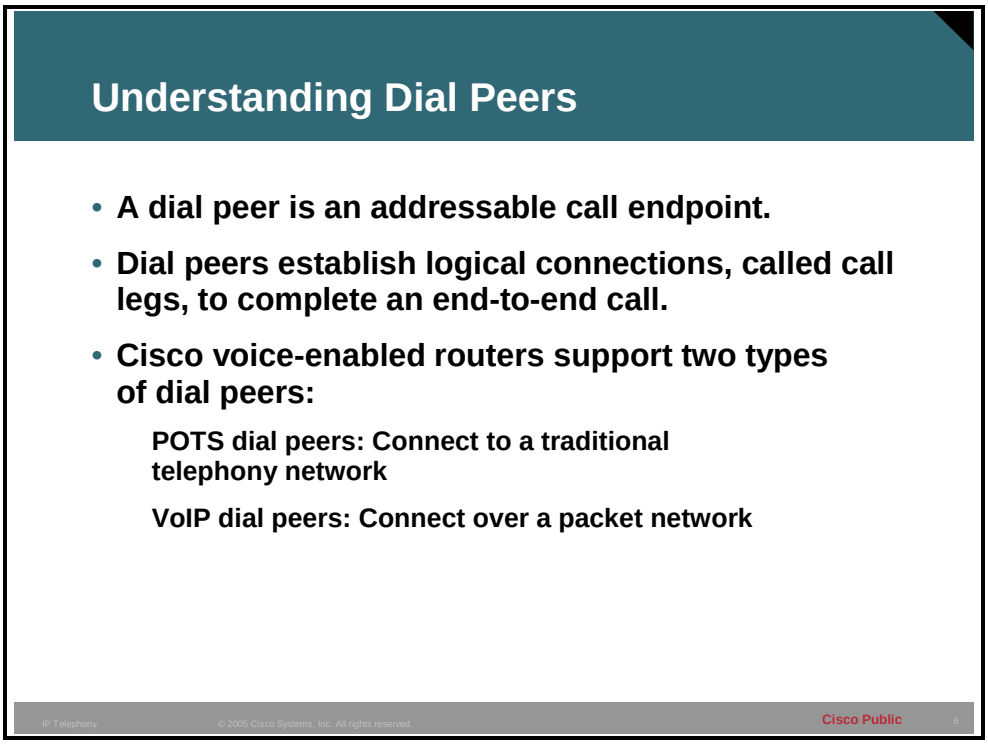
IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 134

The result of the configuration is shown.

Configuring Dial Peers

Understanding Dial Peers

This topic describes dial peers and their applications.



When a call is placed, an edge device generates dialed digits as a way of signaling where the call should terminate. When these digits enter a router voice port, the router must have a way to decide whether the call can be routed, and where the call can be sent. The router does this by looking through a list of dial peers.

A dial peer is an addressable call endpoint. The address is called a *destination pattern* and is configured in every dial peer. Destination patterns can point to one telephone number only or to a range of telephone numbers. Destination patterns use both explicit digits and wildcard variables to define a telephone number or range of numbers.

The router uses dial peers to establish logical connections. These logical connections, known as call legs, are established in either an inbound or outbound direction.

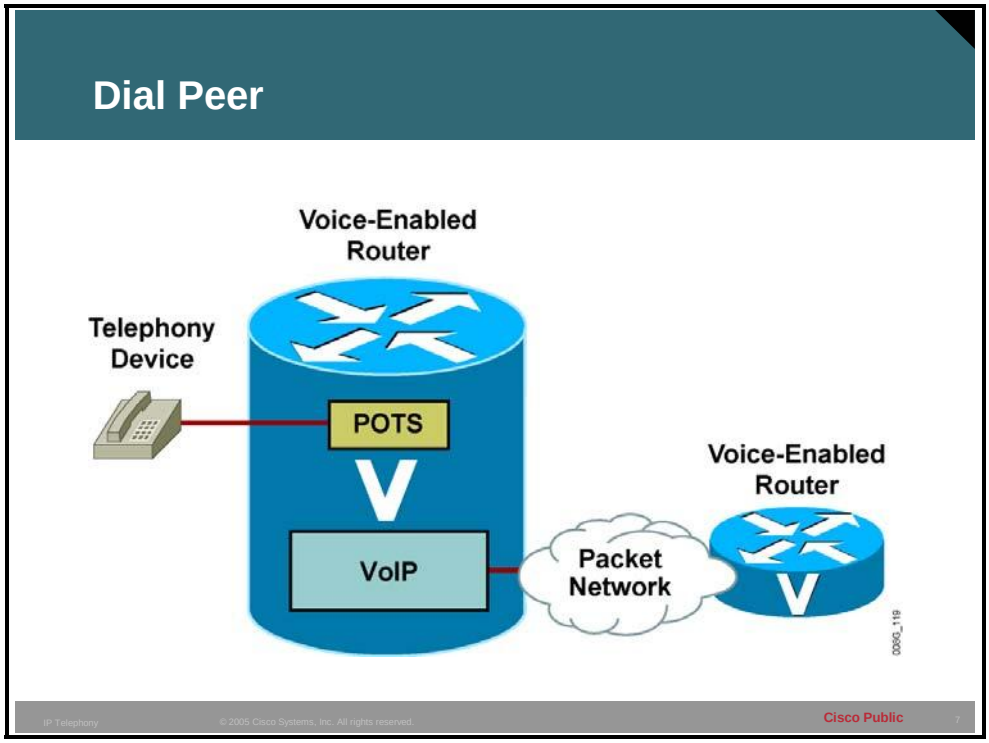
Dial peers define the parameters for the calls that they match; for example, if a call is originating and terminating at the same site, and is not crossing through slow-speed WAN links, then the call can cross the local network uncompressed and without special priority. A call that originates locally and crosses the WAN link to a remote site may require compression with a specific coder-decoder (codec). In addition, this call may require that voice activity detection (VAD) be turned on, and will need to receive preferential treatment by specifying a higher priority level.

Cisco Systems voice-enabled routers support two types of dial peers:

- **POTS dial peers:** Connect to a traditional telephony network, such as the public switched telephone network (PSTN) or a PBX, or to a telephony edge device such as a telephone or fax machine. POTS dial peers perform these functions:
  - Provide an address (telephone number or range of numbers) for the edge network or device
  - Point to the specific voice port that connects the edge network or device
- **VoIP dial peers:** Connect over a packet network. VoIP dial peers perform these functions:
  - Provide a destination address (telephone number or range of numbers) for the edge device that is located across the network
  - Associate the destination address with the next-hop router or destination router, depending on the technology used

Example: Dial-Peer Configuration

This figure shows a dial-peer configuration.



In the figure, the telephony device connects to the Cisco Systems voice-enabled router. The POTS dial-peer configuration includes the telephone number of the telephony device and the voice port to which it is attached. The router knows where to forward incoming calls for that telephone number.

The Cisco voice-enabled router VoIP dial peer is connected to the packet network. The VoIP dial-peer configuration includes the destination telephone number (or range of numbers) and the next-hop or destination voice-enabled router network address.

Follow these steps to place a VoIP call:

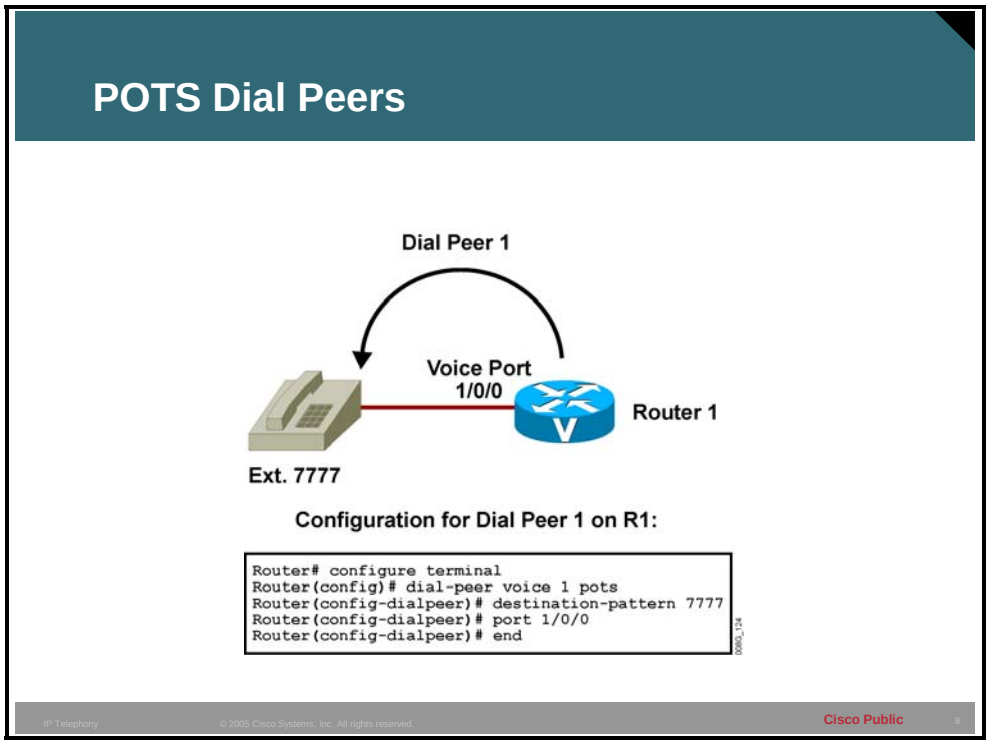
 Copyright © 2005, Cisco Systems, Inc.

How to Place a VoIP Call

Step	Action
1.	Configure the source router with a compatible dial peer that specifies the recipient destination address.
2.	Configure the recipient router with a POTS dial peer that specifies which voice port the router uses to forward the voice call.

Configuring POTS Dial Peers

This topic describes how to configure POTS dial peers.



Before the configuration of Cisco IOS dial peers can begin, the user must have a good understanding of where the edge devices reside, what type of connections need to be made between these devices, and what telephone numbering scheme is applied to the devices.

Follow these steps to configure POTS dial peers:

How to Configure POTS Dial Peers

Step	Action
1.	Configure a POTS dial peer at each router or gateway where edge telephony devices connect to the network.
2.	Use the **destination-pattern** command in the dial peer to configure the telephone number.
3.	Use the **port** command to specify the physical voice port that the POTS telephone is connected to.

The dial-peer type will be specified as POTS because the edge device is directly connected to a voice port and the signaling must be sent from this port to reach the device. There are two basic parameters that need to be specified for the device: the telephone number and the voice port. When a PBX is connecting to the voice port, a range of telephone numbers can be specified.

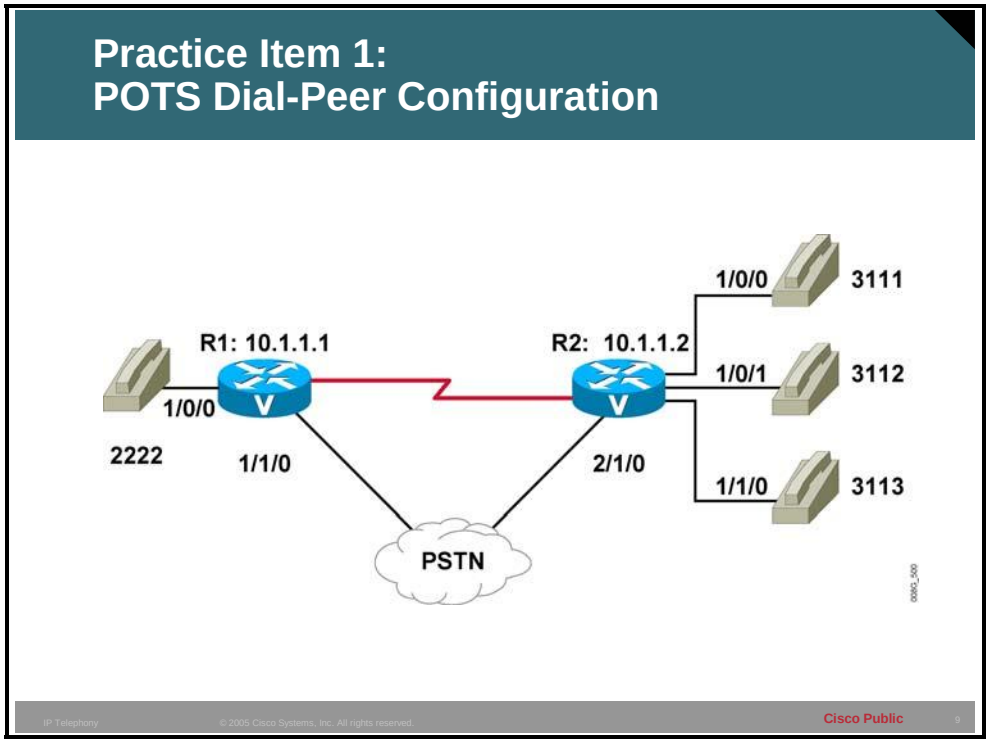
 Copyright © 2005, Cisco Systems, Inc.

Example: POTS Dial-Peer Configuration

The figure illustrates proper POTS dial-peer configuration on a Cisco voice-enabled router. The **dial-peer voice 1 pots** command notifies the router that dial peer 1 is a POTS dial peer with a tag of 1. The **destination-pattern 7777** command notifies the router that the attached telephony device terminates calls destined for telephone number 7777. The **port 1/0/0** command notifies the router that the telephony device is plugged into module 1, voice interface card (VIC) slot 0, voice port 0.

Practice Item 1: POTS Dial-Peer Configuration

Throughout this lesson, you will use practice items to practice what you have learned. In this scenario, assume that there is a data center at the R1 site, and executive offices at the R2 site. Using the diagram, create POTS dial peers for the four telephones shown.



R1

_____

_____

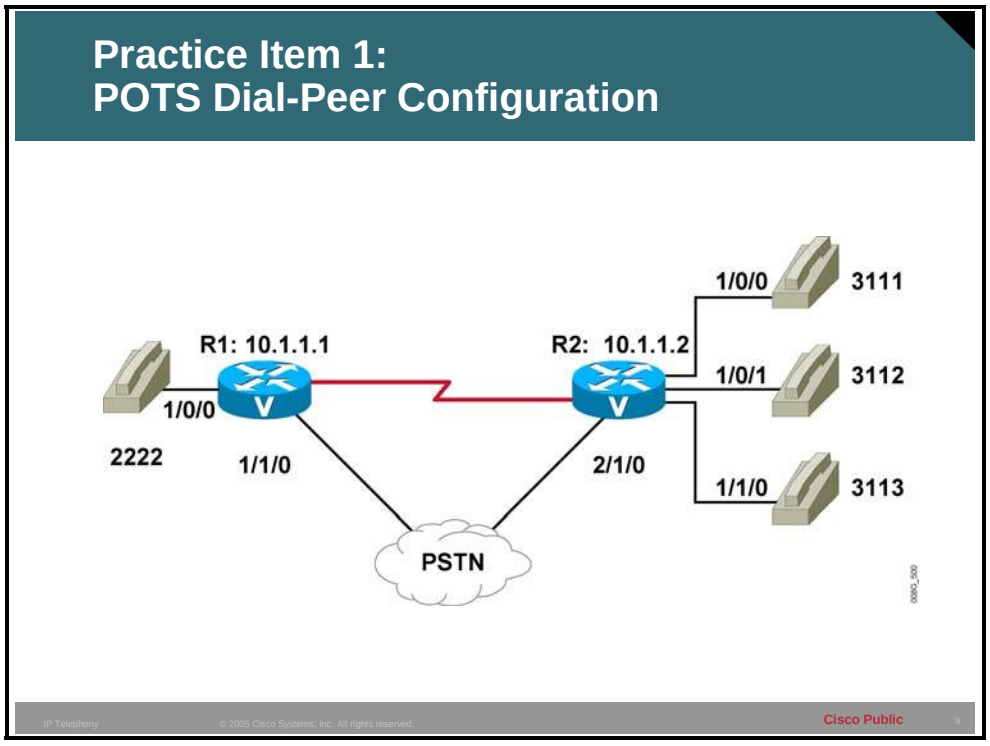
_____

 Copyright © 2005, Cisco Systems, Inc.

R2

Configuring VoIP Dial Peers

This topic describes how to configure VoIP dial peers.



The administrator must know how to identify the far-end voice-enabled device that will terminate the call. In a small network environment, the device may be the IP address of the remote device. In a large environment, identifying the device may mean pointing to a Cisco CallManager or gatekeeper for address resolution and Call Admission Control (CAC) to complete the call.

You must follow these steps to configure VoIP dial peers:

How to Configure VoIP Dial Peers

Step	Action
1.	Configure the path across the network for voice data.
2.	Specify the dial peer as a VoIP dial peer.
3.	Use the **destination-pattern** command to configure a range of numbers reachable by the remote router or gateway.
4.	Use the **session target** command to specify an IP address of the terminating router or gateway.
5.	Use the remote device loopback address as the IP address.

The dial peer is specified as a VoIP dial peer, which alerts the router that it must process a call according to the various parameters that are specified in the dial peer. The dial peer must then package it as an IP packet for transport across the network. Specified parameters may include the codec used for compression (VAD, for example), or marking the packet for priority service.

 Copyright © 2005, Cisco Systems, Inc.

The **destination-pattern** parameter configured for this dial peer is typically a range of numbers that are reachable via the remote router or gateway.

Because this dial peer points to a device across the network, the router needs a destination IP address to put in the IP packet. The **session target** parameter allows the administrator to specify either an IP address of the terminating router or gateway, or another device; for example, a gatekeeper or Cisco CallManager that can return an IP address of that remote terminating device.

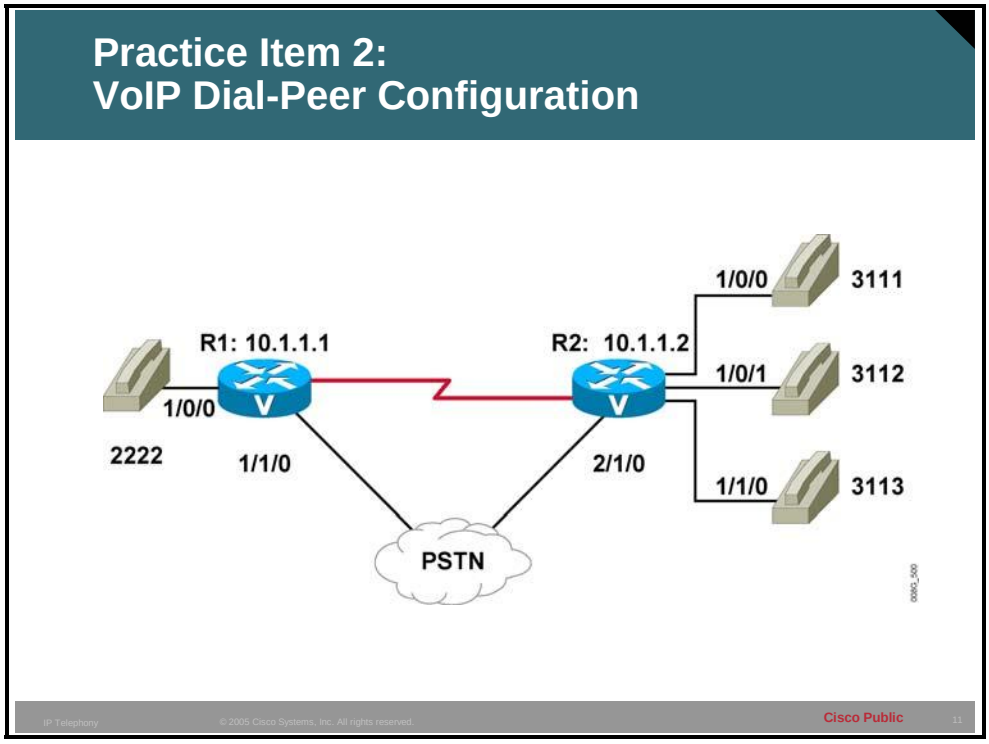
To determine which IP address a dial peer should point to, it is recommended that you use a loopback address. The loopback address is always up on a router, as long as the router is powered on and the interface is not administratively shut down. If an interface IP address is used instead of the loopback, and that interface goes down, the call will fail even if there is an alternate path to the router.

Example: VoIP Dial-Peer Configuration

The figure illustrates the proper VoIP dial-peer configuration on a Cisco voice-enabled router. The **dial-peer voice 2 voip** command notifies the router that dial peer 2 is a VoIP dial peer with a tag of 2. The **destination-pattern 8888** command notifies the router that this dial peer defines an IP voice path across the network for telephone number 8888. The **session target ipv4:10.18.0.1** command defines the IP address of the router that is connected to the remote telephony device.

Practice Item 2: VoIP Dial-Peer Configuration

Using the diagram, create VoIP dial peers for each of the R1 and R2 sites.



R1

_____

_____

_____

R2

_____

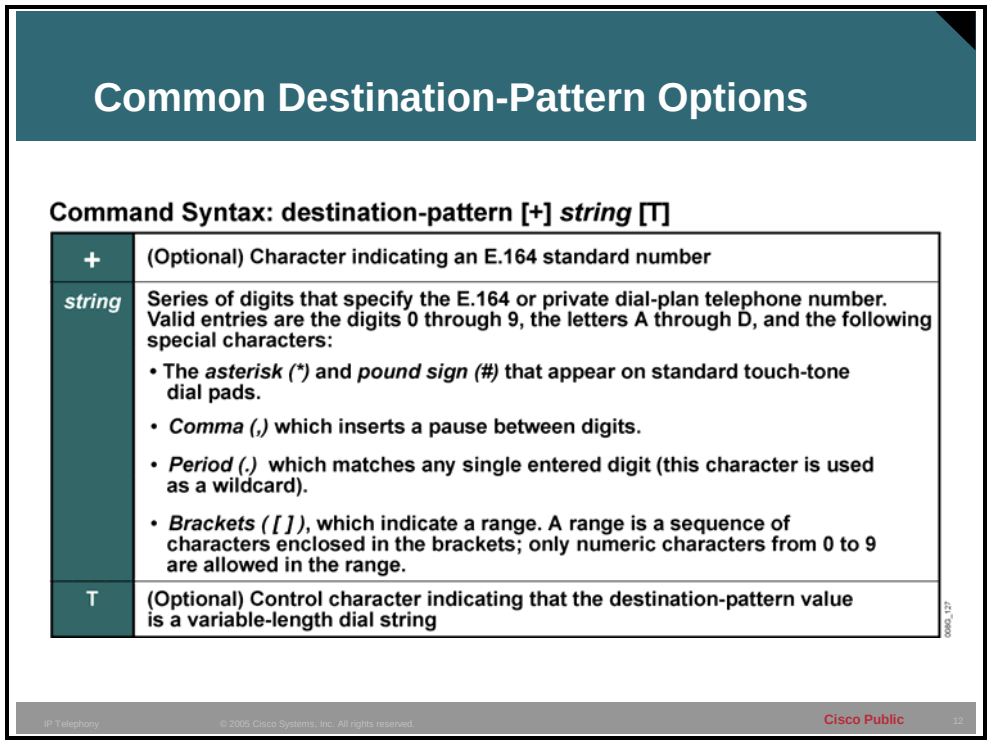
_____

_____

 Copyright © 2005, Cisco Systems, Inc.

Configuring Destination-Pattern Options

This topic describes destination-pattern options and the applicable shortcuts.



The destination pattern associates a telephone number with a given dial peer. The destination pattern also determines the dialed digits that the router collects and forwards to the remote telephony interface, such as a PBX, Cisco CallManager, or the PSTN. You must configure a destination pattern for each POTS and VoIP dial peer that you define on the router.

The destination pattern can indicate a complete telephone number, a partial telephone number with wildcard digits, or it can point to a range of numbers defined in a variety of ways.

Destination-pattern options include the following:

- **Plus sign (+):** An optional character that indicates an E.164 standard number. E.164 is the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) recommendation for the international public telecommunication numbering plan. The plus sign in front of a destination-pattern string specifies that the string must conform to E.164.
- ***string:*** A series of digits specifying the E.164 or private dial-plan telephone number. The examples below show the use of special characters that are often found in destination pattern strings:
  - An asterisk (*) and pound sign (#) appear on standard touch-tone dial pads. These characters may need to be used when passing a call to an automated application that requires these characters to signal the use of a special feature. For example, when calling an interactive voice response (IVR) system that requires a code for access, the number dialed might be “5551212888#”, which would initially dial the telephone number “5551212” and input a code of “888” followed by the pound key to terminate the IVR input query.

- A comma (,) inserts a one-second pause between digits. The comma can be used, for example, where a “9” is dialed to signal a PBX that the call should be processed by the PSTN. The “9” is followed by a comma to give the PBX time to open a call path to the PSTN, after which the remaining digits will be played out. An example of this string is “9,5551212”.
- A period (.) matches any single entered digit from 0 to 9, and is used as a wildcard. The wildcard can be used to specify a group of numbers that may be accessible via a single destination router, gateway, PBX, or Cisco CallManager. A pattern of “200.” allows for ten uniquely addressed devices, while a pattern of “20..” can point to 100 devices. If one site has the numbers 2000 through 2049, and another site has the numbers 2050 through 2099, then the bracket notation would be more efficient.
- Brackets ([ ]) indicate a range. A range is a sequence of characters that are enclosed in the brackets. Only single numeric characters from 0 to 9 are allowed in the range. In the previous example, the bracket notation could be used to specify exactly which range of numbers is accessible through each dial peer. For example, the first site pattern would be “20[0 – 4].”, and the second site pattern would be “20[5-9].”. Note that in both cases, a dot is used in the last digit position to represent any single digit from 0 to 9. The bracket notation offers much more flexibility in how numbers can be assigned.

- **T:** An optional control character indicating that the destination-pattern value is a variable-length dial string. In cases where callers may be dialing local, national, or international numbers, the destination pattern must provide for a variable-length dial plan. If a particular voice gateway has access to the PSTN for local calls and access to a transatlantic connection for international calls, then calls being routed to that gateway will have a varying number of dialed digits. A single dial peer with a destination pattern of ".T" could support the different call types. The interdigit timeout determines when a string of dialed digits is complete. The router continues to collect digits until there is an interdigit pause longer than the configured value, which by default is 10 seconds.

When the calling party finishes entering dialed digits, there is a pause equal to the interdigit timeout value *before* the router processes the call. The calling party can immediately terminate the interdigit timeout by entering the pound character (#), which is the default termination character. Because the default interdigit timer is set to 10 seconds, users may experience a long call setup delay.

Note	Cisco IOS software does not check the validity of the E.164 telephone number. It accepts any series of digits as a valid number.

 Copyright © 2005, Cisco Systems, Inc.

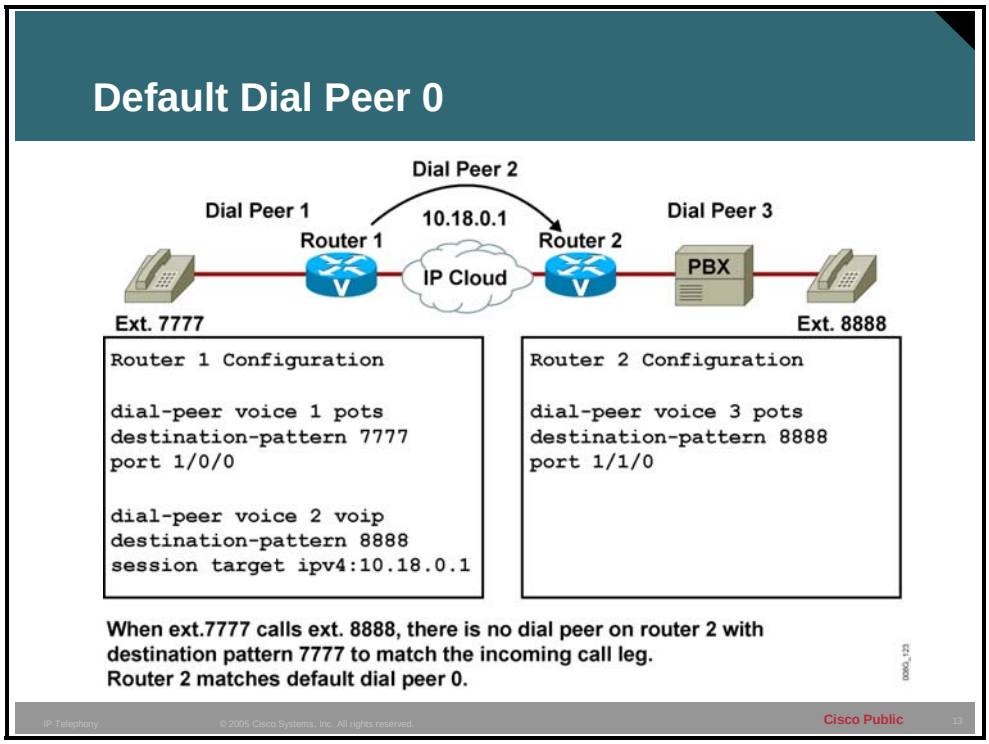
Example: Matching Destination Patterns

Destination-Pattern Options

Destination Pattern	Matching Telephone Numbers
5550124	Matches one telephone number exactly, 5550124. This is typically used when there is a single device, such as a telephone or fax, connected to a voice port.
55501[1-3].	Matches a seven-digit telephone number where the first five digits are 55501, the sixth digit can be a 1, 2, or 3, and the last digit can be any valid digit. This type of destination pattern is used when telephone number ranges are assigned to specific sites. In this example, the destination pattern is used in a small site that does not need more than 30 numbers assigned.
.T	Matches any telephone number that has at least one digit and can vary in length from 1 to 32 digits total. This destination pattern is used for a dial peer that services a variable-length dial plan, such as local, national, and international calls. It can also be used as a default destination pattern so that any calls that do not match a more specific pattern will match this pattern and can be directed to an operator.

Default Dial Peer

This topic describes the default dial peer.



When a matching inbound dial peer is not found, the router resorts to the default dial peer.

Note	Default dial peers are used for inbound matches only. They are not used to match outbound calls that do not have a dial peer configured.

The default dial peer is referred to as *dial peer 0*.

Example: Use of Default Dial Peer

In the figure, only one-way dialing is configured. The caller at extension 7777 can call extension 8888 because there is a VoIP dial peer configured on router 1 to route the call across the network. There is no VoIP dial peer configured on router 2 to point calls across the network toward router 1. Therefore, there is no dial peer on router 2 that will match the calling number of extension 7777 on the inbound call leg. If no incoming dial peer matches the calling number, the inbound call leg automatically matches to a default dial peer (POTS or VoIP).

Note	There is an exception to the previous statement. Cisco voice and dial platforms, such as the AS53*xx* and AS5800, require that a configured inbound dial peer be matched for incoming POTS calls to be accepted as voice calls. If there is no inbound dial-peer match, the call is treated and processed as a dialup (modem) call.

 Copyright © 2005, Cisco Systems, Inc.

Dial peer 0 for inbound VoIP peers has the following configuration:

- **any codec**
- **ip precedence 0**
- **vad enabled**
- **no rsvp support**
- **fax-rate service**

Dial peer 0 for inbound POTS peers has the following configuration:

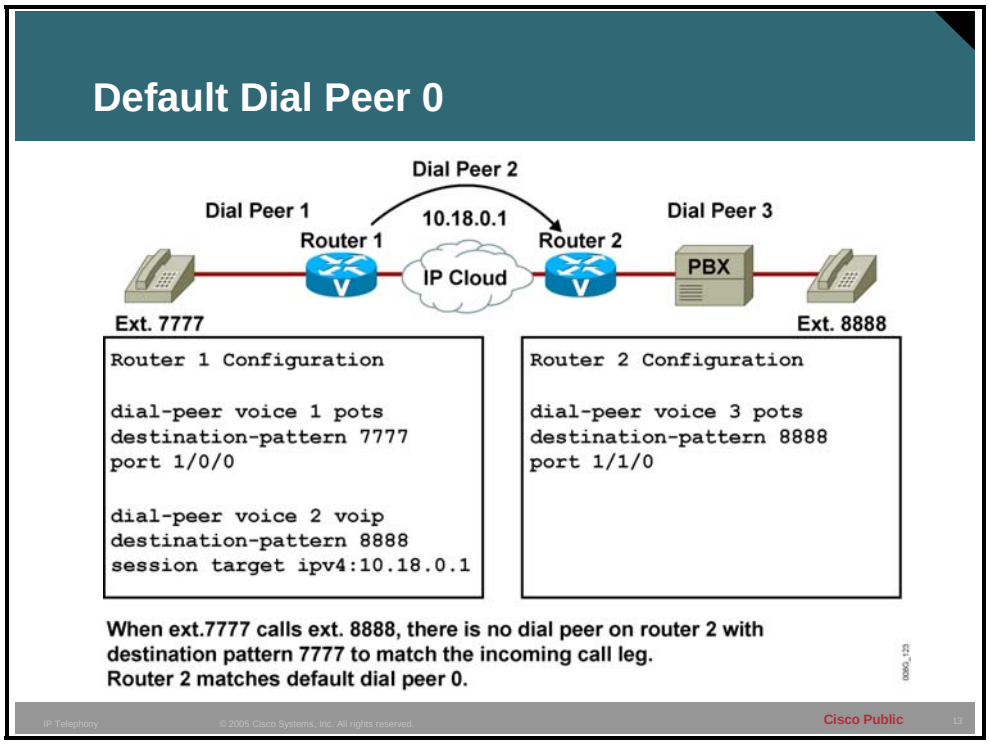
- **no ivr application**

You cannot change the default configuration for dial peer 0. Default dial peer 0 fails to negotiate nondefault capabilities or services. When the default dial peer is matched on a VoIP call, the call leg that is set up in the inbound direction uses any supported codec for voice compression, based on the requested codec capability coming from the source router. When a default dial peer is matched, the voice path in one direction may have different parameters than the voice in the return direction. This may cause one side of the connection to report good-quality voice while the other side reports poor-quality voice; for example, the outbound dial peer has VAD disabled, but the inbound call leg is matched against the default dial peer, which has VAD enabled. In this example, VAD is on in one direction and off in the return direction.

When the default dial peer is matched on an inbound POTS call leg, there is no default IVR application with the port. As a result, the user gets a dial tone and proceeds with dialed digits.

Matching Inbound Dial Peers

This topic describes how the router matches inbound dial peers.



When determining how inbound dial peers are matched on a router, it is important to note whether the inbound call leg is matched to a POTS or VoIP dial peer. Matching occurs in the following manner:

- Inbound POTS dial peers are associated with the incoming POTS call legs of the originating router or gateway.
- Inbound VoIP dial peers are associated with the incoming VoIP call legs of the terminating router or gateway.

Three information elements sent in the call setup message are matched against four configurable dial-peer command attributes.

 Copyright © 2005, Cisco Systems, Inc.

The table describes the three call setup information elements.

Call Setup Information Elements

Call Setup Element	Description
Called Number Dialed Number Identification Service	This is the call-destination dial string, and it is derived from the ISDN setup message or channel associated signaling Dialed Number Identification Service (DNIS).
Calling Number Automatic Number Identification	This is a number string that represents the origin, and it is derived from the ISDN setup message or channel associated signaling (CAS) automatic number identification (ANI). The ANI is also referred to as the calling line ID.
Voice Port	This represents the POTS physical voice port.

When the Cisco IOS router or gateway receives a call setup request, it makes a dial-peer match for the incoming call. This is not digit-by-digit matching; instead, the router uses the full digit string received in the setup request for matching against the configured dial peers.

The router or gateway matches call setup element parameters in the following order:

How the Router or Gateway Matches Inbound Dial Peers

Step	Action
1.	The router or gateway attempts to match the called number of the call setup request with the configured **incoming called-number** of each dial peer.
2.	If a match is not found, the router or gateway attempts to match the calling number of the call setup request with **answer-address** of each dial peer.
3.	If a match is not found, the router or gateway attempts to match the calling number of the call setup request to the **destination-pattern** of each dial peer.
4.	The voice port uses the voice port number associated with the incoming call setup request to match the inbound call leg to the configured dial peer **port** parameter.
5.	If multiple dial peers have the same port configured, then the router or gateway matches the first dial peer added to the configuration.
6.	If a match is not found in the previous steps, then the default is dial peer 0.

Because call setups always include DNIS information, it is recommended that you use the **incoming called-number** command for inbound dial-peer matching. Configuring **incoming called-number** is useful for a company that has a central call center providing support for a number of different products. Purchasers of each product get a unique 1-800 number to call for support. All support calls are routed to the same trunk group destined for the call center. When a call comes in, the computer telephony system uses the DNIS to flash the appropriate message on the computer screen of the agent to whom the call is routed. The agent will then know how to customize the greeting when answering the call.

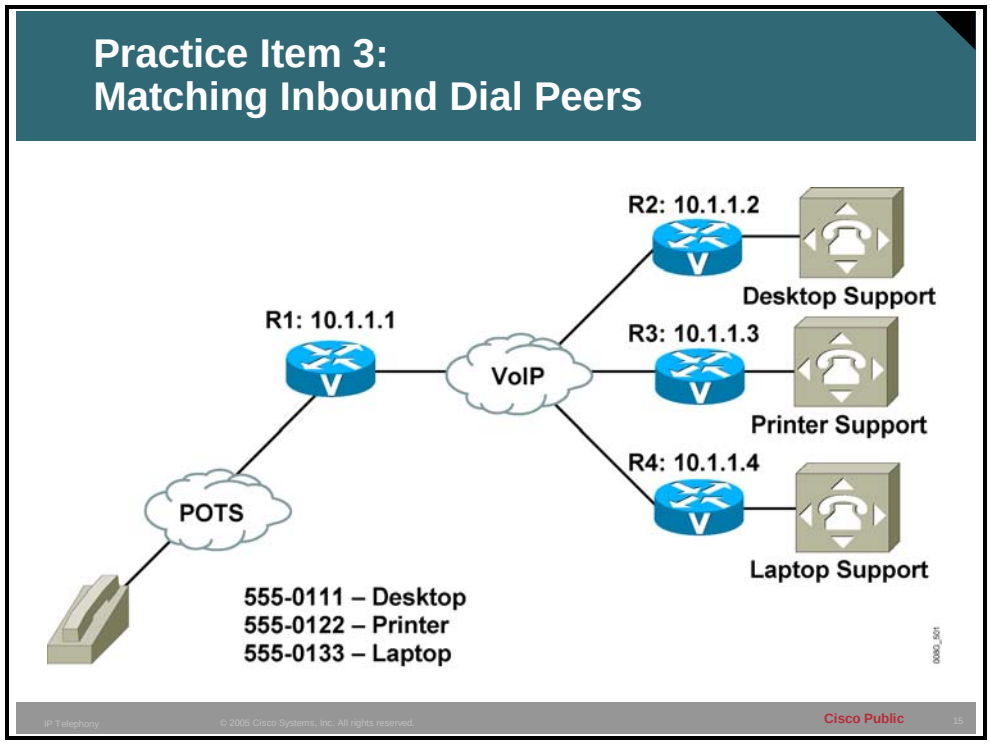
The calling number ANI with **answer-address** is useful when you want to match calls based on the originating calling number. For example, when a company has international customers who require foreign-language-speaking agents to answer the call, the call can be routed to the appropriate agent based on the country of call origin.

You must use the calling number ANI with **destination-pattern** when the dial peers are set up for two-way calling. In a corporate environment, the head office and the remote sites must be connected. As long as each site has a VoIP dial peer configured to point to each site, inbound calls from the remote site will match against that dial peer.

 Copyright © 2005, Cisco Systems, Inc.

Practice Item 3: Matching Inbound Dial Peers

In this practice item, assume that you are setting up a technical support center for desktop PCs, printers, and laptops. Customers who dial specific numbers reach the appropriate technical support staff. Using the diagram, create dial peers on R1 to route incoming calls per the incoming called number to the appropriate site.



R1

_____

_____

_____

_____

_____

_____

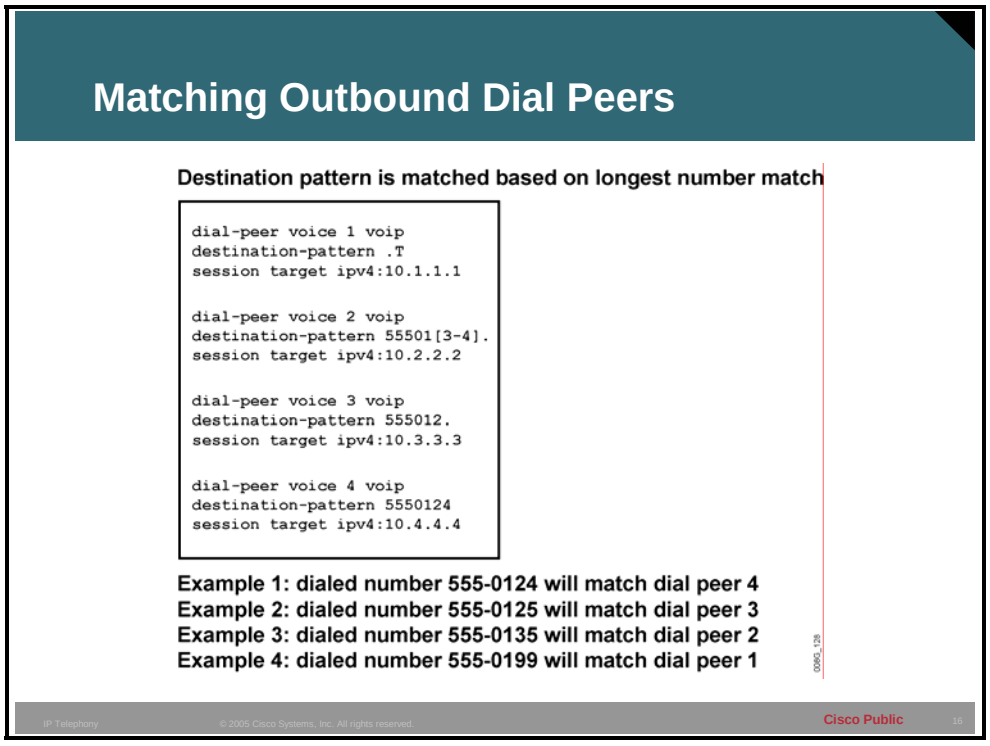
_____

_____

_____

Matching Outbound Dial Peers

This topic describes how the router matches outbound dial peers.



Outbound dial-peer matching is completed on a digit-by-digit basis. Therefore, the router or gateway checks for dial-peer matches after receiving each digit and then routes the call when a full match is made.

The router or gateway matches outbound dial peers in the following order:

How the Router or Gateway Matches Outbound Dial Peers

Step	Action
1.	The router or gateway uses the dial peer **destination-pattern** command to determine how to route the call.
2.	The **destination-pattern** command routes the call in the following manner: ■ On POTS dial peers, the **port** command forwards the call. ■ On VoIP dial peers, the **session target** command forwards the call.
3.	Use the **show dialplan number *string*** command to determine which dial peer is matched to a specific dialed string. This command displays all matching dial peers in the order that they are used.

Example: Matching Outbound Dial Peers

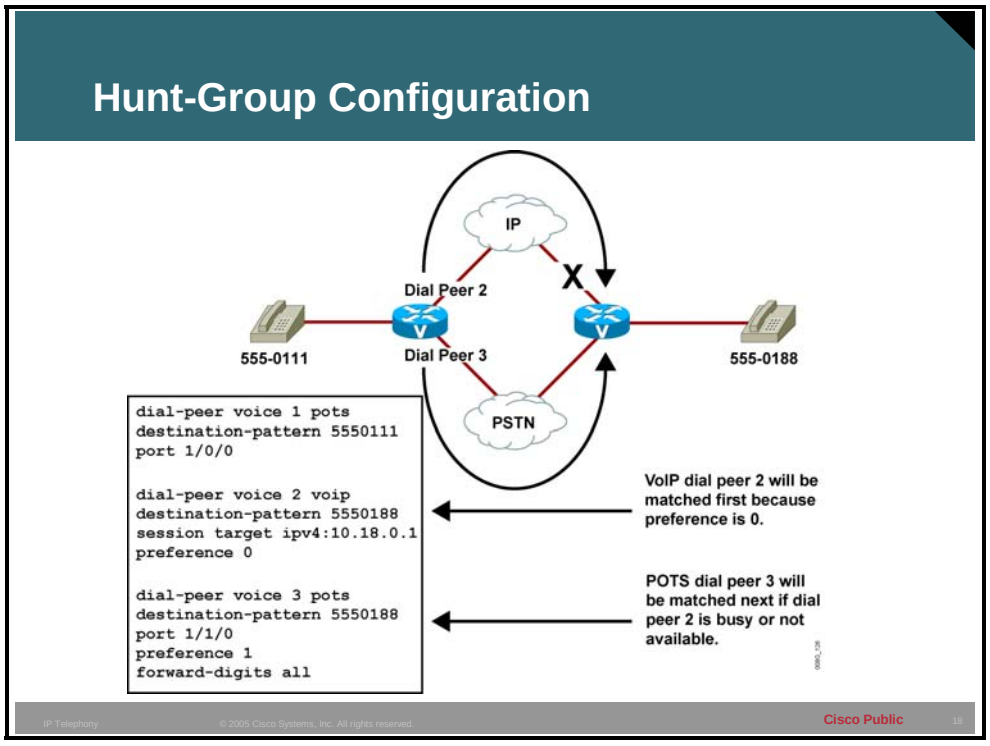
In the figure, dial peer 1 matches any digit string that has not matched other dial peers more specifically. Dial peer 2 matches any seven-digit number in the 30 and 40 range of numbers starting with 55501. Dial peer 3 matches any seven-digit number in the 20 range of numbers starting with 55501. Dial peer 4 matches the specific number 5550124 only. When the number

 Copyright © 2005, Cisco Systems, Inc.

5550124 is dialed, dial peers 1, 3, and 4 all match that number, but dial peer 4 places that call because it has the most specific destination pattern.

Hunt-Group Commands

This topic describes hunt-group commands.



Cisco voice-enabled routers support the concept of *hunt groups*, sometimes called *rotary groups*, in which multiple dial peers are configured with the same destination pattern. Because the destination of each POTS dial peer is a single voice port to a telephony interface, hunt groups help ensure that calls get through even when a specific voice port is busy. If the router is configured to hunt, it can forward a call to another voice port when one voice port is busy.

The following is a list of hunt-group commands:

- **preference:** Sets priority for dial peers. The destination with the lowest setting has the highest priority.
- **huntstop:** Disables dial-peer hunting on the dial peer.
- **dial-peer hunt:** Changes the default selection order for hunting through dial peers.

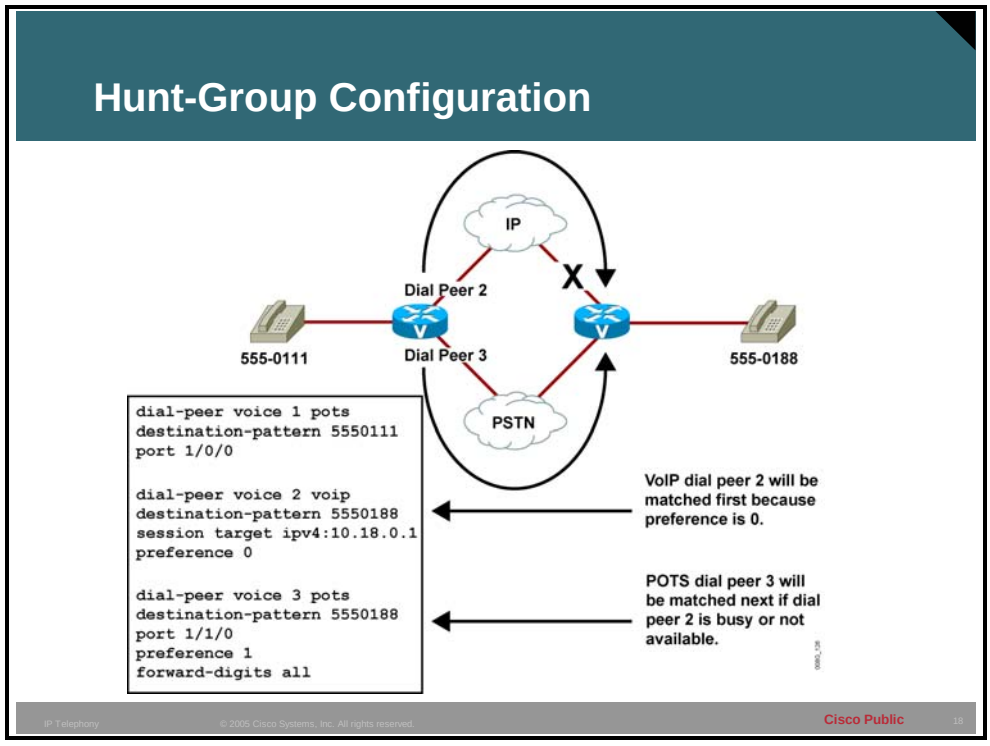
You can also use the following command to view dial-peer hunt current settings:

- **show dial-peer voice summary**: Shows the current settings for dial-peer hunt.

 Copyright © 2005, Cisco Systems, Inc.

Configuring Hunt Groups

This topic describes how to configure hunt groups.



In some business environments, such as call centers or sales departments, there may be a group of agents available to answer calls coming in to a single number. Scenario 1 may randomly distribute the calls between all agents. Scenario 2 may send calls to the senior agents first, and send calls to the junior agents only when all senior agents are busy. Both of these scenarios can be serviced by configuring a hunt group with specific commands to control the hunt actions.

Follow these steps to configure hunt groups:

How to Configure Hunt Groups

Step	Action
1.	Configure the same destination pattern across multiple dial peers.
2.	The destination pattern matches the greatest number of dialed digits.
3.	Use the **preference** command if the destination pattern of the dial peer is the same for several dial peers.
4.	If the preference does not act as the tiebreaker, then the router picks the matching dial peer randomly.

You must use the **dial-peer hunt** global configuration command to change the default selection order of the procedure or to choose different methods for hunting through dial peers. To view the current setting for **dial-peer hunt**, use the **show dial-peer voice summary** command.

If the desired action is not hunting through a range of dial peers, the **huntstop** command disables dial-peer hunting on the dial peer. After you enter this command, no further hunting is allowed if a call fails on the selected dial peer. This is useful in situations where it is undesirable to hunt to a less-specific dial peer if the more specific call fails; for example, if a call is destined for a particular staff member and the person is on the phone, the router searches for any other dial peer that may match the dialed number. If there is a more generic destination pattern in another dial peer that also matches, the call is routed to the generic destination pattern. If this is not the desired action, then configuring the **huntstop** command in the more specific dial peer will send the caller a busy signal.

You can mix POTS and VoIP dial peers when creating hunt groups. This is useful if you want incoming calls sent over the packet network; however, if that network connectivity fails, you want to reroute the calls back through the PBX, or through the router, to the PSTN.

By default, the router selects dial peers in a hunt group according to the following criteria, in the order listed:

How the Router Selects Dial Peers in a Hunt Group

Step	Action
1.	The router matches the most specific telephone number.
2.	The router matches according to the preference setting.
3.	The router matches randomly.

The destination pattern that matches the greatest number of dialed digits is the first dial peer selected by the router. For example, if one dial peer is configured with a dial string of “345….” and a second dial peer is configured with “3456789”, the router selects “3456789” first because it has the longest explicit match of the two dial peers. Without a PBX, if the line is currently in use, the desired action is to send a call to a voice-mail system or a secretary, instead of giving the caller a busy signal.

If the destination pattern is the same for several dial peers, you can configure the priority by using the **preference** dial-peer command. You would use the **preference** command to configure service for scenario 2, where the dial peers connecting to the senior agents would have the preference 0 and the dial peers connecting to the junior agents would have the preference 1. The lower the preference setting, the higher the priority for that dial peer to handle the call.

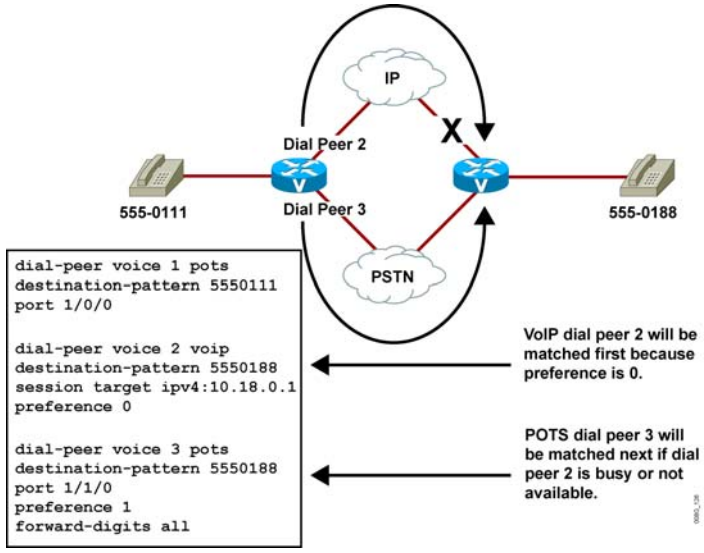
If all destination patterns are equal, by default, the preference is set to 0 on all dial peers. If the preference does not act as the tiebreaker, then a dial peer matching the called number will be picked randomly. This configuration would service scenario 1.

Example: Hunt-Group Application

The figure shows an example of configuring a hunt group to send calls to the PSTN if the IP network fails. For all calls going to 555-0188, VoIP dial peer 2 is matched first because the preference is set to zero. If the path through the IP network fails, POTS dial peer 3 is matched and the call is forwarded through the PSTN. The **forward-digits** command forwards all digits to the PSTN to automatically complete the call without a secondary dial tone.

 Copyright © 2005, Cisco Systems, Inc.

Hunt-Group Configuration




```
dial-peer voice 1 pots
destination-pattern 5550111
port 1/0/0

dial-peer voice 2 voip
destination-pattern 5550188
session target ipv4:10.18.0.1
preference 0

dial-peer voice 3 pots
destination-pattern 5550188
port 1/1/0
preference 1
forward-digits all
```

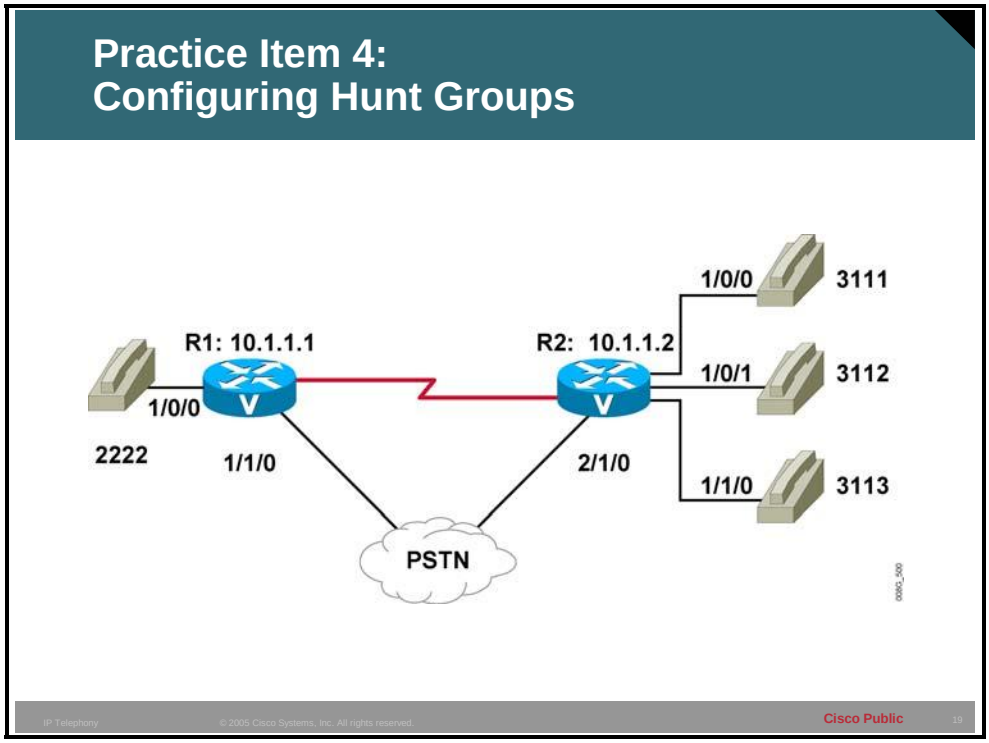
VoIP dial peer 2 will be matched first because preference is 0.

POTS dial peer 3 will be matched next if dial peer 2 is busy or not available.

IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 18

Practice Item 4: Configuring Hunt Groups

Using the diagram, configure a hunt group using the preference command on R2 such that if extension 3111 is busy, the call rings extension 3112. Assume that you have POTS dial peers for all three extensions already configured.



R2: Already configured

```
dial-peer voice 1 pots
destination-pattern 3111
port 1/0/0

dial-peer voice 2 pots
destination-pattern 3112
port 1/0/1

dial-peer voice 3 pots
destination-pattern 3113
port 1/1/0
```

R2: Hunt group dial peer

_____

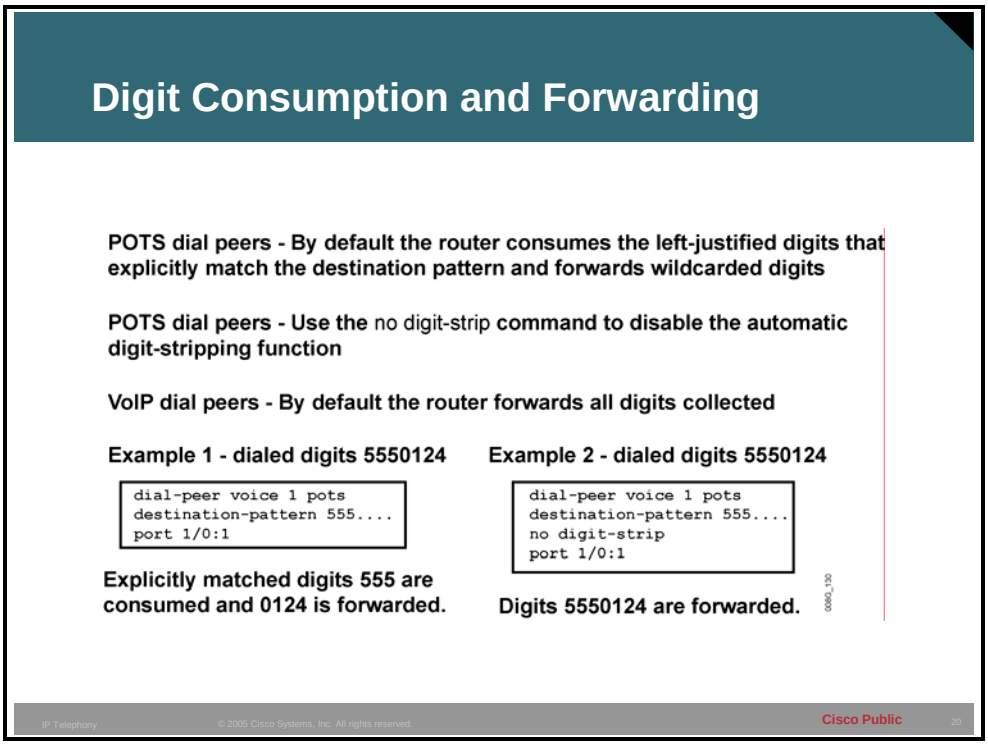
_____

_____

 Copyright © 2005, Cisco Systems, Inc.

Digit Collection and Consumption

This topic describes how the router collects and consumes digits and applies them to the dial-peer statements.

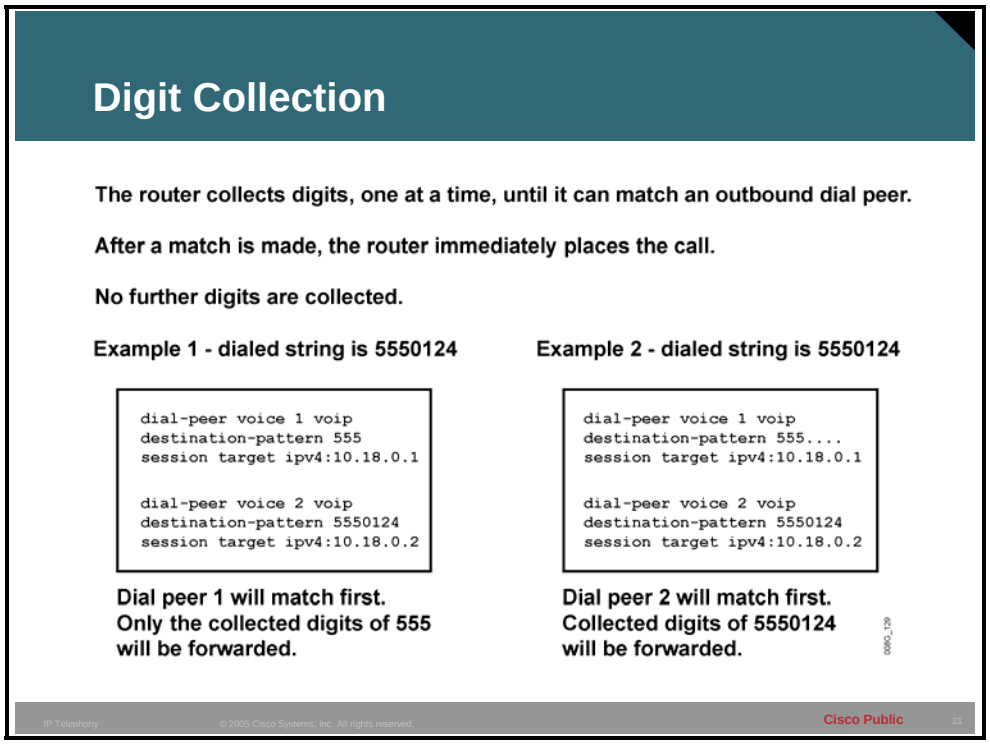


Use the **no digit-strip** command to disable the automatic digit-stripping function. This allows the router to match digits and pass them to the telephony interface.

By default, when the terminating router matches a dial string to an outbound POTS dial peer, the router strips off the left-justified digits that explicitly match the destination pattern. The remaining digits, or *wildcard digits,* are forwarded to the telephony interface, which connects devices such as a PBX or the PSTN.

Digit stripping is the desired action in some situations. There is no need to forward digits out of a POTS dial peer if it is pointing to a Foreign Exchange Station (FXS) port that connects a telephone or fax machine. If digit stripping is turned off on this type of port, the user may hear tones after answering the call because any unconsumed and unmatched digits are passed through the voice path after the call is answered.

In other situations, where a PBX or the PSTN is connected through the POTS dial peer, digit stripping is not desired because these devices need additional digits to further direct the call. In these situations, the administrator must assess the number of digits that need to be forwarded for the remote device to correctly process the call. With a VoIP dial peer, all digits are passed across the network to the terminating voice-enabled router.



When a voice call enters the network, the router collects digits as follows:

How the Router Collects Digits

Step	Action
1.	The originating router collects dialed digits until it matches an outbound dial peer.
2.	The router immediately places the call and forwards the associated dial string.
3.	The router collects no additional dialed digits.

Example: Digit Collection

The figure demonstrates the impact that overlapping destination patterns have on the call-routing decision. In example 1, the destination pattern in dial peer 1 is a subset of the destination pattern in dial peer 2. Because the router matches one digit at a time against available dial peers, an exact match will always occur on dial peer 1, and dial peer 2 will never be matched.

In example 2, the length of the destination patterns in both dial peers is the same. Dial peer 2 has a more specific value than dial peer 1, so it will be matched first. If the path to IP address 10.18.0.2 is unavailable, dial peer 1 will be used.

Destination patterns are matched based on the longest explicit number match. Digits collected are dependant on the configured destination pattern. The table describes how different number combinations are matched and collected.

 Copyright © 2005, Cisco Systems, Inc.

Matching Destination Patterns

Dialed Digits	Destination Pattern	Dialed Digits Collected
5550124	5……	5550124
5550124	555….	5550124
5550124	555	555
5550124	555T	5550124

In the first row of the table, the destination pattern specifies a seven-digit string. The first digit must be a five, and the remaining six digits can be any valid digits. All seven digits must be entered before the destination pattern is matched.

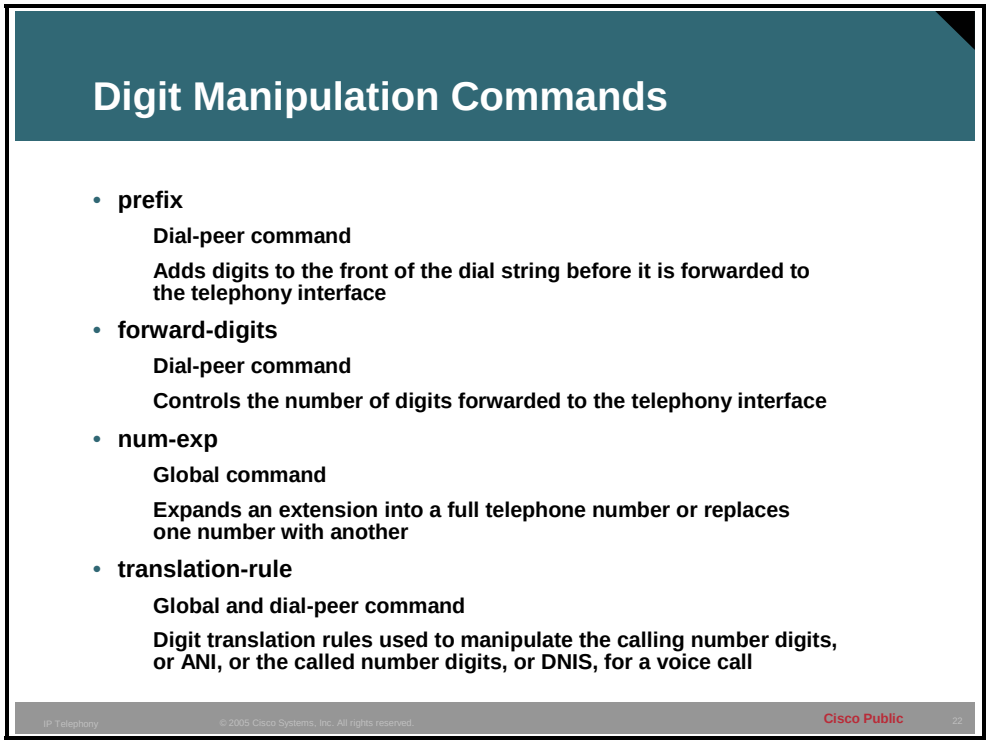
In the second row, the destination pattern specifies a seven-digit string. The first three digits must be 555, and the remaining four digits can be any valid digits. All seven digits must be entered before the destination pattern is matched.

In the third row, the destination pattern specifies a three-digit string. The dialed digits must be exactly 555. When the user begins to dial the seven-digit number, the destination pattern matches after the first three digits are entered. The router then stops collecting digits and places the call. If the call is set up quickly, the answering party at the other end may hear the remaining four digits as the user finishes dialing the string. After a call is set up, any dual tone multifrequency (DTMF) tones are sent through the voice path and played out at the other end.

In the last row, the destination pattern specifies a variable-length digit string that is at least three digits long. The first three digits must be exactly 555, and the remaining digits can be any valid digits. The “T” tells the router to continue collecting digits until the interdigit timer expires. The router stops collecting digits when the timer expires, or when the user presses the pound (#) key.

Understanding Digit Manipulation

This topic describes digit manipulation and the commands that are used to connect to a specified destination.



Digit manipulation is the task of adding or subtracting digits from the original dialed number to accommodate user dialing habits or gateway needs. The digits can be manipulated before matching an inbound or outbound dial peer. The following is a list of digit manipulation commands and their uses:

- **prefix:** This dial-peer command adds digits to the front of the dial string before it is forwarded to the telephony interface. This occurs after the outbound dial peer is matched, but before digits get sent out of the telephony interface. Use the **prefix** command when the dialed digits leaving the router must be changed from the dialed digits that had originally matched the dial peer; for example, a call is dialed using a four-digit extension such as 0123, but the call needs to be routed to the PSTN, which requires ten-digit dialing. If the four-digit extension matches the last four digits of the actual PSTN telephone number, then you can use the **prefix 902555** command to prepend the six additional digits needed for the PSTN to route the call to 902-555-0123. After the POTS dial peer is matched with the destination pattern of 0123, the **prefix** command prepends the additional digits, and the string “9025550123” is sent out of the voice port to the PSTN.
- **forward-digits:** This dial-peer command specifies the number of digits that must be forwarded to the telephony interface, regardless of whether they are explicitly matched or wildcard matched. This command occurs after the outbound dial peer is matched, but before the digits are sent out of the telephony interface. When a specific number of digits are configured for forwarding, the count is right justified. For example, if the POTS dial peer has a destination pattern configured to match all extensions in the 1000 range (**destination-pattern 1…**), by default, only the last three digits are forwarded to the PBX that is connected to the specified voice port. If the PBX needs all four digits to route the

 Copyright © 2005, Cisco Systems, Inc.

call, you must use the command **forward-digits 4**, or **forward-digits all**, so that the appropriate number of digits are forwarded. To restore the **forward-digits** command to its default setting, use the **default forward-digits** command. Using the **no forward-digits** command specifies that no digits are to be forwarded.

- **num-exp:** The **num-exp** global command expands an extension into a full telephone number or replaces one number with another. The number expansion table manipulates the called number. This command occurs before the outbound dial peer is matched; therefore, you must configure a dial peer with the expanded number in the destination pattern for the call to go through. The number expansion table is useful, for example, where the PSTN changes the dialing requirements from seven-digit dialing to ten-digit dialing. In this scenario, you can do one of the following:
  - Make all the users dial all ten digits to match the new POTS dial peer that is pointing to the PSTN.
  - Allow the users to continue dialing the seven-digit number as they have before, but expand the number to include the area code before the ten-digit outbound dial peer is matched.

Note You must use the **show num-exp** command to view the configured number-expansion table. You must use the **show dialplan number** *number* command to confirm the presence of a valid dial peer to match the newly expanded number.

- **translation-rule:** Digit translation is a two-step configuration process. First, the translation rule is defined at the global level. Then, the rule is applied at the dial-peer level either as inbound or outbound translation on either the called or calling number. Translation rules manipulate the ANI or DNIS digits for a voice call. Translation rules convert a telephone number into a different number before the call is matched to an inbound dial peer, or before the outbound dial peer forwards the call; for example, an employee may dial a five-digit extension to reach another employee of the same company at another site. If the call is routed through the PSTN to reach the other site, the originating gateway may use translation rules to convert the five-digit extension into the ten-digit format that is recognized by the central office (CO) switch.

You can also use translation rules to change the numbering type for a call. For example, some gateways may tag a number with more than 11 digits as an international number, even when the user must dial “9” to reach an outside line. In this case, the number that is tagged as an international number needs to be translated into a national number—without the 9—before it is sent to the PSTN.

As illustrated in this topic, there are numerous ways to manipulate digits at various stages of call completion. The administrator needs to determine which command will be most suitable and the requirements that are necessary for manipulation.

Note To test configured translation rules, you must use the **test translation** command.

Example: Using Digit Manipulation Tools

The following is a sample configuration using the **prefix** command:

```
dial-peer voice 1 pots
destination-pattern 555....
prefix 555
port 1/0/0
```

In the sample configuration using the **prefix** command, the device attached to port 1/0/0 needs all seven digits to process the call. On a POTS dial peer, only wildcard-matched digits are forwarded by default. Use the **prefix** command to send the prefix numbers 555 before forwarding the four wildcard-matched digits.

The following is a sample configuration using the **forward-digits** command:

```
dial-peer voice 1 pots
destination-pattern 555....
forward-digits 7
port 1/0/0
```

In the sample configuration using the **forward-digits** command, the device attached to port 1/0/0 needs all seven digits to process the call. On a POTS dial peer, only wildcard-matched digits are forwarded by default. The **forward-digits** command allows the user to specify the total number of digits to forward.

The following is a sample configuration using the number expansion table (**num-exp**) command:

```
num-exp 2... 5552...
dial-peer voice 1 pots
destination-pattern 5552...
port 1/1/0
```

In the sample configuration using the **num-exp** command, the extension number 2… is expanded to 5552… before an outbound dial peer is matched; for example, the user dials 2401, but the outbound dial peer 1 is configured to match 5552401.

The following is a sample configuration using the digit translation (**translation-rule**) command:

```
translation-rule 5
rule 1 2401 5552401
dial-peer voice 1 pots
translate-outgoing called-number 5
```

In the sample configuration using the **translation-rule** command, the rule is defined to translate 2401 into 5552401. The dial peer **translate-outgoing called-number 5** command notifies the router to use the globally defined translation rule 5 to translate the number before sending the string out the port. It is applied as an outbound translation from the POTS dial peer.

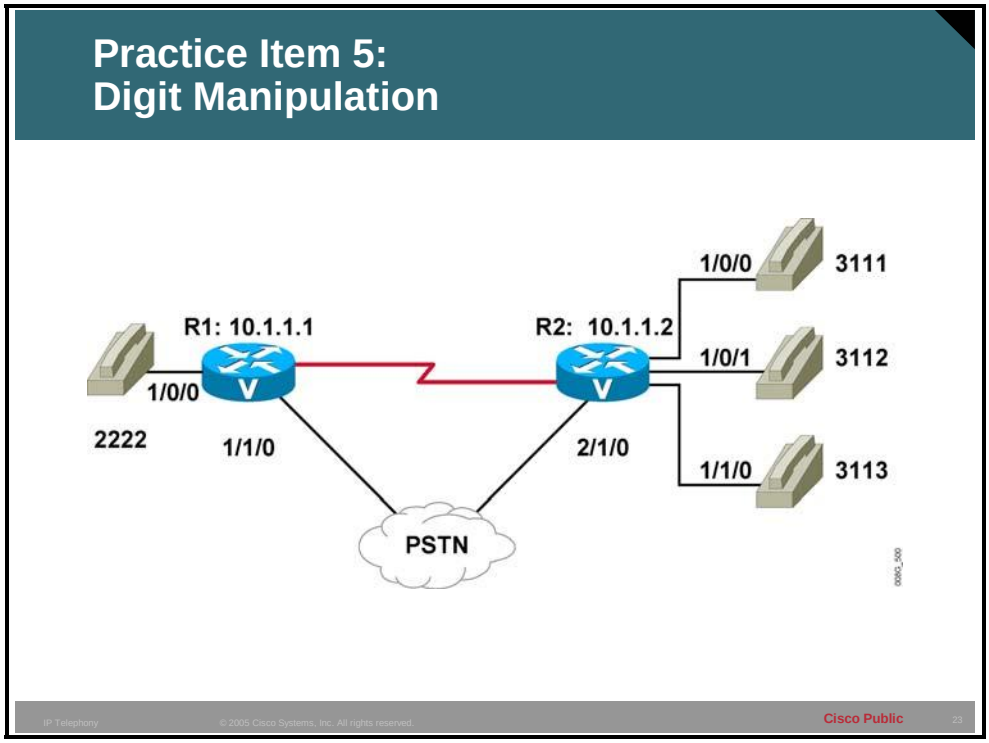
 Copyright © 2005, Cisco Systems, Inc.

The following example shows a translation rule that converts any called number that starts with 91 and is tagged as an international number into a national number without the 9 before sending it to the PSTN.

```
translation-rule 20
rule 1 91 1 international national
!
!
dial-peer voice 10 pots
destination-pattern 91.........
translate-outgoing called 20
port 1/1:5
forward-digits all
```

Practice Item 5: Digit Manipulation

Assuming that all POTS and VoIP dial peers are configured, create a dial peer to divert calls from R1 to R2 across the PSTN in the event of failure of the VoIP network. Assume that digits must be forwarded to the PSTN, and a prefix of 555 is necessary.



R1

_____

_____

_____

_____

_____

_____

 Copyright © 2005, Cisco Systems, Inc.

Practice Item Answer Key

Practice Item 1: POTS Dial Peers

R1:

```
dial-peer voice 1 pots
destination-pattern 2222
port 1/0/0
```

R2:

```
dial-peer voice 1 pots
destination-pattern 3111
port 1/0/0

dial-peer voice 2 pots
destination-pattern 3112
port 1/0/1

dial-peer voice 3 pots
destination-pattern 3113
port 1/1/0
```

Practice Item 2: VoIP Dial-Peer Configuration

R1:

```
dial-peer voice 101 voip
destination-pattern 3...
session target ipv4:10.1.1.2
```

R2:

```
dial-peer voice 101 voip
destination-pattern 2...
session target ipv4:10.1.1.1
```

Practice Item 3: Matching Inbound Dial Peers

R1:

```
dial-peer voice 202 voip
incoming called-number 5550111
session target ipv4:10.1.1.2

dial-peer voice 203 voip
incoming called-number 5550122
session target ipv4:10.1.1.3

dial-peer voice 204 voip
incoming called-number 5550133
session target ipv4:10.1.1.4
```

Practice Item 4: Configuring Hunt Groups

R2:

```
dial-peer voice 4 pots
destination-pattern 3111
port 1/0/1
preference 2
```

Practice Item 5: Digit Manipulation

R1:

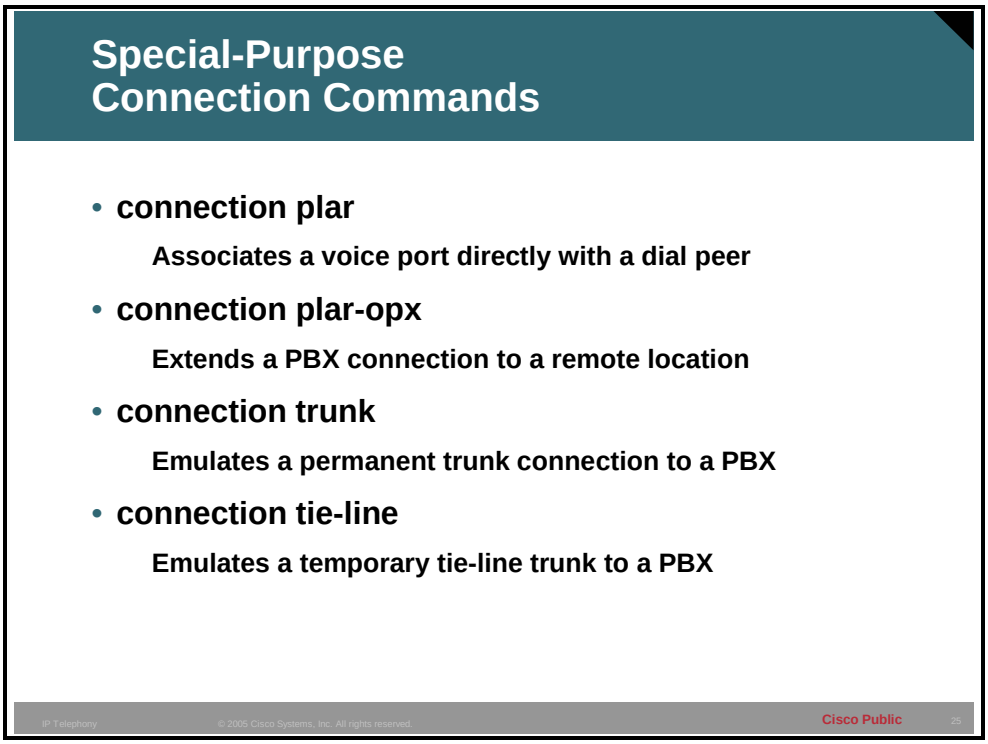
```
dial-peer voice 300 pots
destination-pattern 3...
port 1/1/0
forward-digits all
prefix 555
preference 2
```

 Copyright © 2005, Cisco Systems, Inc.

Special-Purpose Connections

Connection Commands

This topic identifies different special-purpose connection commands.



You can configure voice ports to support special connection requirements. These requirements usually reflect the needs of a specific business environment that must connect to the network in a special way. The following is a list of available connection commands and their application:

- **connection plar:** Private line, automatic ringdown (PLAR) is an autodialing mechanism that permanently associates a voice port with a far-end voice port, allowing call completion to a specific telephone number or PBX. When the calling telephone goes off hook, a predefined network dial peer is automatically matched, which sets up a call to the destination telephone or PBX. The caller does not hear a dial tone and does not have to dial a number. PLAR connections are widely used in the business world. One common use is to connect stockbrokers with trading floors. Timing is critical when dealing with stock transactions—the amount of time it may take to dial a number and get a connection can be costly in some cases. Another common use is in the travel sector, directly connecting travelers with services. Often, at places like airports, the traveler will see display boards advertising taxi companies, car rental companies, and local hotels. These displays often have telephones that will connect the traveler directly with the service of choice; the device is preconfigured with the telephone number of the desired service. One obvious difference between these telephones and a normal telephone is that they do not have a dial mechanism.
- **connection plar-opx:** Most frequently, a PLAR-Off Premises eXtension (OPX) is a PBX extension that is not located on the business site even though it operates as though it is

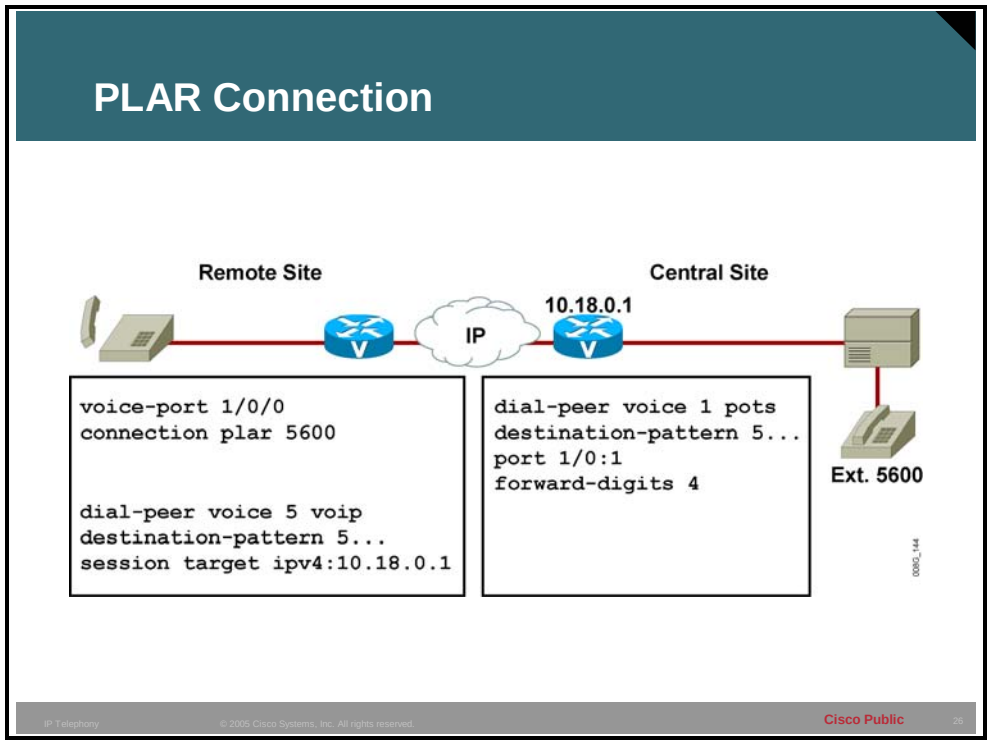
directly connected to the PBX. Company staff can dial an extension and reach the remote telephone as though it were on site. The remote telephone has access to PBX services such as voice mail and extension dialing. This functionality is most often used when onsite staff turns into telecommuters. Many companies are cutting back on office space in expensive locations and are setting up their staff with home offices. A PLAR-OPX connection is configured between the office and the remote site so that the telecommuter can continue to access all the corporate telephony services in the same manner as before. This allows the telecommuter to dial the same extensions to reach other staff, and to have access to long-distance dialing and other voice services via the same calling codes. From the office perspective, onsite staff can reach the telecommuter by dialing the same extension as before. One OPX connection feature is that when a call is being attempted, the voice-enabled router or gateway that takes the call from the PBX or Cisco CallManager will not report a call completion until the far end has answered the call. Without the OPX configuration, the PBX or Cisco CallManager passes the call to the local gateway or router. Then, the gateway or router routes the call to the PSTN. After the PSTN sends ringing to the telephone, the router will report call completion back to the PBX or Cisco CallManager. At this point, the call is completed. The problem is that if the call is not answered, there is no way to reroute the call to the corporate voice-mail server. From the PBX or Cisco CallManager perspective, the call is completed. When you configure the OPX, however, the gateway or router will not report call completion unless the telephone is actually answered.

- **connection trunk:** The **connection trunk** command specifies a connection that emulates a permanent trunk connection between two PBXs, a PBX and a local extension, or some combination of telephony interfaces with signaling passed transparently through the packet data network. A trunk connection remains permanent in the absence of active calls and is established immediately after configuration. The ports on either end of the connection are dedicated until you disable trunking for that connection. If, for some reason, the link between the two voice ports goes down, the virtual trunk reestablishes itself after the link comes back up. This configuration is useful when a permanent connection is desired between two devices. In this scenario, a caller at one end of the trunk connection can pick up the telephone and speak into it without dialing any digits or waiting for call setup. This is analogous to the red telephone to the Kremlin that is depicted in vintage movies. With a trunk connection, there is no digit manipulation performed by the gateway or router. Because this is a permanent connection, digit manipulation is not necessary.
- **connection tie-line:** The **connection tie**-line command specifies a connection that emulates a temporary tie-line trunk to a PBX. Although a tie-line connection is similar to a trunk connection, it is automatically set up for each call and torn down when the call ends. Another difference is that digits are added to the dial string *before* matching an outbound dial peer; for example, if a user were to dial extension 8000, which terminates at a remote office, the voice port is configured with an identifying number for that remote office. If that office ID is the number 7, then the digits that are sent to be matched against the outbound dial peer would be 78000. This new five-digit number would be carried across the network to the remote site. At the remote site, the number 7 can be stripped off or, if necessary, passed to the destination device.

 Copyright © 2005, Cisco Systems, Inc.

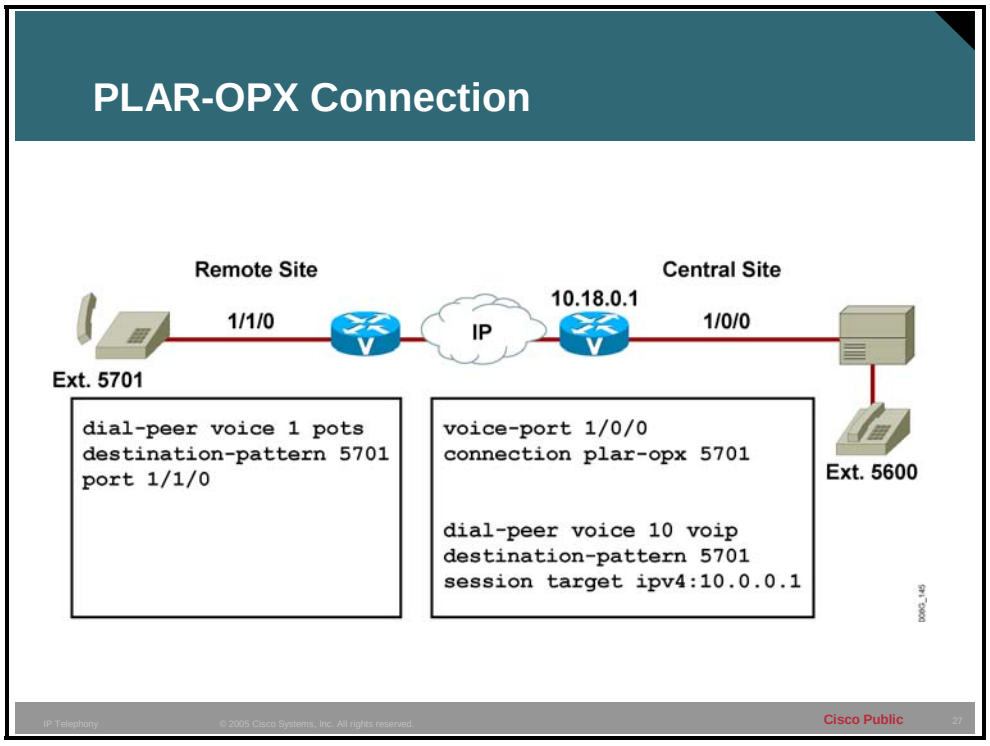
PLAR and PLAR-OPX

This topic describes the use of PLAR and PLAR-OPX connections.



As demonstrated in the figure, the following actions must occur to establish a PLAR connection:

1. A user at the remote site lifts the handset.
2. A voice port at the remote site router automatically generates digits 5600 for a dial-peer lookup.
3. The router at the remote site matches digits 5600 to VoIP dial peer 5 and sends the setup message with the digits 5600 to IP address 10.18.0.1 as designated in the **session target** statement.
4. The router at the central site matches received digits 5600 to POTS dial peer 1 and forwards digits 5600 out voice port 1/0:1. At the same time, it sends a call-complete setup message to the router at the remote site because both the inbound and outbound call legs on the central-site router were processed correctly.
5. The PBX receives digits 5600 and rings the appropriate telephone.



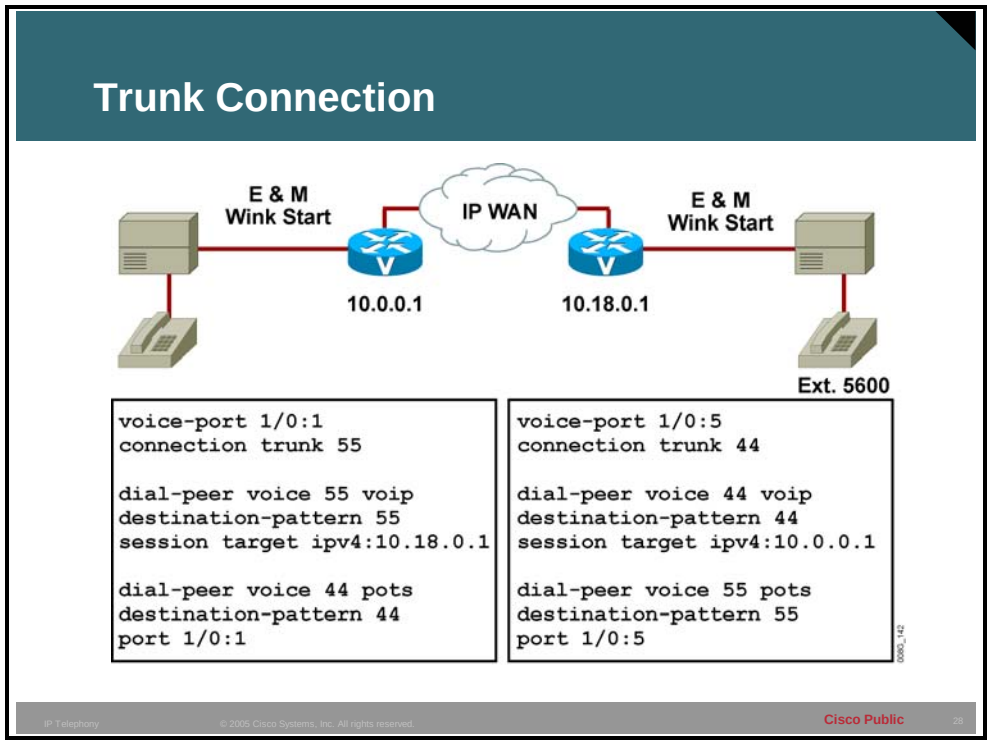
As demonstrated in the figure, the following actions must occur to establish a PLAR-OPX connection:

1. A user at the central site calls a user at a remote site using the extension 5701.
2. PBX routes the call to the central-site router port 1/0/0, which is configured for PLAR-OPX and pointing to extension 5701.
3. The central-site router matches VoIP dial peer 10 and sends a setup message to the corresponding IP address. In the meantime, port 1/0/0 does not respond immediately to the PBX with a seizure or off hook indication, but waits for the remote site call setup complete message.
4. After the remote router sends the call setup complete message, the central-site router sends a trunk seizure indication to the PBX and opens a voice path.

 Copyright © 2005, Cisco Systems, Inc.

Configuring Trunk Connections

This topic describes how to configure trunk connections.



As demonstrated in the figure, the following must occur to establish a trunk connection:

1. Use the **connection trunk** command to establish a two-way permanent connection between two voice ports across the IP network.
2. Configure the **connection trunk** parameter on the voice ports connecting the two PBXs and configure the session target for each IP address.

In the example, the router on the left is configured to set up a trunk connection from voice port 1/0:1 to a remote voice-enabled router with the IP address of 10.18.0.1 (the router on the right). This is done by specifying the same number in the **connection trunk** voice port command as in the appropriate dial peer **destination-pattern** command. In this example, the router on the left uses **connection trunk 55**, which matches VoIP dial peer 55. The call is routed to the router on the right, which matches the 55 in a POTS dial peer. The router on the right is also configured to set up a trunk connection from its voice port 1/0:5 to a remote voice-enabled router with the IP address of 10.0.0.1 (the router on the left). The router on the right uses 44 as its connection trunk number. These trunk connections are set up when the routers power on and remain up until the router is powered down or the ports are shut down.

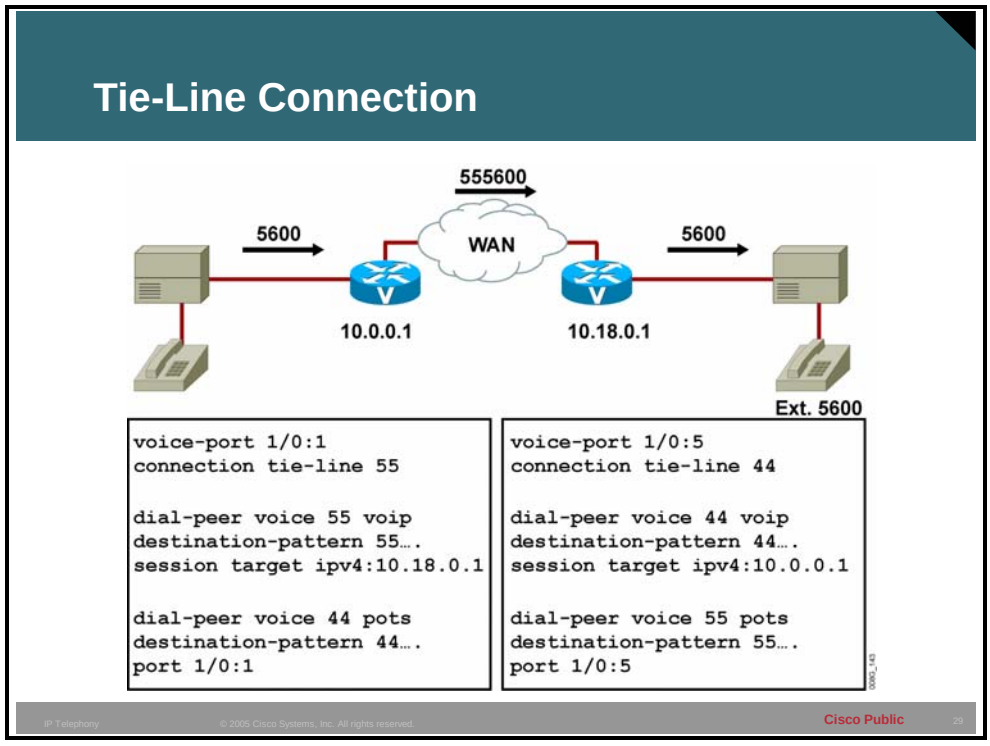
The following conditions must be met for VoIP to support virtual trunk connections:

- You must use the following voice port combinations:
  - recEive and transMit or ear and mouth (E&M) to E&M (same type)
  - FXS to Foreign Exchange Office (FXO)
  - FXS to FXS (with no signaling)
- You must not perform number expansion on the destination-pattern telephone numbers configured for trunk connection.
- You must configure both end routers for trunk connections.

 Copyright © 2005, Cisco Systems, Inc.

Tie-Line Connections

This topic describes the use and application of tie-lines.



In traditional telephony networks, companies often had dedicated circuits called tie-lines connecting two PBXs. This, in effect, allowed callers at one site to reach callers at the remote site only through that tie-line connection. Now that the IP network is replacing the traditional telephony connection, the two sites are logically "tied" together through the use of the **connection tie-line** command at both sites. Callers at one site can still reach callers at the remote site only, but the call goes over the IP network. The **connection tie-line** command emulates tie-lines between PBXs.

As demonstrated in the figure, you must complete the following procedure to establish a tie-line connection:

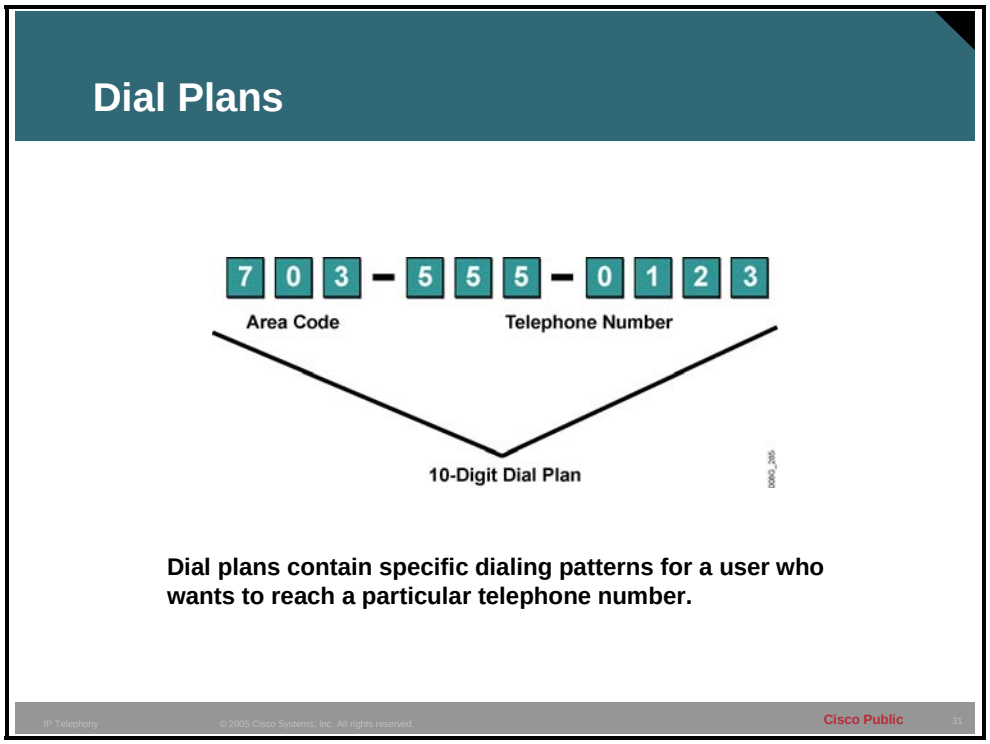
1. Use the **connection tie-line** command when the dial plan requires the addition of digits in front of any digits dialed by the PBX.
2. Use the combined set of digits to route the call onto the network.
3. The tie-line port waits to collect digits from the PBX.
4. The terminating router automatically strips the tie-line digits.

In the figure, the caller on the left picks up the telephone and dials the four-digit extension, 5600. Because the voice port on the left router is configured for **connection tie-line**, the router collects the four digits and prepends the tie-line digits "55" to make a six-digit number, 555600. That number is then matched to a VoIP dial peer and sent to the appropriate IP address. After the call reaches the far-end router, it is matched against a POTS dial peer with the destination pattern "55….". Because POTS dial peers, by default, forward only wildcard digits, only the four-digit extension 5600 is passed to the PBX.

Building a Scalable Numbering Plan

Scalable Numbering Plan

This topic describes the need for a scalable numbering plan in a VoIP network.



Although most people are not acquainted with dial plans by name, they use them daily.

Example: Dial Plan Implementations

The North American telephone network is designed around a 10-digit dial plan that consists of 3-digit area codes and 7-digit telephone numbers. For telephone numbers that are located within an area code, the PSTN uses a 7-digit dial plan. Features within a CO-based PBX, such as Centrex, allow the use of a custom 5-digit dial plan for customers who subscribe to that service. PBXs are more flexible and allow for variable-length dial plans containing 3 to 11 digits.

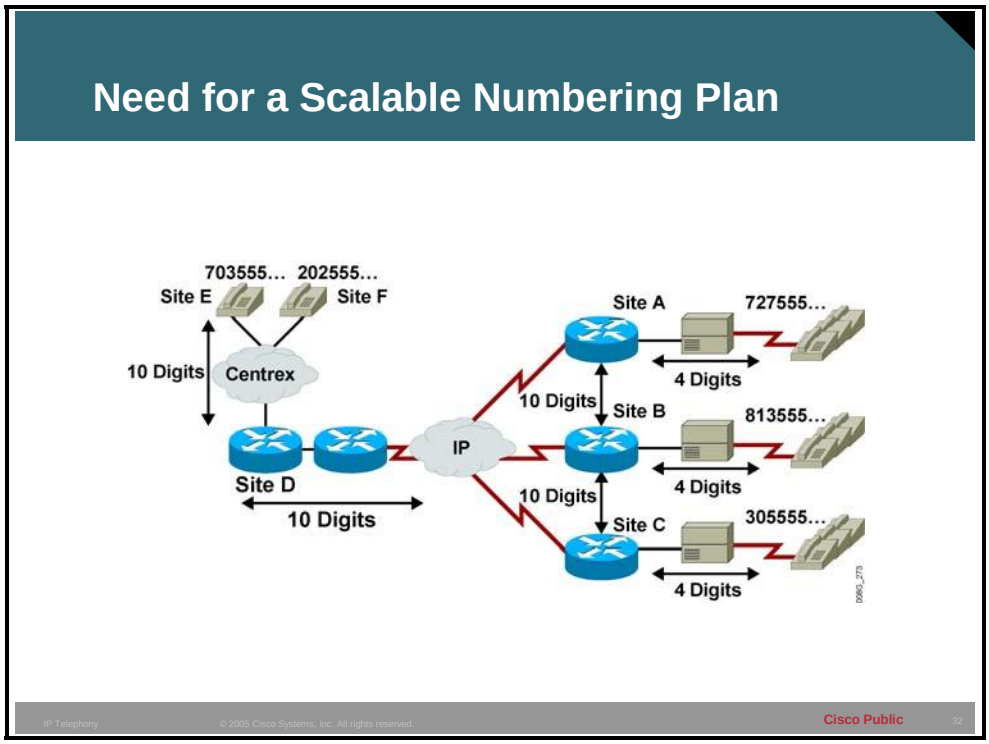
Dial plans contain specific dialing patterns for a user who wants to reach a particular telephone number. Dial plans also contain access codes, area codes, specialized codes, and combinations of the numbers of digits dialed.

Dial plans require knowledge of the customer network topology, current telephone number dialing patterns, proposed router and gateway locations, and traffic-routing requirements. If the dial plans are for a private internal voice network that is not accessed by the outside voice network, the telephone numbers can be any number of digits.

Typically, companies that implement VoIP networks carry voice traffic within the least expensive systems and paths. Implementing this type of system involves routing calls through IP networks, private trunks, PBXs, key systems, and the PSTN. The numbering plan to support

 Copyright © 2005, Cisco Systems, Inc.

the system is scalable, easily understood by the user, and transportable between all of the system components. The use of alternate path components reduces instances of call failure. Finally, the numbering plan conforms to all applicable standards and formats for all of the systems involved.

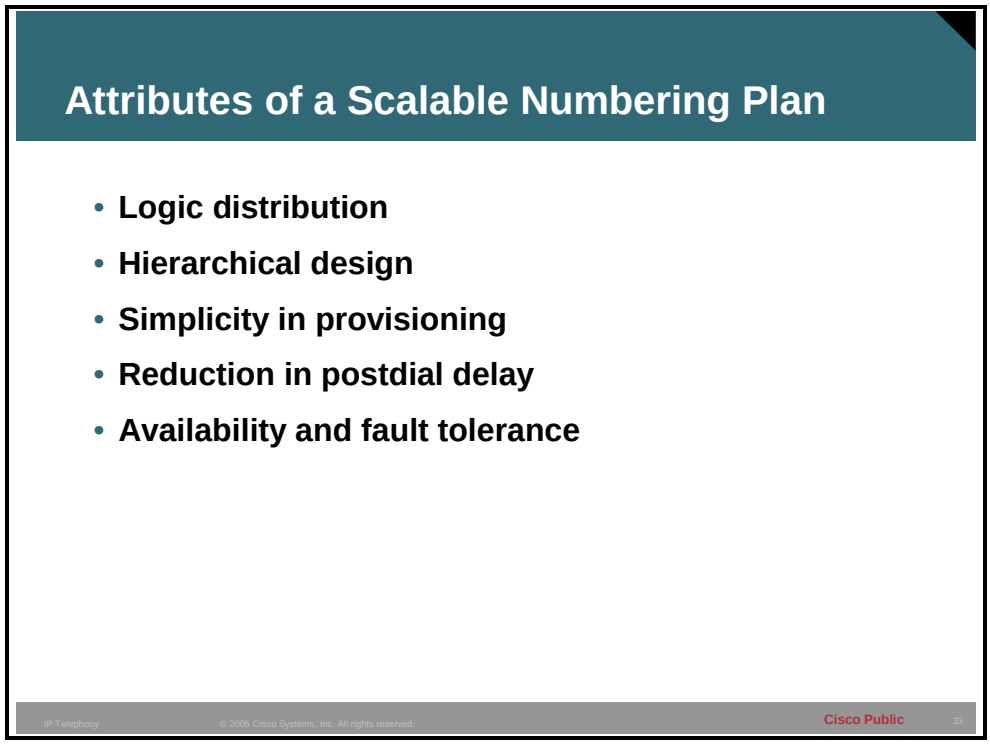


This figure illustrates a complex voice network that consists of the components discussed in this topic. A comprehensive and scalable numbering plan must be well-planned and well-implemented on networks such as this. The Centrex service requires 7-digit dialing between itself and site D; the IP network requires 7-digit dialing toward sites A, B, and C; and each of the PBXs requires 3-digit dialing.

 Copyright © 2005, Cisco Systems, Inc.

Scalable Numbering Plan Attributes

This topic describes the attributes of a scalable numbering plan.



When designing a large-scale numbering plan, you must adhere to the following attributes:

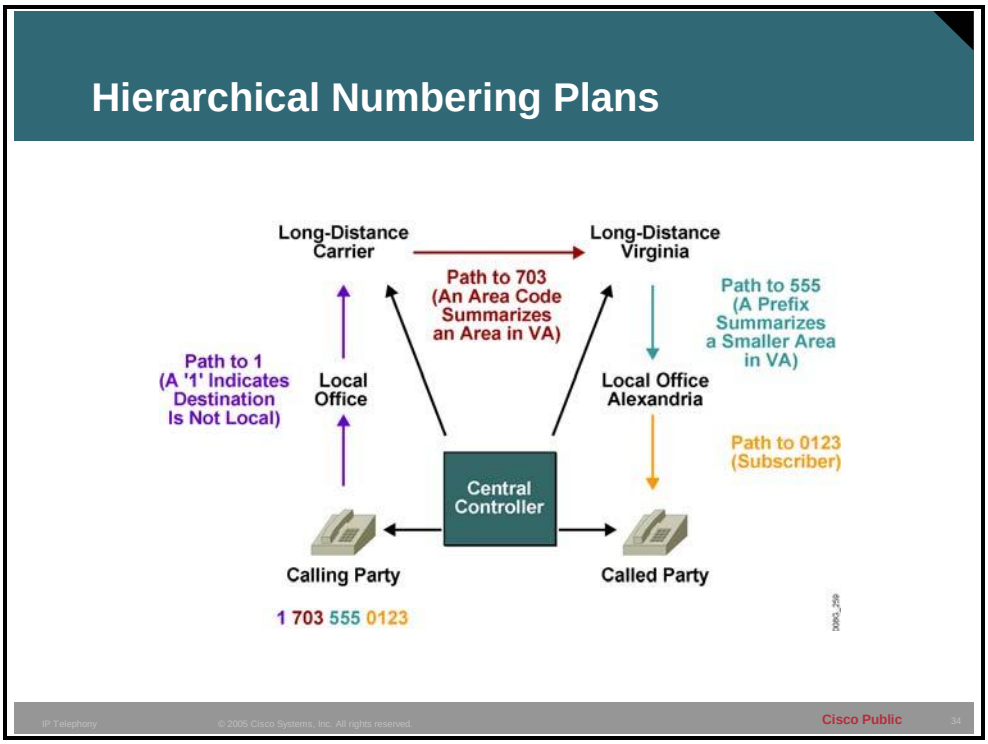
- **Logic distribution:** Good dial plan architecture relies on the effective distribution of the dial plan logic among the various components. Devices that are isolated to a specific portion of the dial plan reduce the complexity of the configuration. Each component focuses on a specific task accomplishment. Generally, the local switch or gateway handles details that are specific to the local point of presence (POP). Higher-level routing decisions are passed along to the gatekeepers and PBXs. A well-designed network places the majority of the dial plan logic at the gatekeeper devices.
- **Hierarchical design (scalability):** You must strive to keep the majority of the dial plan logic (routing decisions and failover) at the highest-component level. Maintaining a hierarchical design makes the addition and deletion of number groups more manageable. Scaling the overall network is much easier when configuration changes are made to a single component.
- **Simplicity in provisioning:** Keep the dial plan simple and symmetrical when designing a network. Try to keep consistent dial plans on the network by using translation rules to manipulate the local digit dialing patterns. These number patterns are normalized into a standard format or pattern before the digits enter the VoIP core. Putting digits into a standard format simplifies provisioning and dial-peer management.

- **Reduction in postdial delay:** Consider the effects of postdial delay in the network when you design a large-scale dial plan. Postdial delay is the time between the last digit dialed and the moment the phone rings at the receiving location. In the PSTN, people expect a short postdial delay and to hear ringback within seconds. The more translations and lookups that take place, the longer the postdial delay becomes. Overall network design, translation rules, and alternate pathing affect postdial delay. You must strive to use these tools most efficiently to reduce postdial delay.
- **Availability and fault tolerance:** Consider overall network availability and call success rate when you design a dial plan. Fault tolerance and redundancy within VoIP networks are most important at the gatekeeper level. By using an alternate path you help provide redundancy and fault tolerance in the network.

 Copyright © 2005, Cisco Systems, Inc.

Hierarchical Numbering Plans

This topic describes the advantages and attributes of hierarchical numbering plans.



Scalable telephony networks require telephone-numbering plans that are hierarchical. A hierarchical design has the following advantages:

- **Simplified provisioning:** Provides the ability to easily add new groups and modify existing groups
- **Simplified routing:** Keeps local calls local and uses a specialized number key, such as an area code, for long-distance calls
- **Summarization:** Establishes groups of numbers in a specific geographical area or functional group
- **Scalability:** Adds scalability to the number plan by adding additional high-level number groups
- **Management:** Controls number groups from a single point in the overall network

It is not easy to design a hierarchical numbering plan. Existing numbering plans in the network (such as proprietary PBXs, key systems, and telephony services such as Centrex), and the necessity to conform to the PSTN at gateways, all contribute to the complexity of the design. Translation between these systems is a difficult task. If possible, avoid retraining system users. The goal is to design a numbering plan that has the following attributes:

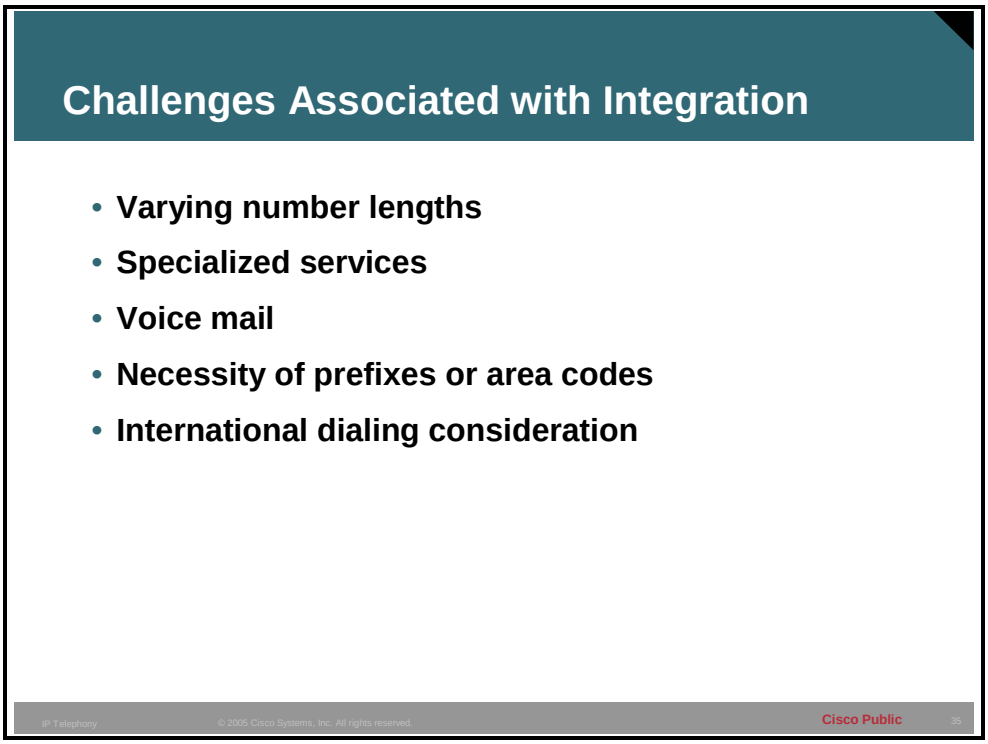
- Minimal impact on existing systems
- Minimal impact on users of the system
- Minimal translation configuration
- Consideration of anticipated growth

- Conformance to public standards, where applicable

 Copyright © 2005, Cisco Systems, Inc.

Internal Numbering and Public Numbering Plan Integration

This topic describes the challenges associated with integrating internal numbering with the public numbering plan.



Numbering plans vary greatly throughout the world. Different countries use different number lengths and hierarchical plans within their borders. Telephony equipment manufacturers and service providers use nonstandard numbering. In an attempt to standardize numbering plans, the International Telecommunication Union (ITU) developed the E.164 worldwide prefix scheme.

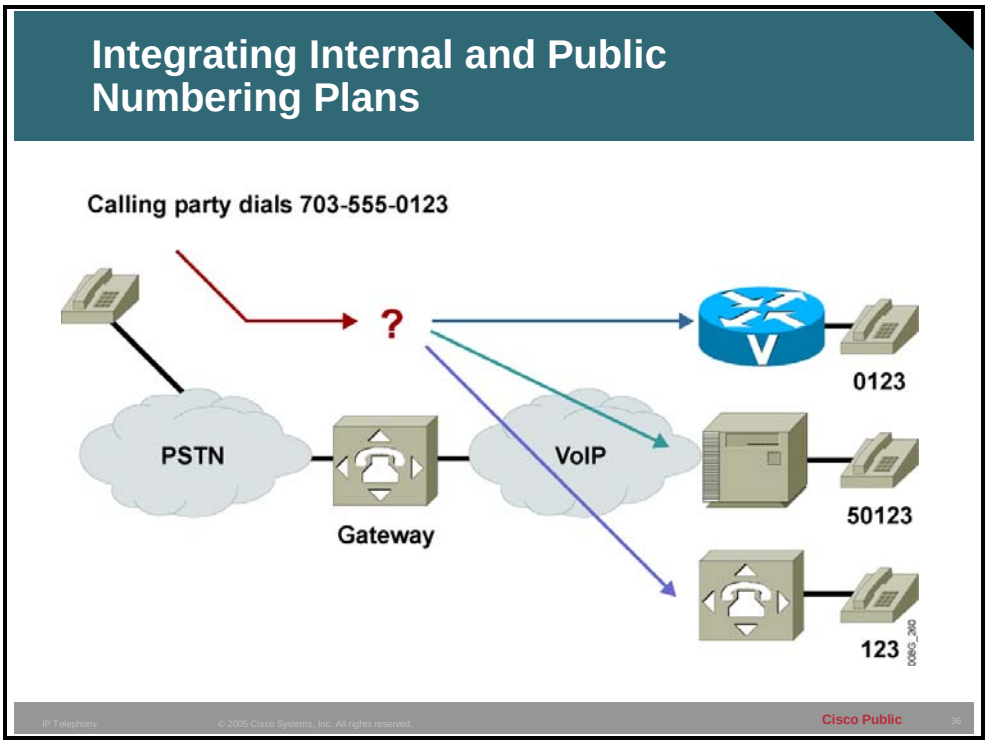
Number plan integration from an internal system such as a VoIP and PBX system to the PSTN requires careful planning. The hierarchical structure of the number plan and the problems associated with varying number lengths in different systems make number plan integration complex.

The challenges that you face with number plan integration include the following:

- **Varying number lengths:** Within the IP network, consideration is given to varying number lengths that exist outside the IP network. Local, long-distance, key system, and Centrex dialing from within the IP network may require digit manipulation.
- **Specialized services:** Services such as Centrex and their equivalents typically have 4- or 5-digit numbers. Dialing from the PSTN into a private VoIP network and then out to a Centrex extension can also require extensive digit manipulation.
- **Voice mail:** When a called party cannot be reached, the network may have to redirect the call to voice mail. Since the voice-mail system can require a completely different number plan than the endpoint telephones, translation is necessary.

- **Necessity of prefixes or area codes:** It can be necessary to strip or add area codes, or prepend or replace prefixes. Rerouting calls from the IP network to the PSTN for failure recovery can require extra digits.
- **International dialing consideration:** Country codes and number plans vary in length within countries. Dialing through an IP network to another country requires careful consideration.

 Copyright © 2005, Cisco Systems, Inc.

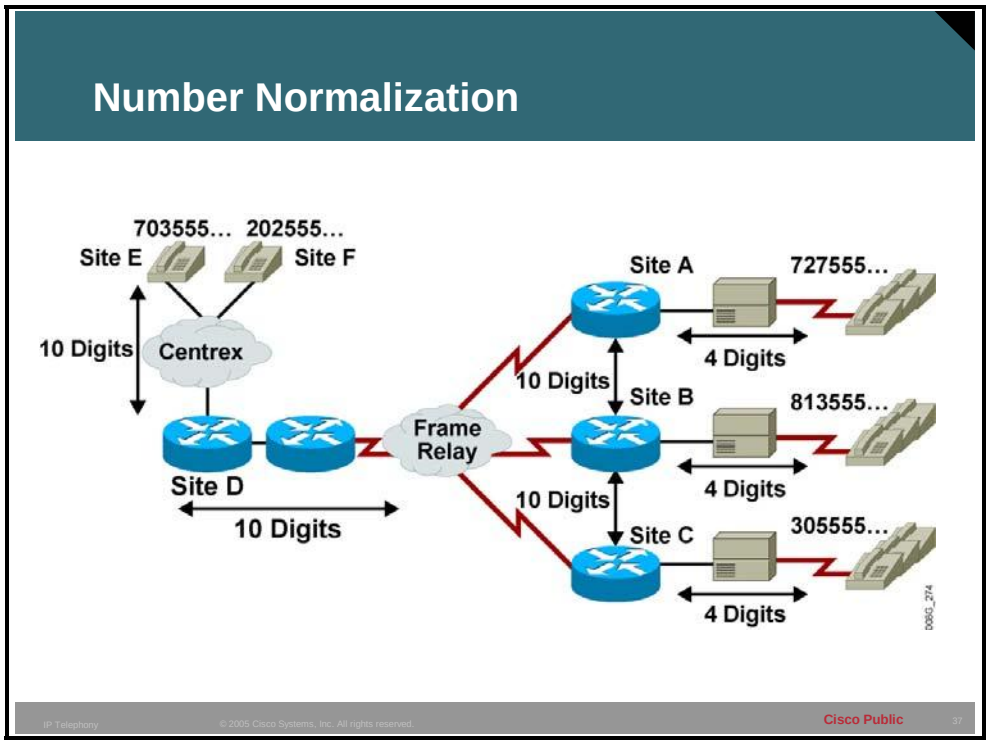


This figure shows a call from the PSTN destined for 1-703-555-0123. The gateway must realize the true destination. All endpoints end with the correct digit sequence, but which is the correct endpoint? Should the gateway append or prepend digits to the dialed number? Should it strip and omit digits?

Different PBXs support variable-length dial plans that contain 3 to 11 digits. The length variations present challenges when private plans merge with public number plans. Issues also arise when no one answers a number and the call is forwarded to a voice-mail system.

Enhancing and Extending an Existing Plan to Accommodate VoIP

This topic describes methods for integrating existing number plans into a VoIP network.



There are many ways that you can enhance and extend an existing number plan to accommodate the VoIP network; all of them require careful planning and consideration. This lesson will discuss two of these ways: number normalization and technology prefixes.

Example: Number Normalization

When site E (703555….) dials 7275550199, the full 10-digit dialed string is passed through the Centrex to the router at site D. Router D matches the destination pattern 7275550199 and forwards the 10-digit dial string to router A. Router A matches the destination pattern 727555…., strips off the matching 727555, and forwards the remaining 4-digit dial string to the PBX. The PBX matches the correct station and completes the call to the proper extension.

Calls in the reverse direction are handled similarly. However, because the Centrex service requires the full 10-digit dial string to complete calls, the POTS dial peer at router D is configured with digit stripping disabled. An alternate solution involves enabling digit stripping and configuring the dial peer with a 6-digit prefix (in this case 703555), which results in forwarding the full dial string to the Centrex service.

 Copyright © 2005, Cisco Systems, Inc.

Router Digit Stripping Comparison

Router A	Router D
dial-peer voice 1 pots	dial-peer voice 4 pots
destination-pattern 727555….	destination-pattern 703555….
port 1/0:1	**no digit-strip**
!	port 1/0:1
dial-peer voice 4 voip	!
destination-pattern 703555….	dial-peer voice 5 pots
session target ipv4:10.10.10.2	destination-pattern 202555….
!	**no digit-strip**
dial-peer voice 5 voip	port 1/0:1
destination-pattern 202555….	!
session target ipv4:10.10.10.3	dial-peer voice 1 voip
!	destination-pattern 727555….
	session target ipv4:10.10.10.1
	!

Another method, called “technology prefixes,” allows you to include special characters in the called number. These special characters (most commonly designated as 1#, 2#, 3#, etc.) are prepended to the called number on the outgoing VoIP dial peer. The gatekeeper then checks its gateway technology prefix table for gateways that are registered with that particular technology prefix. Technology prefixes also identify a type, class, or pool of gateways.

Example: Technology Prefixes Applied

Voice gateways can register with technology prefix 1#; H.320 gateways with technology prefix 2#; and voice-mail gateways with technology prefix 3#. Multiple gateways can register with the same type prefix. When this happens, the gatekeeper makes a random selection among gateways of the same type.

If the callers know the type of device that they are trying to reach, they can include the technology prefix in the destination address to indicate the type of gateway to use to get to the destination. For example, if a caller knows that address 7275550111 belongs to a regular telephone, the caller can use the destination address of 1#7275550111, where 1# indicates that the address should be resolved by a voice gateway. When the voice gateway receives the call for 1#7275550111, it strips off the technology prefix and routes the next leg of the call to the telephone at 7275550111.

You can enter technology prefix commands on gateways and gatekeepers in two places, depending on how you want to design the technology prefix decision intelligence: the gateway VoIP interface or the gateway dial peer.

You can implement this type of digit manipulation and management of dialed numbers in various ways, depending on the infrastructure of the network. All of the components, including

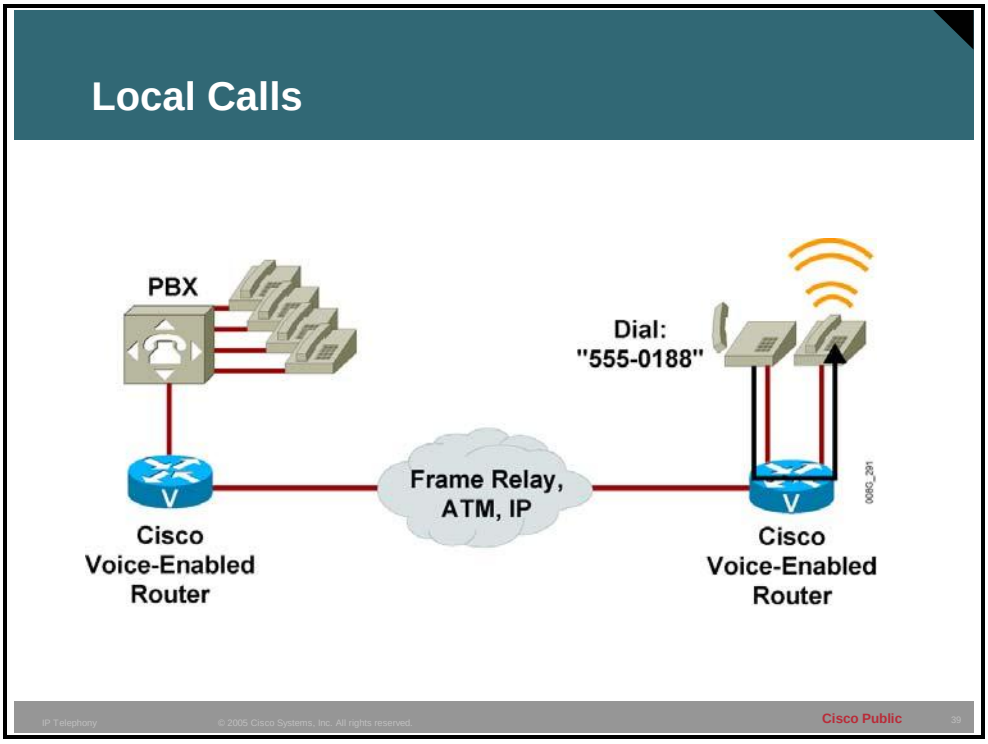
the gatekeepers, gateways, Cisco CallManagers, PBXs, key systems, and other systems, may need to be included in the process.

 Copyright © 2005, Cisco Systems, Inc.

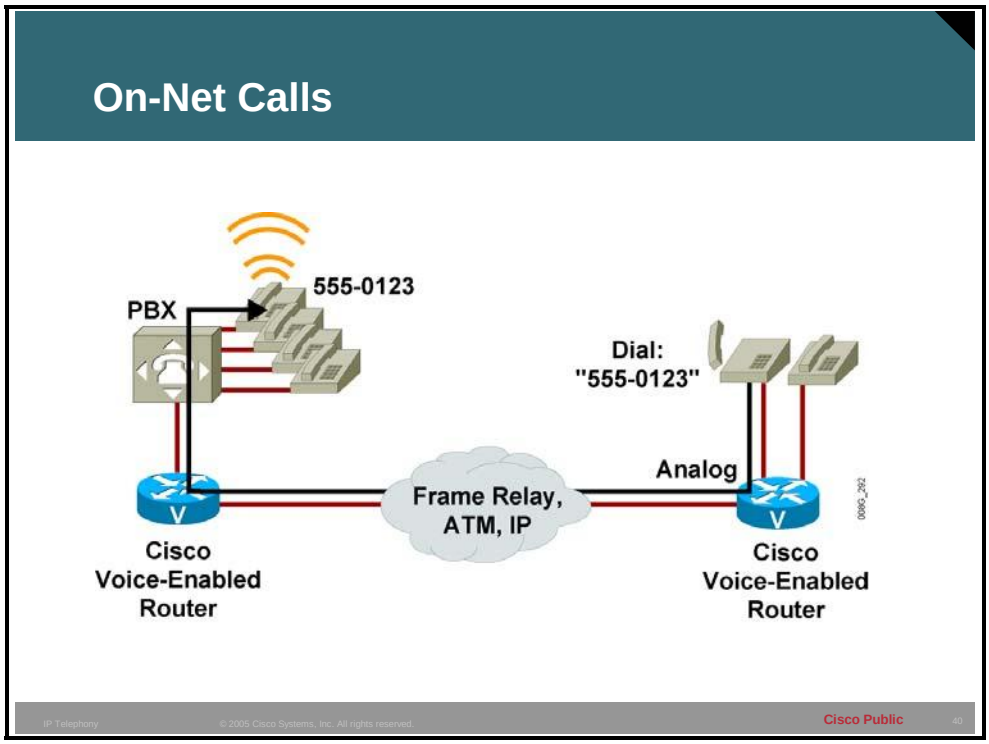
Configuring Voice Ports

Voice Port Applications

Different types of applications require specific types of ports. In many instances, the type of port is dependent on the voice device that is connected to the network. This topic identifies the different types of voice port applications within the network.

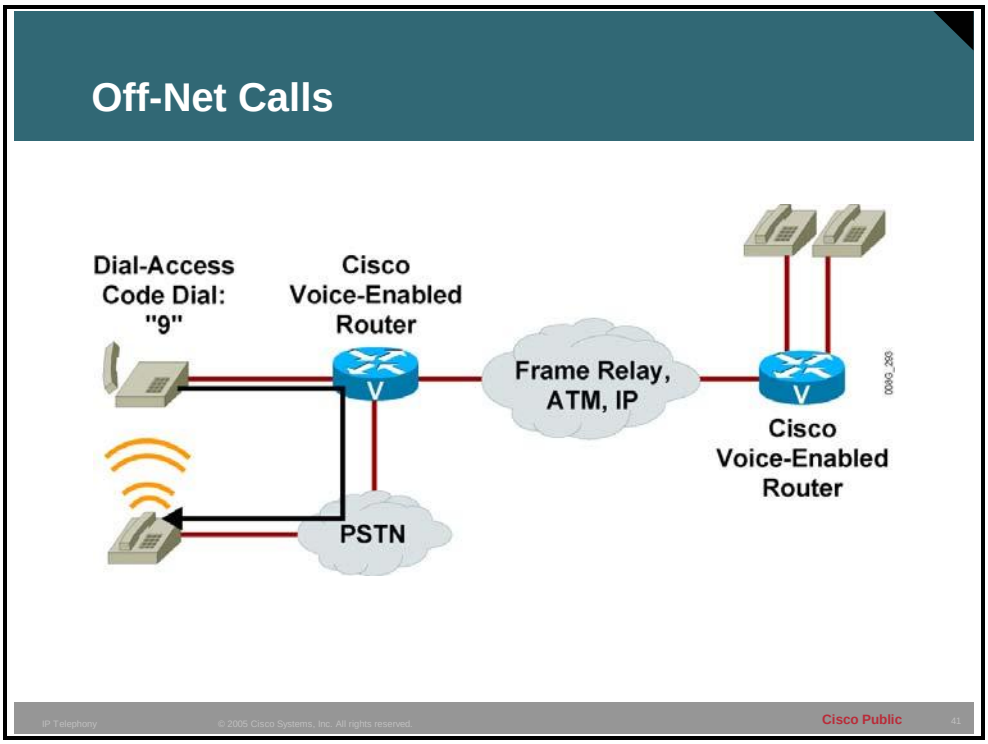


Local calls occur between two telephones connected to one Cisco voice-enabled router. This type of call is handled entirely by the router and does not travel over an external network. Both telephones are directly connected to Foreign Exchange Station (FXS) ports on the router.

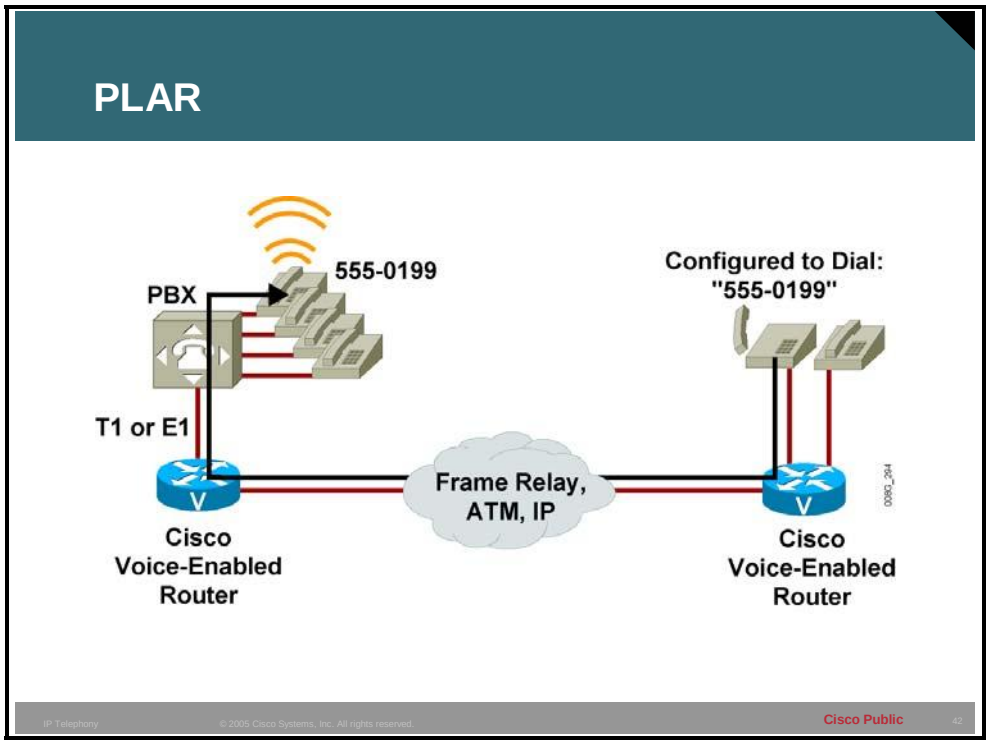


On-net calls occur between two telephones on the same data network. The calls can be routed through one or more Cisco voice-enabled routers, but the calls remain on the same data network. The edge telephones attach to the network through direct connections and FXS ports, or through a PBX, which typically connects to the network via a T1 connection. IP Phones that connect to the network via switches place on-net calls either independently or through Cisco CallManager. The connection across the data network can be a LAN connection, as in a campus environment, or a WAN connection, as in an enterprise environment.

 Copyright © 2005, Cisco Systems, Inc.

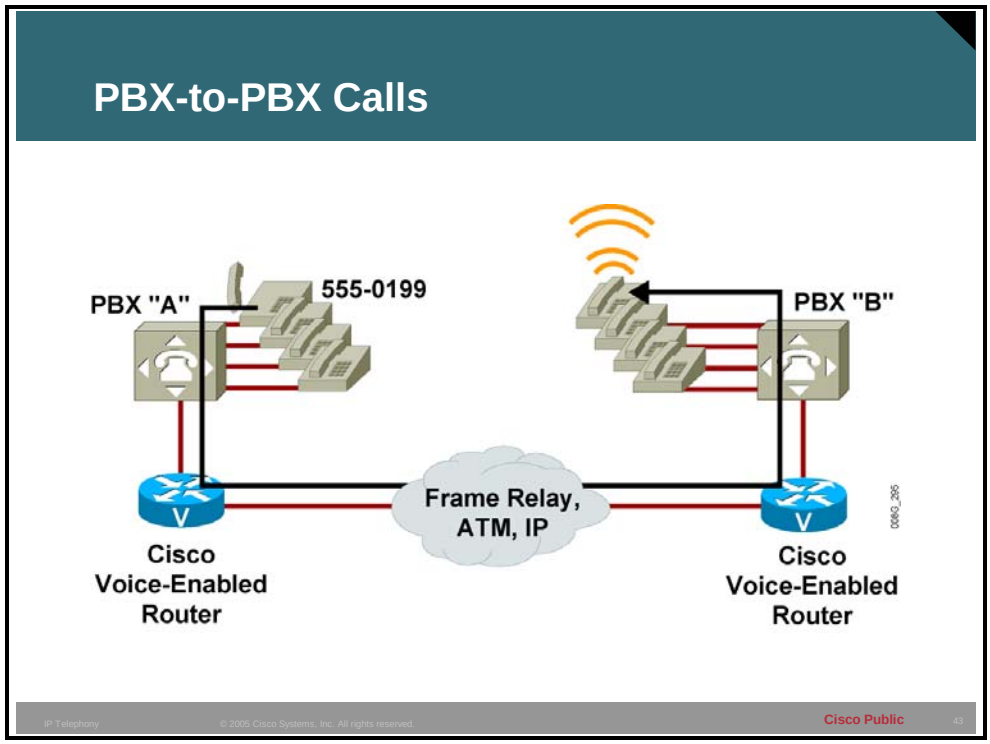


Off-net calls occur when, to gain access to the public switched telephone network (PSTN), the user dials an access code, such as “9,” from a telephone that is directly connected to a Cisco voice-enabled router or PBX. The connection to the PSTN is a single analog connection via a Foreign Exchange Office (FXO) port or a digital T1 or E1 connection.

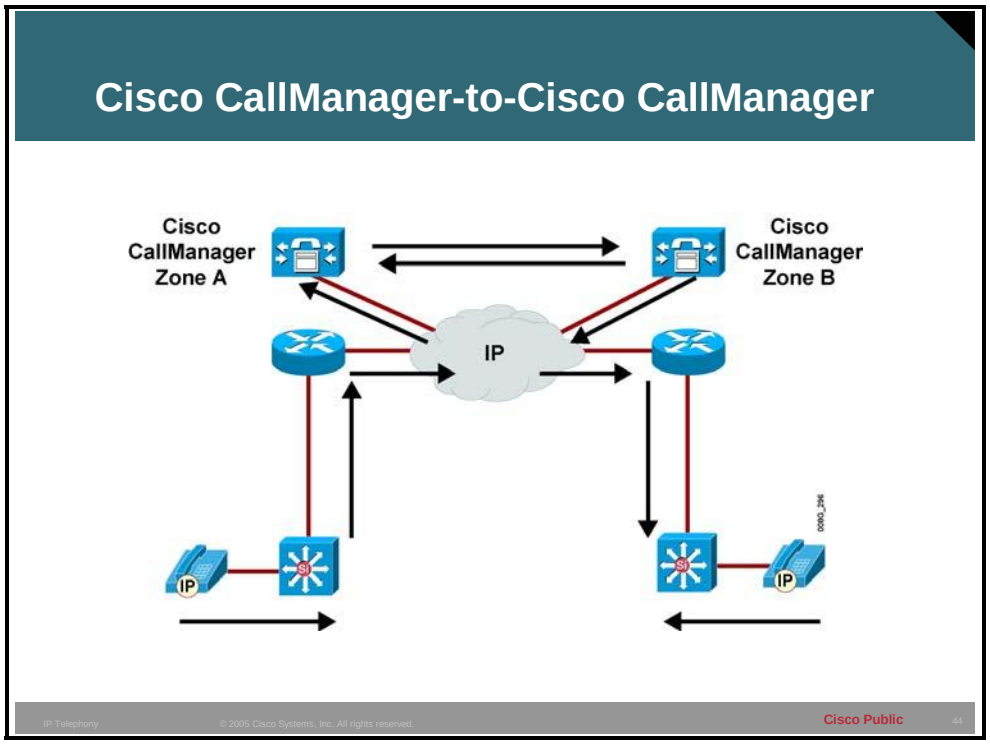


Private line, automatic ringdown (PLAR) calls automatically connect a telephone to a second telephone when the first telephone goes off hook. When this connection occurs, the user does not get a dial tone because the voice-enabled port that the telephone is connected to is preconfigured with a specific number to dial. A PLAR connection can work between any types of signaling, including recEive and transMit (ear and mouth [E&M]), FXO, FXS, or any combination of analog and digital interfaces.

 Copyright © 2005, Cisco Systems, Inc.

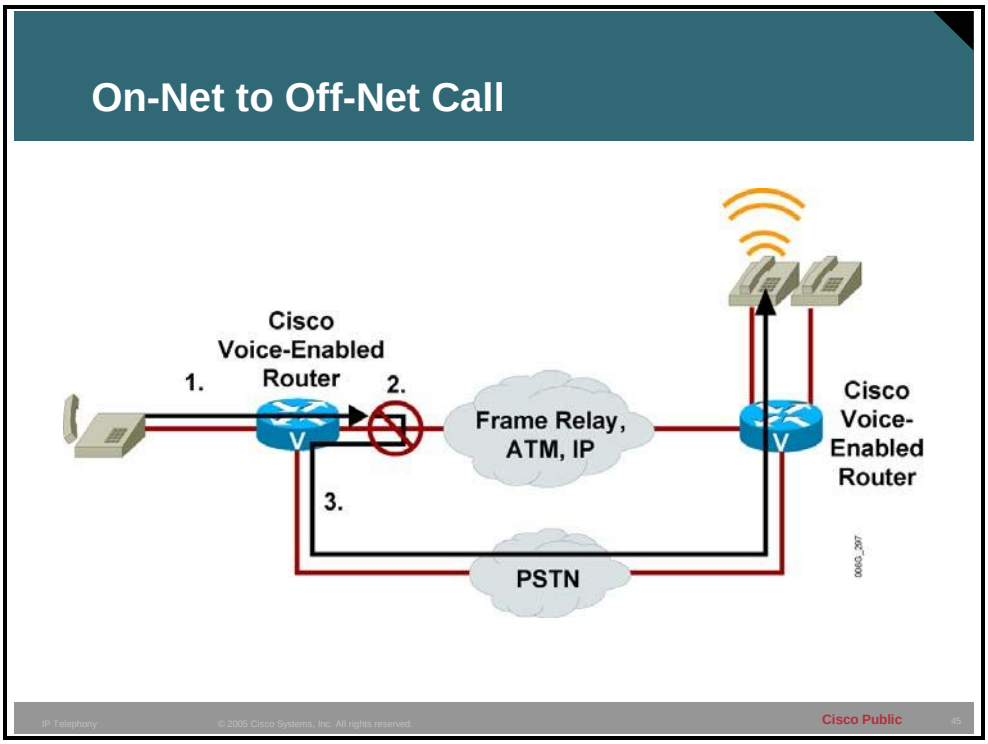


A PBX-to-PBX call originates at a PBX at one site and terminates at a PBX at another site while using the network as the transport between the two locations. Many business environments connect sites with private tie trunks. When migrating to a converged voice and data network, this same tie-trunk connection can be emulated across the IP network. Modern PBX connections to the network are typically digital T1 or E1 with channel associated signaling (CAS) or PRI signaling, although PBX connections can also be analog.



As part of an overall migration strategy, a business may replace PBXs with a Cisco CallManager infrastructure. This infrastructure includes IP telephones that plug directly into the IP network. Cisco CallManager performs the same call-routing functions formerly provided by the PBX. When an IP Phone uses Cisco CallManager to place a call, Cisco CallManager—based on its configuration—assesses if the call is destined for another IP Phone under its control, or if the call must be routed through a remote Cisco CallManager for call completion. Although the call stays on the IP network, it may be sent between zones. Every Cisco CallManager is part of a zone. A zone is a collection of devices that are under a common administration, usually a Cisco CallManager or gatekeeper.

 Copyright © 2005, Cisco Systems, Inc.



When planning a resilient call-routing strategy, it may be necessary to reroute calls through a secondary path should the primary path fail. On-net to off-net calls originate on an internal network and are routed to an external network, usually to the PSTN. On-net to off-net call-switching functionality may be necessary when a network link is down, or if a network becomes overloaded and unable to handle all calls presented.

Example: Voice Port Applications

The table lists application examples for each type of call.

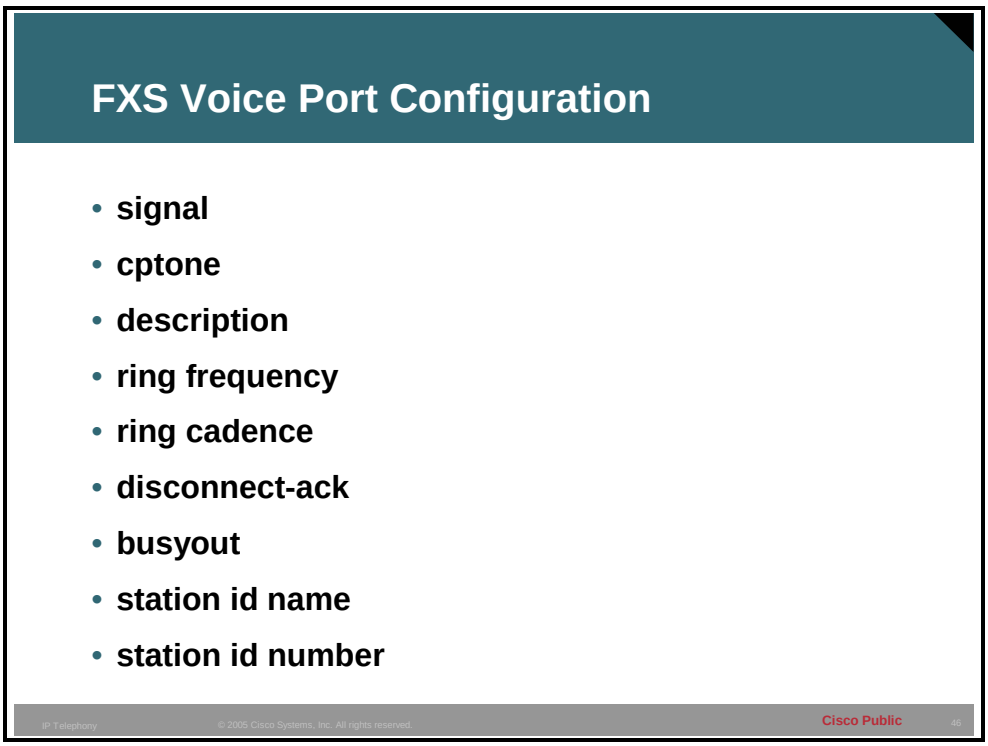
Voice Port Call Types

Type of Call	Example
Local calls	One staff member calls another staff member at the same office. The call is switched between two ports on the same voice-enabled router.
On-net calls	One staff member calls another staff member at a remote office. The call is sent from the local voice-enabled router, across the IP network, and terminated on the remote office voice-enabled router.
Off-net calls	A staff member calls a client who is located in the same city. The call is sent from the local voice-enabled router that acts as a gateway to the PSTN. The call is then sent to the PSTN for call termination.
PLAR calls	A client picks up a customer service telephone located in the lobby of the office and is automatically connected to a customer service representative without dialing any digits. The call is automatically dialed, based on the PLAR configuration of the voice port. In this case, as soon as the handset goes off hook, the voice-enabled router generates the prespecified digits to place the call.
PBX-to-PBX calls	One staff member calls another staff member at a remote office. The call is sent from the local PBX, through a voice-enabled router, across the IP network, through the remote voice-enabled router, and terminated on the remote office PBX.
Cisco CallManager-to-Cisco CallManager calls	One staff member calls another staff member at a remote office using IP Phones. The call setup is handled by the Cisco CallManagers at both locations. After the call is set up, the IP Phones generate IP packets carrying voice between sites.
On-net to off-net calls	One staff member calls another staff member at a remote office while the IP network is congested. When the originating voice-enabled router determines that it cannot terminate the call across the IP network, it sends the call to the PSTN with the appropriate dialed digits to terminate the call at the remote office via the PSTN network.

 Copyright © 2005, Cisco Systems, Inc.

FXS Ports

FXS ports connect analog edge devices. This topic identifies the parameters that are configurable on the FXS port.



In North America, the FXS port connection functions with default settings most of the time. The same cannot be said for other countries and continents. Remember, FXS ports look like switches to the edge devices that are connected to them. Therefore, the configuration of the FXS port should emulate the switch configuration of the local PSTN.

Example: Configuring FXS Ports

For example, consider the scenario of an international company with offices in the United States and England. The PSTN of each country provides signaling that is standard for that country. In the United States, the PSTN provides a dial tone that is different from the tone in England. When the telephone rings to signal an incoming call, the ring is different in the United States. Another instance when the default configuration might be changed is when the connection is a trunk to a PBX or key system. In that case, the FXS port must be configured to match the settings of that device.

Configuration Parameters

FXS port configuration allows you to set parameters based on the requirements of the connection if default settings need to be altered or the parameters need to be set for fine-tuning. You can set the following configuration parameters:

- **signal:** Sets the signaling type for the FXS port. In most cases, the default signaling of loop start works well. If the connected device is a PBX or a key system, the preferred signaling is ground start. Modern PBXs and key systems do not normally use FXS ports as connections to the network, but older systems may still have these interfaces. When

connecting the FXS port to a PBX or key system, you must check the configuration of the voice system and set the FXS port to match the system setting.

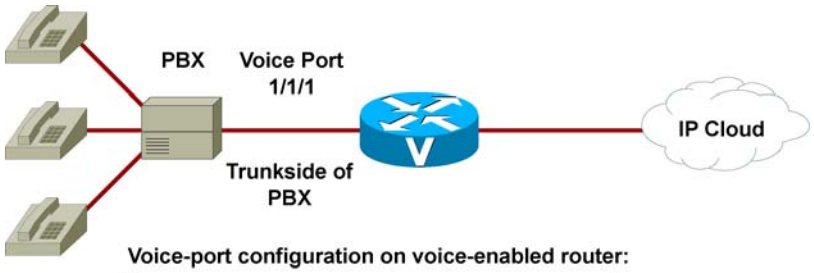
- **cptone:** Configures the appropriate call-progress tone for the local region. The call-progress tone setting determines the dial tone, busy tone, and ringback tone to the originating party.
- **description:** Configures a description for the voice port. You must use the description setting to describe the voice port in **show** command output. It is always useful to provide some information about the usage of a port. The description could specify the type of equipment that is connected to the FXS port.
- **ring frequency:** Configures a specific ring frequency (in Hz) for an FXS voice port. You must select the ring frequency that matches the connected equipment. If set incorrectly, the attached telephone might not ring or might buzz. In addition, the ring frequency is usually country-dependent, and you should take into account the appropriate ring frequency for your area before you configure this command.
- **ring cadence:** Configures the ring cadence for an FXS port. The ring cadence defines how ringing voltage is sent to signal a call. The normal ring cadence in North America is 2 seconds of ringing followed by 4 seconds of silence. In England, normal ring cadence is a short ring followed by a longer ring. When configured, the **cptone** setting automatically sets the ring cadence to match that country. You can manually set the ring cadence if you want to override the default country value. You may have to shut down and reactivate the voice port before the configured value takes effect.
- **disconnect-ack:** Configures an FXS voice port to remove line power if the equipment on an FXS loop-start trunk disconnects first. This removal of line power is not something the user hears, but instead is a method for electrical devices to signal that one side has ended the call.
- **busyout:** Configures the ability to busy out an analog port.
- **station id name:** Provides the station name associated with the voice port. This parameter is passed as a calling name to the remote end if the call is originated from this voice port. If no Caller ID is received on an FXO voice port, this parameter will be used as the calling name. Maximum string length is limited to 15.
- **station id number:** Provides the station number that is to be used as the calling number associated with the voice port. This parameter is optional and, if provided, will be used as the calling number if the call is originated from this voice port. If not specified, the calling number will be used from a reverse dial-peer search. If no Caller ID is received on an FXO voice port, this parameter will be used as the calling number. Maximum string length is 15.

Example: FXS Port Configuration

The example shows how the British office is configured to enable ground-start signaling on a Cisco 2600 or 3600 series router on FXS voice port 1/0/0. The call-progress tones are set for Great Britain, and the ring cadence is set for pattern 1.

 Copyright © 2005, Cisco Systems, Inc.

FXS Voice Port Configuration



Voice-port configuration on voice-enabled router:

```
Router# configure terminal
Router (config)# voice-port 1/0/0
Router (config-voiceport)# signal ground-start
Router (config-voiceport)# cptone GB
Router (config-voiceport)# ring cadence pattern01
```

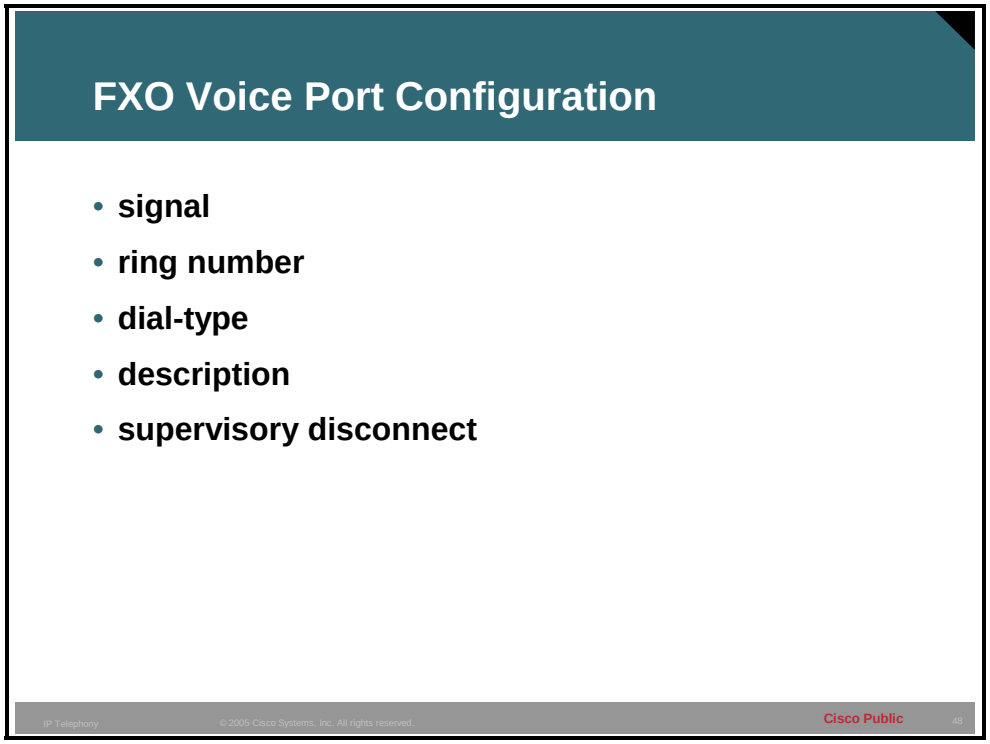
Enters voice-port configuration mode
Enables ground-start signaling
Sets call-progress tones for Great Britain
Specifies ring cadence pattern 1

D060_450

IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 47

FXO Ports

FXO ports act like telephones and connect to central office (CO) switches or to a station port on a PBX. This topic identifies the configuration parameters that are specific to FXO ports.



Configuration Parameters

In most instances, the FXO port connection functions with default settings. FXO port configuration allows you to set parameters based on the requirements of the connection where default settings need to be altered or parameters set for fine-tuning. You can set the following configuration parameters:

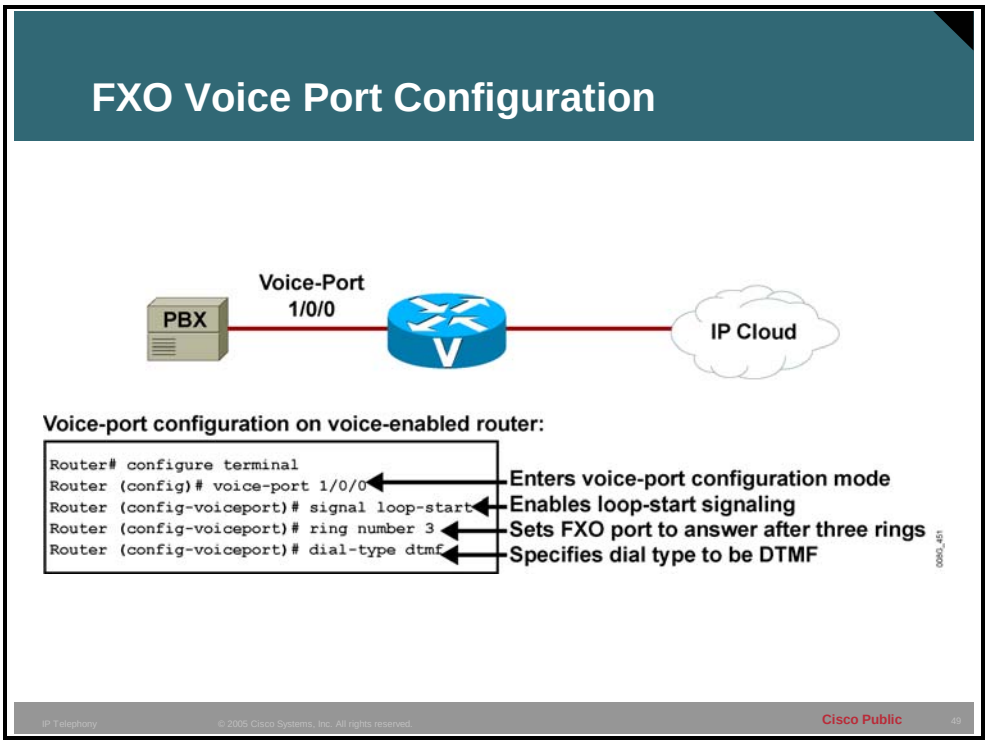
- **signal:** Sets the signaling type for the FXO port. If the FXO port is connected to the PSTN, the default settings are adequate. If the FXO port is connected to a PBX, the signal setting must match the PBX.
- **ring number:** Configures the number of rings before an FXO port answers a call. This is useful when you have other equipment available on the line to answer incoming calls. The FXO port answers if the equipment that is online does not answer the incoming call within the configured number of rings.
- **dial-type:** Configures the appropriate dial type for outbound dialing. Older PBXs or key sets may not support dual-tone multifrequency (DTMF) dialing. If you are connecting an FXO port to this type of device, you may need to set the dial type for pulse dialing.
- **description:** Configures a description for the voice port. Use the description setting to describe the voice port in **show** command output.

 Copyright © 2005, Cisco Systems, Inc.

- **supervisory disconnect:** Configures supervisory disconnect signaling on the FXO port. Supervisory disconnect signaling is a power denial from the switch that lasts at least 350 ms. When this condition is detected, the system interprets this as a disconnect indication from the switch and clears the call. You should disable supervisory disconnect on the voice port if there is no supervisory disconnect available from the switch. Typically, supervisory disconnect is available when connecting to the PSTN and is enabled by default. When the connection extends out to a PBX, you should verify the documentation to ensure that supervisory disconnect is supported.

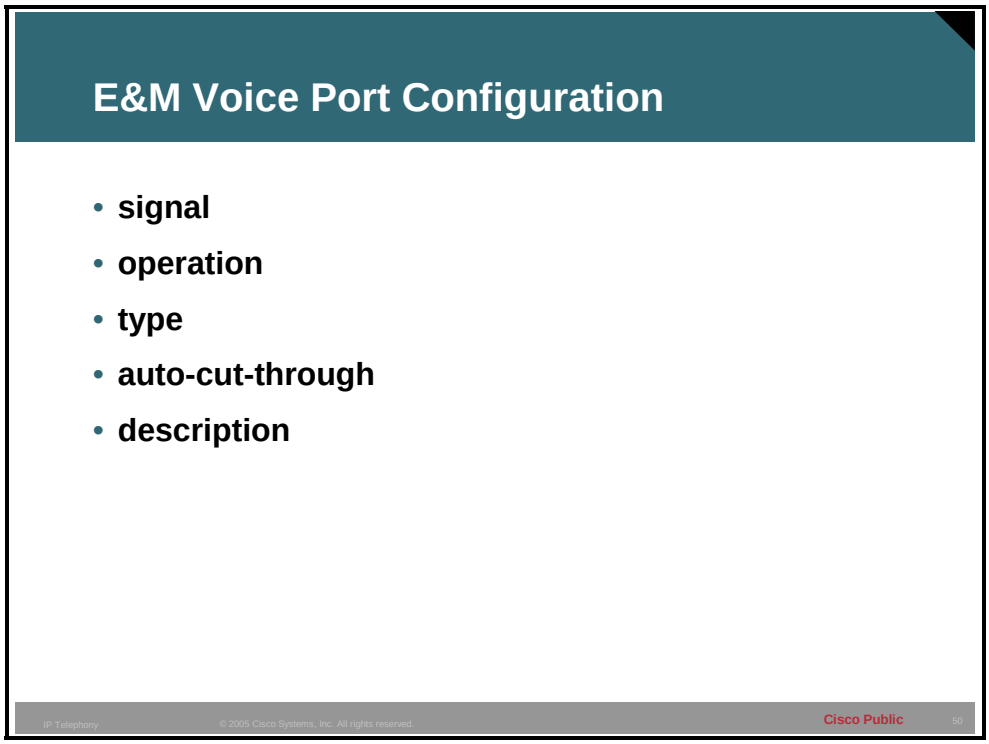
Example: FXO Port Configuration

The configuration in the figure enables loop-start signaling on a Cisco 2600 or 3600 series router on FXO voice port 1/0/0. The ring-number setting of "3" specifies that the FXO port does not answer the call until after the third ring, and the dial type is set to DTMF.



E&M Ports

E&M ports provide signaling that is used generally for switch-to-switch or switch-to-network trunk connections. This topic identifies the configuration parameters that are specific to the E&M port.



Configuration Parameters

Although E&M ports have default parameters, you must usually configure these parameters to match the device that is connected to the E&M port. You can set the following configuration parameters:

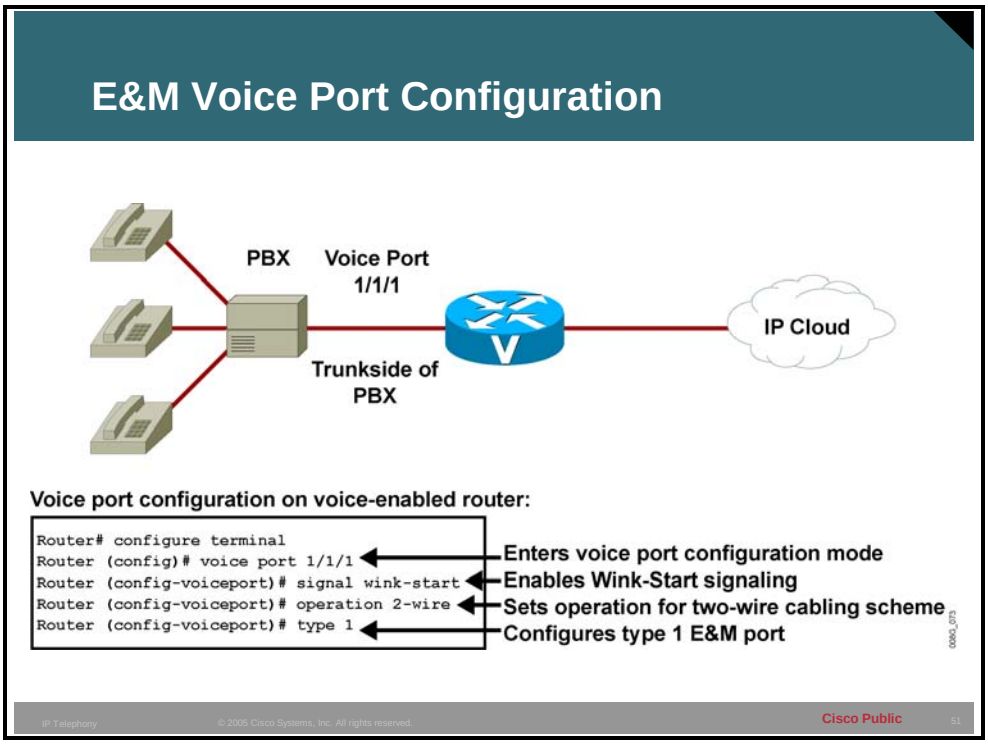
- **signal:** Configures the signal type for E&M ports and defines the signaling that is used when notifying a port to send dialed digits. This setting must match that of the PBX to which the port is connected. You must shut down and reactivate the voice port before the configured value takes effect. With Wink-Start signaling, the router listens on the M-lead to determine when the PBX wants to place a call. When the router detects current on the M-lead, it waits for availability of digit registers and then provides a short *wink* on the E-lead to signal the PBX to start sending digits. With delay-start, the router provides current on the E-lead immediately upon seeing current on the M-lead. When current is stopped for the digit-sending duration, the E-lead stays high until digit registers are available. With immediate-start, the PBX simply waits a short time after raising the M-lead and then sends the digits without a signal from the router.
- **operation:** Configures the cabling scheme for E&M ports. The **operation** command affects the voice path only. The signaling path is independent of two-wire versus four-wire settings. If the wrong cable scheme is specified, the user may get voice traffic in one direction only. You must verify with the PBX configuration to ensure that the settings match. You must then shut down and reactivate the voice port for the new value to take effect.

 Copyright © 2005, Cisco Systems, Inc.

- **type:** Configures the E&M interface type for a specific voice port. The type defines the electrical characteristics for the E- and M-leads. The E- and M-leads are monitored for on-hook and off-hook conditions. From a PBX perspective, when the PBX attempts to place a call, it goes high (off hook) on the M-lead. The switch monitors the M-lead and recognizes the request for service. If the switch attempts to pass a call to the PBX, the switch goes high on the E-lead. The PBX monitors the E-lead and recognizes the request for service by the switch. To ensure that the settings match, you must verify them with the PBX configuration.
- **auto-cut-through:** Configures the ability to enable call completion when a PBX does not provide an M-lead response. For example, when the router is placing a call to the PBX, even though they may have the same correct signaling configured, not all PBXs provide the wink with the same duration or voltage. The router may not understand the PBX wink. The **auto-cut-through** command allows the router to send digits to the PBX, even when the expected wink is not detected.
- **description:** Configures a description for the voice port. Use the **description** setting to describe the voice port in **show** command output.

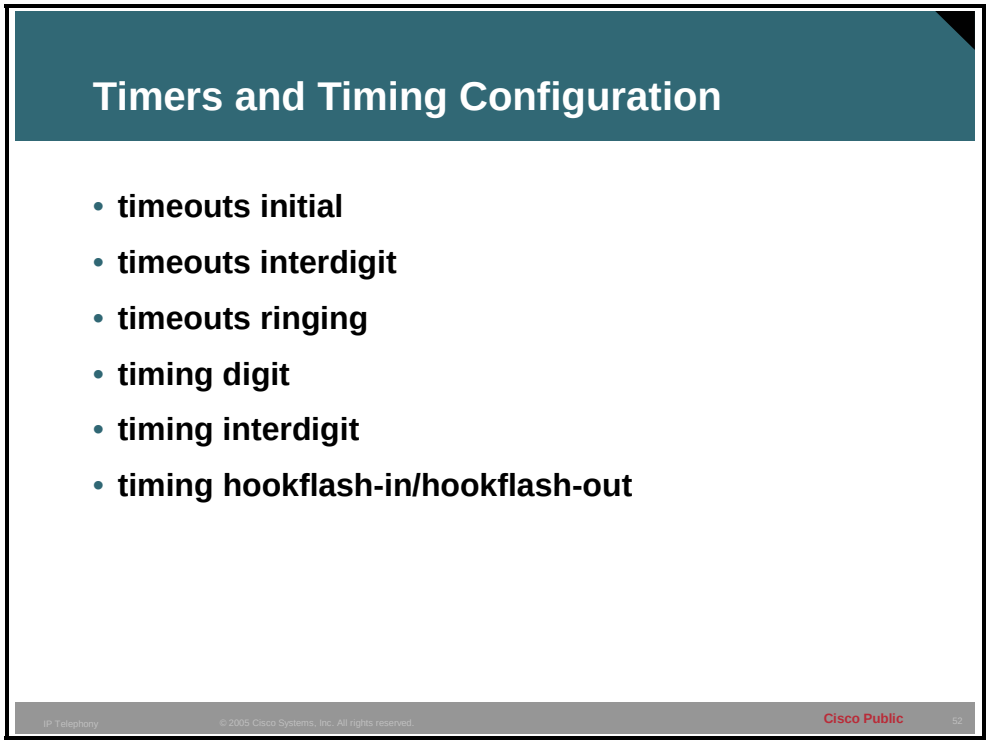
Example: E&M Port Configuration

The configuration in the figure enables Wink-Start signaling on a Cisco 2600 or 3600 series router on E&M voice port 1/1/1. The operation is set for the two-wire voice-cabling scheme and the type is set to 1.



Timers and Timing

This topic identifies the timing requirements and adjustments that are applicable to voice interfaces. Under normal use, these timers do not need adjusting. In instances where ports are connected to a device that does not properly respond to dialed digits or hookflash, or where the connected device provides automated dialing, these timers can be configured to allow more or less time for a specific function.



Configuration Parameters

You can set a number of timers and timing parameters for fine-tuning the voice port. Following are voice port configuration parameters that you can set:

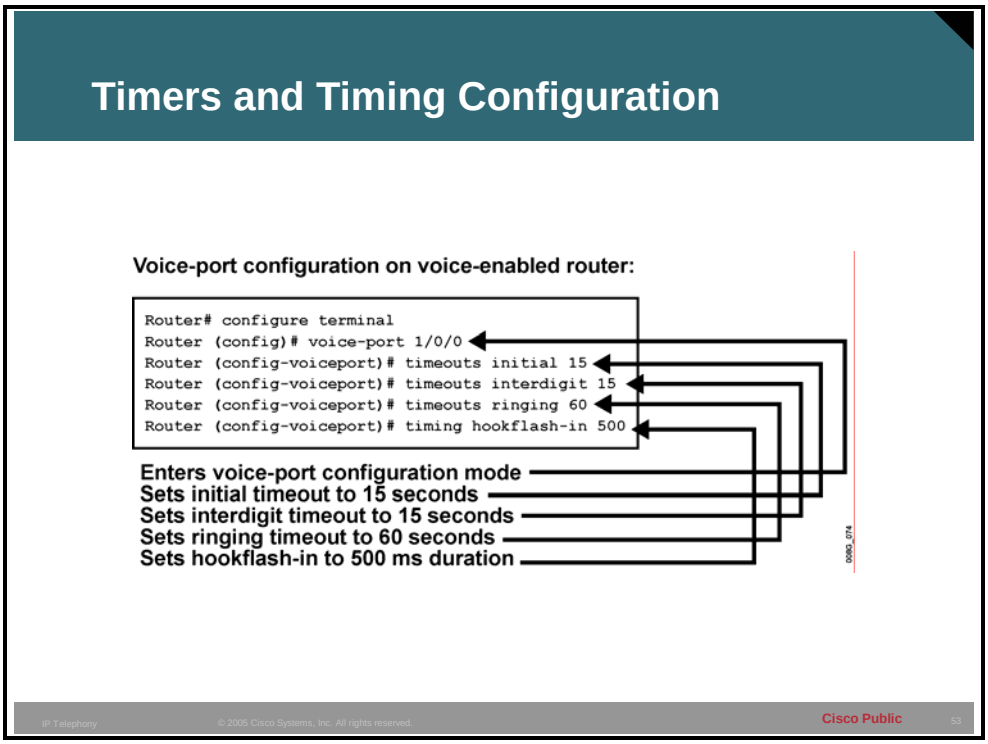
- **timeouts initial:** Configures the initial digit timeout value in seconds. This value controls how long the dial tone is presented before the first digit is expected. This timer typically does not need to be changed.
- **timeouts interdigit:** Configures the number of seconds for which the system will wait for the caller to input a subsequent digit of the dialed digits, after the caller has input the initial digit. If the digits are coming from an automated device, and the dial plan is a variable-length dial plan, you can shorten this timer so that the call proceeds without having to wait the full default of 10 seconds for the interdigit timer to expire.
- **timeouts ringing:** Configures the length of time that a caller can continue ringing a telephone when there is no answer. You can configure this setting to be less than the default of 180 seconds so that you do not tie up the voice port when it is evident that the call is not going to be answered.

 Copyright © 2005, Cisco Systems, Inc.

- **timing digit:** Configures the DTMF digit-signal duration for a specified voice port. You can use this setting to fine-tune a connection to a device that may have trouble recognizing dialed digits. If a user or device dials too quickly, the digit may not be recognized. By changing the timing on the digit timer, you can provide for a shorter or longer DTMF duration.
- **timing interdigit:** Configures the DTMF interdigit duration for a specified voice port. You can change this setting to accommodate faster or slower dialing characteristics.
- **timing hookflash-in and hookflash-out:** Configures the maximum duration (in milliseconds) of a hookflash indication. Hookflash is an indication by a caller that the caller wishes to do something specific with the call, such as transfer the call or place the call on hold. For hookflash-in, if the hookflash lasts longer than the specified limit, the FXS interface processes the indication as on hook. If you set the value too low, the hookflash may be interpreted as a hang up; if you set the value too high, the handset has to be left hung up for a longer period to clear the call. For hookflash-out, the setting specifies the duration (in milliseconds) of the hookflash indication that the gateway generates outbound. You can configure this to match the requirements of the connected device.

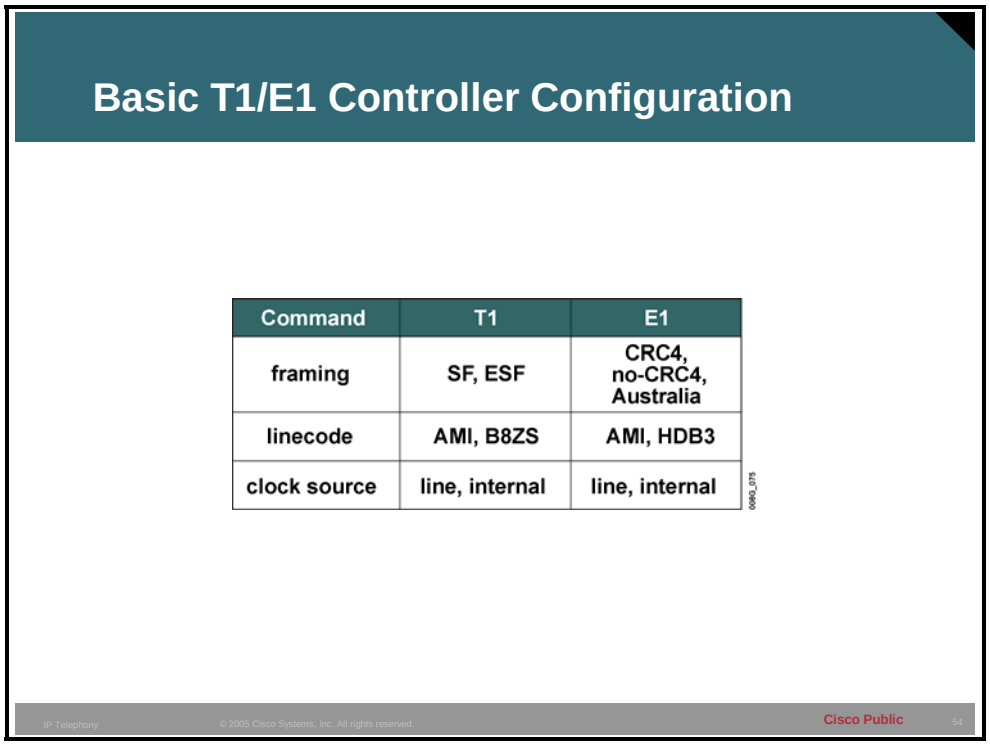
Example: Timers Configuration

The installation in the figure is for a home for the elderly, where users may need more time to dial digits than in other residences. Also, the requirement is to allow the telephone to ring, unanswered, for only one minute. The configuration in the figure enables several timing parameters on a Cisco voice-enabled router voice port 1/0/0. The initial timeout is lengthened to 15 seconds, the interdigit timeout is lengthened to 15 seconds, the ringing timeout is set to 60 seconds, and the hookflash-in timer is set to 500 ms.



Digital Voice Ports

This topic identifies the configuration parameters that are specific to T1 and E1 digital voice ports.



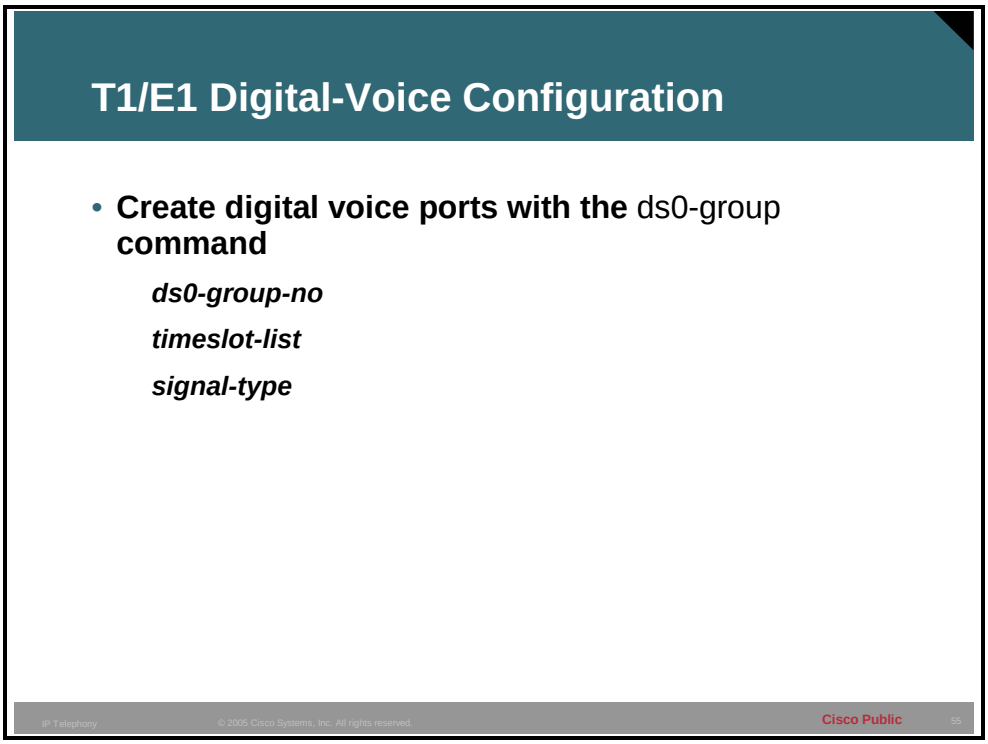
Configuration Parameters

When you purchase a T1 or E1 connection, make sure that your service provider gives you the appropriate settings. Before you configure a T1 or E1 controller to support digital voice ports, you must enter the following basic configuration parameters to bring up the interface.

- **framing:** Selects the frame type for a T1 or E1 data line. The framing configuration differs between T1 and E1.
  - **Options for T1:** Super Frame (SF) or Extended Superframe (ESF)
  - **Options for E1:** 4-bit cyclic redundancy check (CRC4), no-CRC4, or Australia
  - **Default for T1:** SF
  - **Default for E1:** CRC4
- **linecode:** Configures the line-encoding format for the DS1 link.
  - **Options for T1:** alternate mark inversion (AMI) or binary 8-zero substitution (B8ZS)
  - **Options for E1:** AMI or high density binary 3 (HDB3)
  - **Default for T1:** AMI
  - **Default for E1:** HDB3
- **clock source:** Configures clocking for individual T1 or E1 links.
  - **Options:** line or internal

 Copyright © 2005, Cisco Systems, Inc.

— **Default:** line



You must create a digital voice port in the T1 or E1 controller to make the digital voice port available for specific voice port configuration parameters. You must also assign timeslots and signaling to the logical voice port through configuration. The first step is to create the T1 or E1 digital voice port with the **ds0-group** *ds0-group-no* **timeslots** *timeslot-list* **type** *signal-type* command.

The **ds0-group** command automatically creates a logical voice port that is numbered as *slot/port*:*ds0-group-no*.

The *ds0-group-no* parameter identifies the DS0 group (number from 0 to 23 for T1 and from 0 to 30 for E1). This group number is used as part of the logical voice port numbering scheme.

The **timeslots** command allows the user to specify which timeslots are part of the DS0 group. The *timeslot-list* parameter is a single timeslot number, a single range of numbers, or multiple ranges of numbers separated by commas.

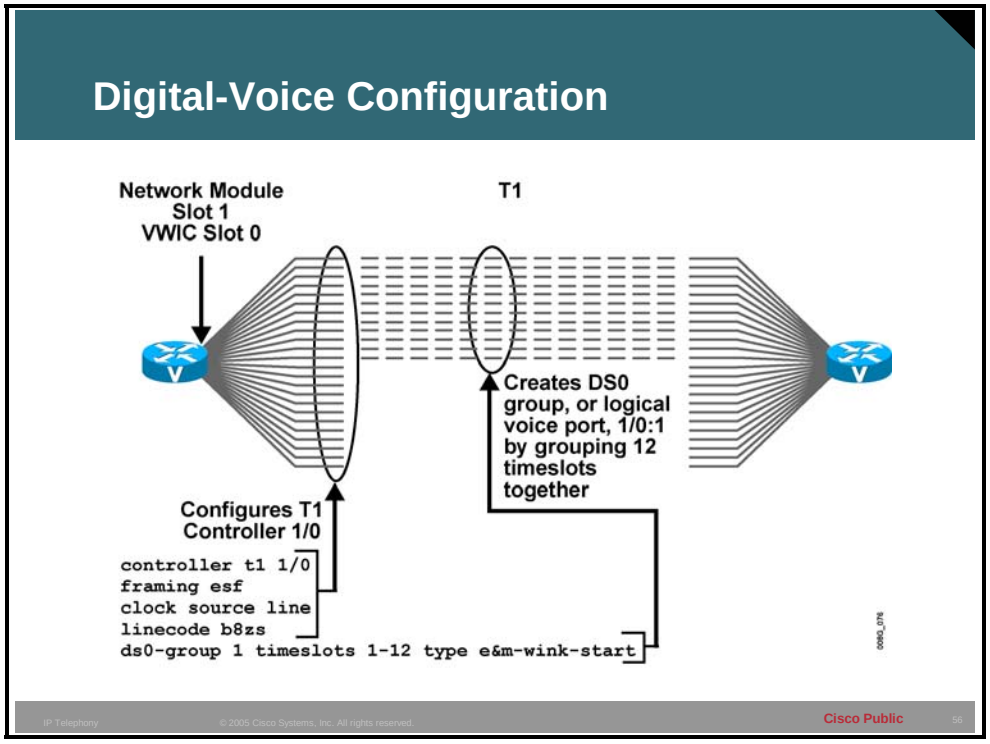
The **type** command defines the emulated analog signaling method that the router uses to connect to the PBX or PSTN. The type depends on whether the interface is T1 or E1.

After you specify a **ds0-group** command, the system creates a logical voice port. You must then enter the voice-port configuration mode to configure port-specific parameters. To enter voice-port configuration mode on a Cisco 2600 or 3600 series platform, use the **voice-port** *slot/port*:*ds0-group-no* command.

To delete a DS0 group, you must first shut down the logical voice port. When the port is in shutdown state, you can remove the DS0 group from the T1 or E1 controller with the **no ds0-group** *ds0-group-no* command.

Example: T1 Configuration

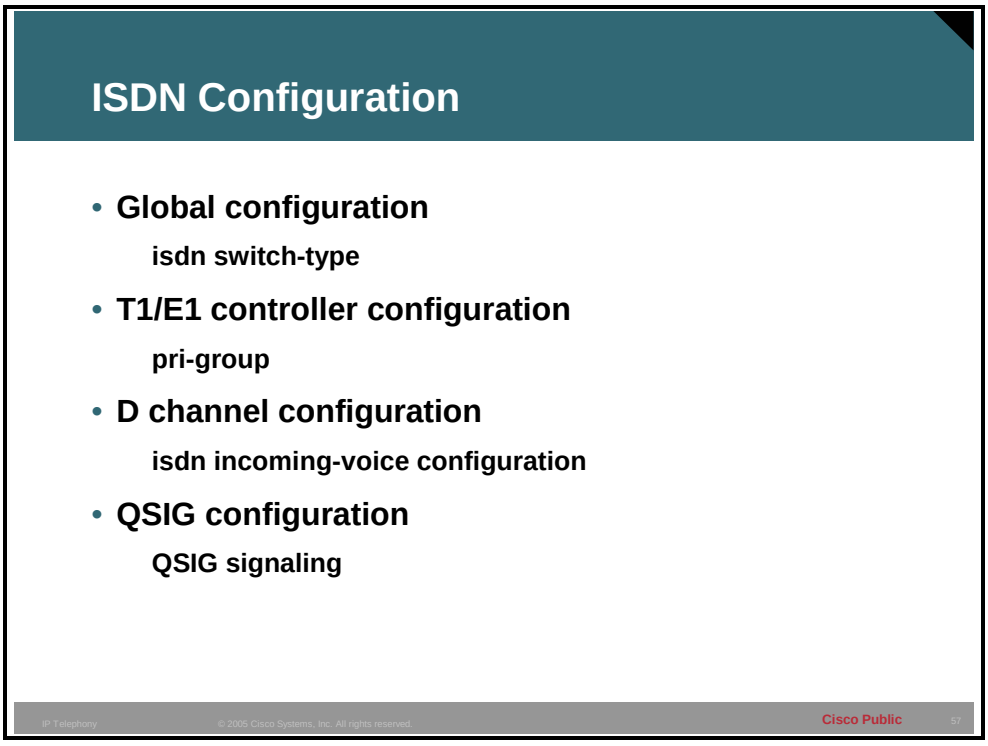
This example configures the T1 controller for ESF, B8ZS line code, and timeslots 1 through 12 with E&M Wink-Start signaling. The resulting logical voice port is **1/0:1**, where **1/0** is the module and slot number and **:1** is the *ds0-group-no* value that was assigned during configuration. You can configure the remaining timeslots for other signaling types or leave them unused.



 Copyright © 2005, Cisco Systems, Inc.

ISDN

This topic identifies ISDN configurations for voice ports.



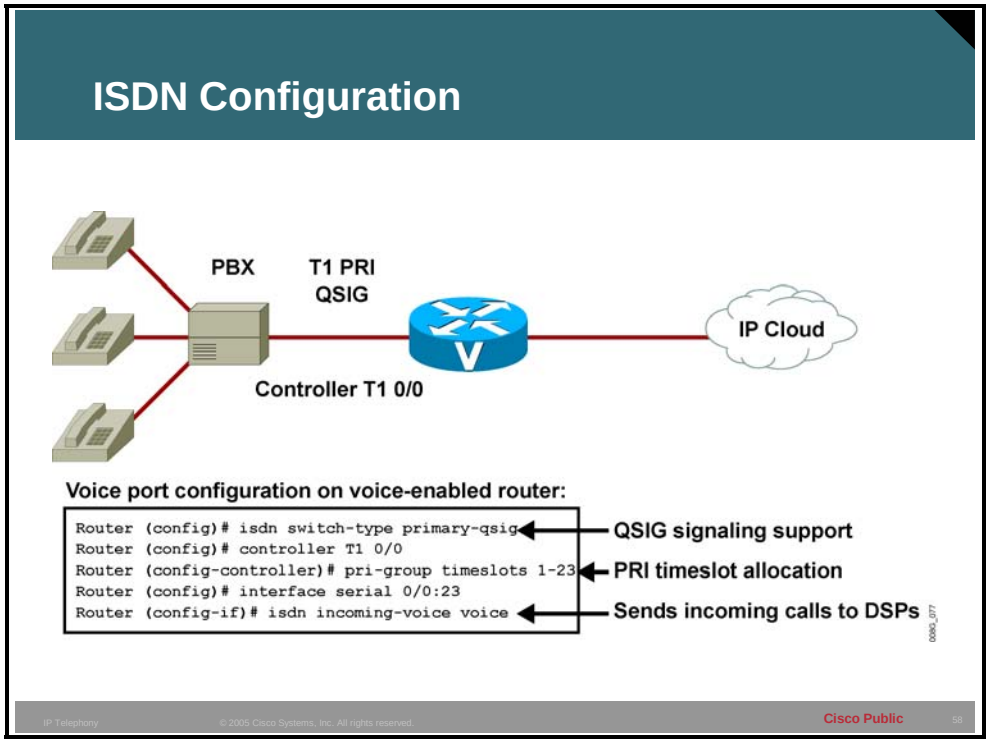
Configuration Parameters

Cisco voice-capable devices provide support for both PRI and BRI voice connections. Many PBX vendors support either T1/E1 PRI or BRI connections. In Europe, where ISDN is more popular, many PBX vendors support BRI connections. When designing how the PBX passes voice to the network, you must ensure that the router supports the correct connection. The first step in configuring ISDN capabilities for T1 or E1 PRI is to configure the T1 or E1 controller basics. After the clock source, framing, and line code are configured, ISDN voice functionality requires the following configuration commands:

- **isdn switch-type:** Configures the ISDN switch type. You can enter this parameter in global configuration mode or at the interface level. If you configure both, the interface switch type takes precedence over the global switch type. This parameter must match the provider ISDN switch. This setting is required for both BRI and PRI connections.
- **pri-group:** Configures timeslots for the ISDN PRI group. T1 allows for timeslots 1 to 23, with timeslot 24 allocated to the D channel. E1 allows for timeslots 1 to 31, with timeslot 16 allocated to the D channel. You can configure the PRI group to include all available timeslots, or you can configure a select group of timeslots for the PRI group.
- **isdn incoming-voice voice:** Configures the interface to send all incoming calls to the digital signal processor (DSP) card for processing.
- **QSIG signaling:** Configures the use of Q Signaling (QSIG) signaling on the D channel. You typically use this setting when connecting via ISDN to a PBX. The command to enable QSIG signaling is **isdn switch-type primary-qsig** for PRI and **isdn switch-type basic-qsig** for BRI connections.

Example: ISDN QSIG Configuration

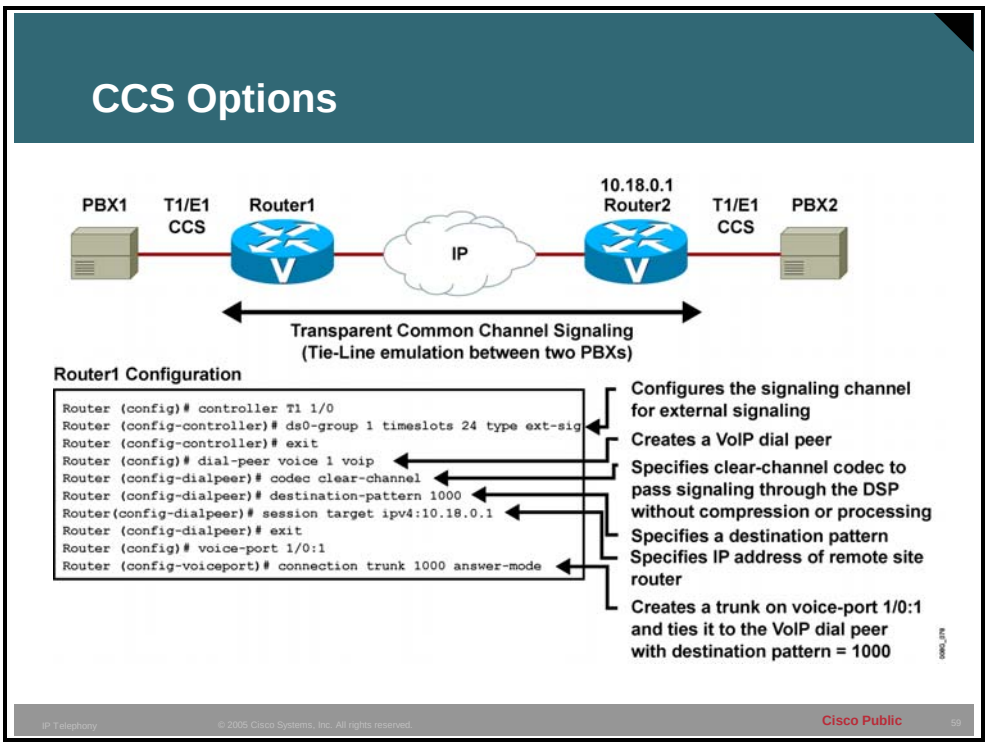
This example shows the configuration for a PBX connection to the Cisco voice-enabled router. The connection is configured for QSIG signaling across all 23 timeslots.



 Copyright © 2005, Cisco Systems, Inc.

CCS Options

This topic describes how to pass proprietary signaling between two PBXs through the use of Transparent Common Channel Signaling (T-CCS).



In many cases, PBXs support proprietary signaling that is used to signal supplementary services only, such as making a light on the telephone blink when voice mail is waiting. Because the router does not understand this proprietary signaling, the signaling must be carried transparently across the network without interpretation. T-CCS allows the connection of two PBXs with digital interfaces that use a proprietary or unsupported common channel signaling (CCS) protocol. T1 and E1 traffic is transported transparently through the data network, and the T-CCS feature preserves proprietary signaling. From the PBX standpoint, this type of communication is accomplished through a point-to-point connection. Calls from the PBXs are not routed, but they do follow a preconfigured route to the destination.

T-CCS Configuration Process

The configuration for T-CCS in a Voice over IP (VoIP) environment calls for the following three-step process:

Step 1 Define the DS0 group.

Configure the command **ds0-group** *ds0-group-no* **timeslots** *timeslot-list* **type ext-sig** in the T1 or E1 controller configuration mode. The **timeslots** command specifies the D channel that carries call signaling. The **type ext-sig** command specifies that the signaling is coming from an external source.

Step 2 Create the dial peer.

- Configure a VoIP dial peer that points to the IP address of the remote voice-enabled router that connects to the remote PBX.

- Configure the dial peer for clear-channel codec that signals the DSP to pass the signaling without interpretation.
- The destination pattern specified in this dial peer is used to create a trunk in Step 3. The number entered here must match the number entered in the **trunk** command.
- The session target specifies the IP address of the remote voice-enabled router.
- Configure the dial peer to point to the IP address of the remote site voice-enabled router using the **session target** command.

Step 3 Create the voice port trunk.

Configure the **connection trunk** *digits* **answer-mode** command at the logical voice port to create a trunk from that port through the VoIP dial peer and across the IP network to the remote router. The *digits* parameter must match the destination pattern in the VoIP dial peer created in Step 2. The **answer-mode** parameter specifies that the router should not attempt to initiate a trunk connection but should wait for an incoming call before establishing the trunk.

The process for passing the signal transparently through the IP network is as follows:

Step 1 PBX1 sends proprietary signaling across the signaling channel to router 1.

Step 2 The logical voice port that corresponds to the signaling channel is configured for trunking, so the router looks for the dial peer that matches the **trunk** *digits* parameter.

Step 3 The VoIP dial peer is configured for clear-channel codec and points to the IP address of the remote router (router 2) connecting the remote PBX (PBX2).

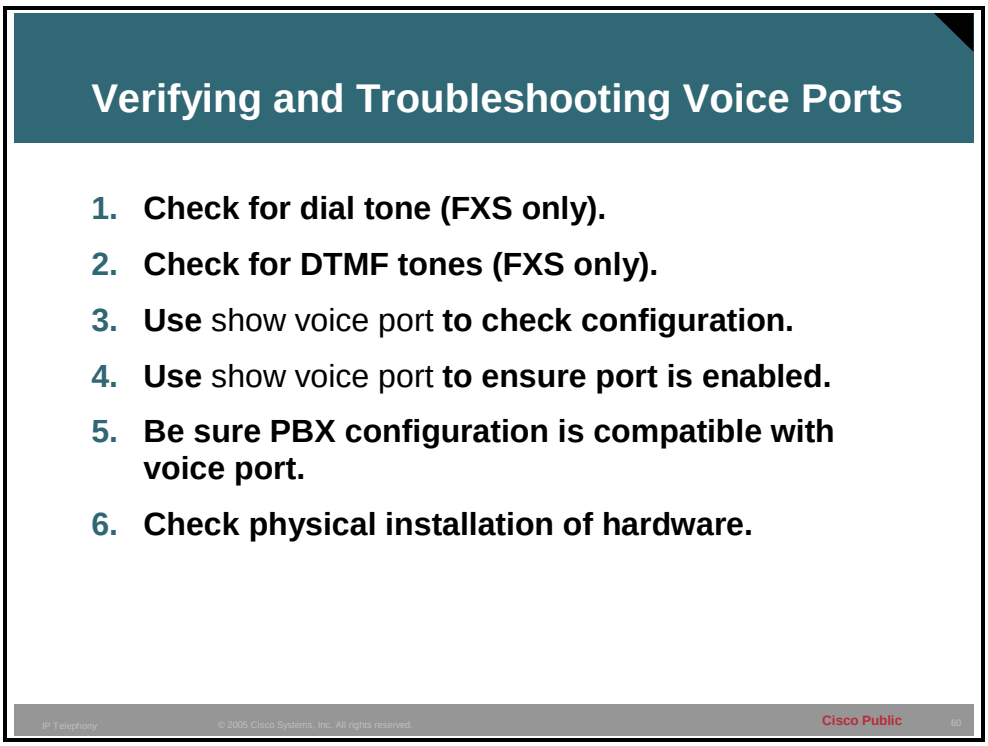
Step 4 The remote router has a plain old telephone service (POTS) dial peer configured that points to the logical voice port that is associated with the signaling channel of PBX2. The signal arrives at PBX2 in its native form.

This process shows the T-CCS signaling part of the configuration only. Additional DS0 group and dial-peer configuration is necessary for transport of the voice channels.

 Copyright © 2005, Cisco Systems, Inc.

Monitoring and Troubleshooting

This topic describes the **show** and **test** commands that are used to monitor and troubleshoot voice ports.



You can perform the following steps to verify voice port configuration:

Step 1 Pick up the handset of an attached telephony device and check for a dial tone. If there is no dial tone, check the following:

- Is the plug firmly seated?
- Is the voice port enabled?
- Is the voice port recognized by the Cisco IOS?
- Is the router running the correct version of Cisco IOS in order to recognize the module?

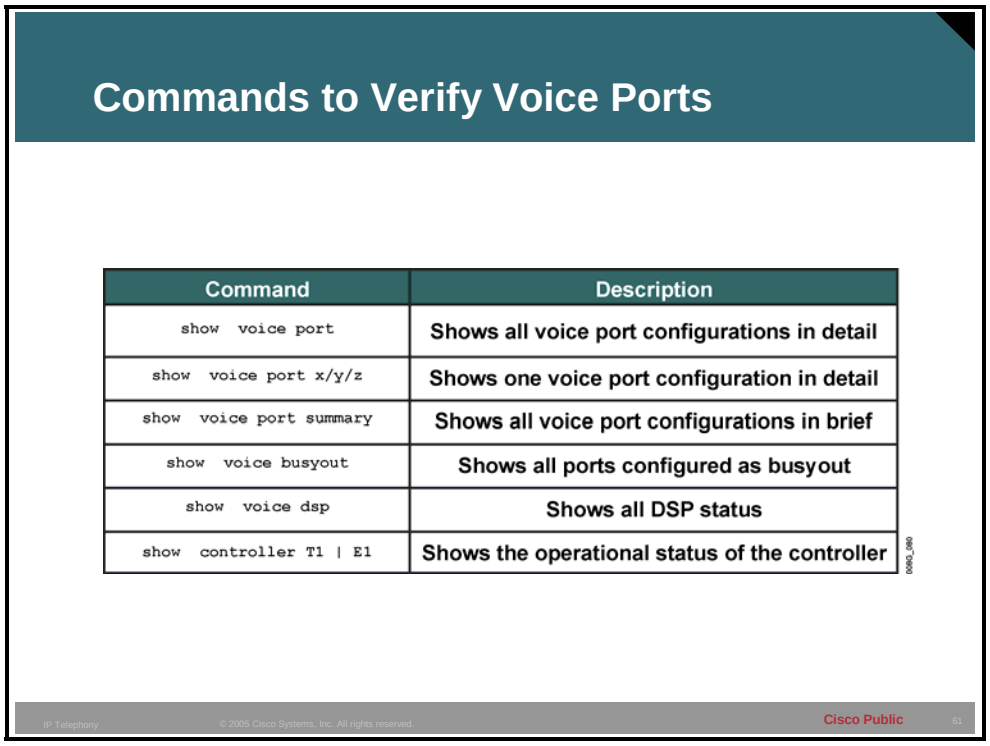
Step 2 If you have a dial tone, check for DTMF voice band tones, such as touch-tone detection. If the dial tone stops when you dial a digit, the voice port is probably configured properly.

Step 3 Use the **show voice port** command to verify that the data configured is correct. If you have trouble connecting a call, and you suspect that the problem is associated with voice port configuration, you can try to resolve the problem by performing Steps 4 through 6.

Step 4 Use the **show voice port** command to make sure that the port is enabled. If the port is administratively down, use the **no shutdown** command. If the port was working previously and is not working now, it is possible that the port is in a hung state. Use the **shutdown**/**no shutdown** command sequence to reinitialize the port.

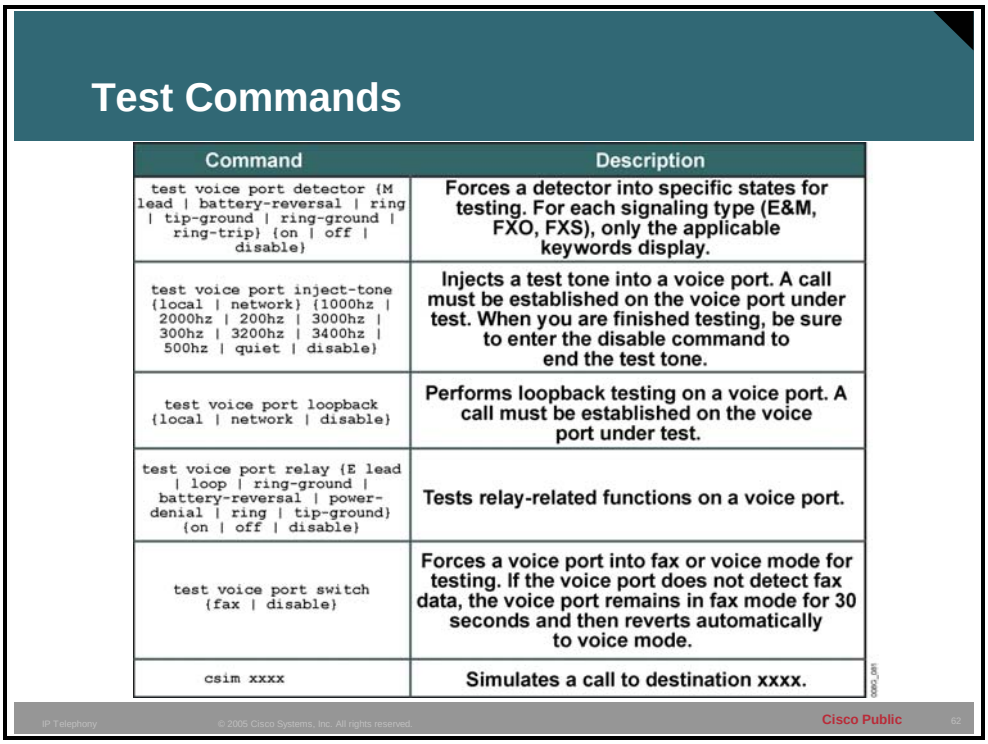
Step 5 If you have configured E&M interfaces, make sure that the values associated with your specific PBX setup are correct. Specifically, check for two-wire or four-wire Wink-Start, immediate-start, or delay-start signaling types, and the E&M interface type. These parameters need to match those set on the PBX for the interface to communicate properly.

Step 6 You must confirm that the voice network module (VNM) is correctly installed. With the device powered down, remove the VNM and reinsert it to verify the installation. If the device has other slots available, try inserting the VNM into another slot to isolate the problem. Similarly, you must move the voice interface card (VIC) to another VIC slot to determine if the problem is with the VIC card or with the module slot.



There are six **show** commands for verifying the voice port and dial-peer configuration. These commands and their functions are shown in the figure.

 Copyright © 2005, Cisco Systems, Inc.



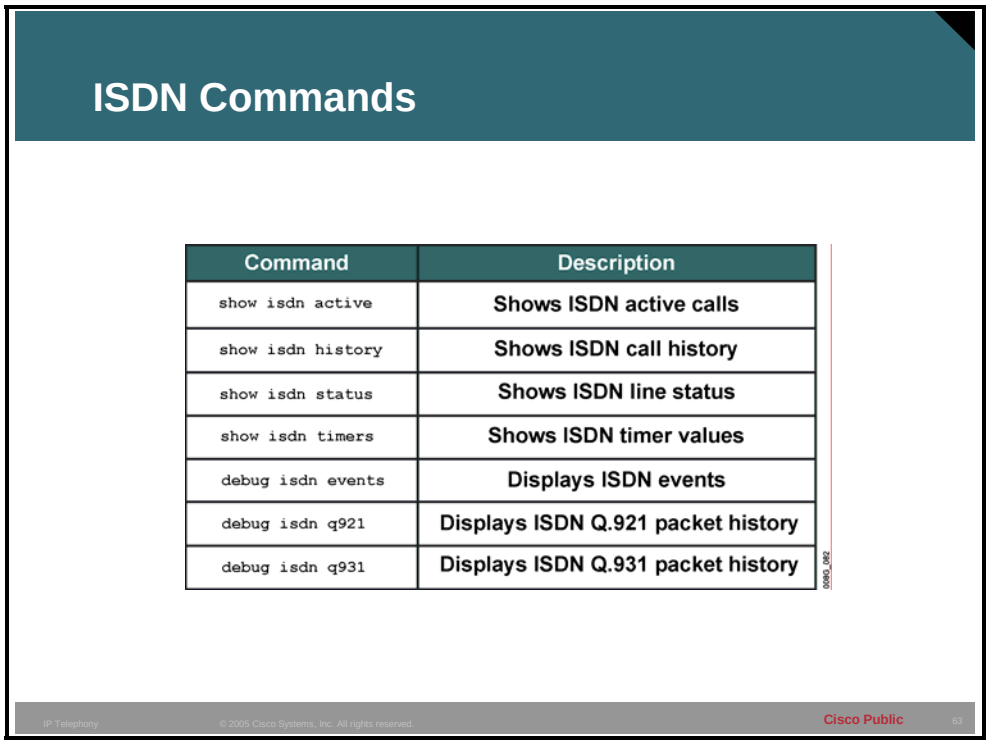
The **test** commands provide the ability to analyze and troubleshoot voice ports on the Cisco 2600 and 3600 series routers. There are five **test** commands to force voice ports into specific states to test the voice port configuration.

When you finish the loopback testing, be sure to enter the **disable** command to end the forced loopback.

After you enter the **test voice port switch fax** command, you can use the **show voice call** command to check whether the voice port is able to operate in fax mode.

The **csim** command simulates a call to any end station for testing purposes. It is most useful when testing dial plans.

Note Refer to the *Voice Port Testing Enhancements in Cisco 2600 and 3600 Series Routers* document for further information.



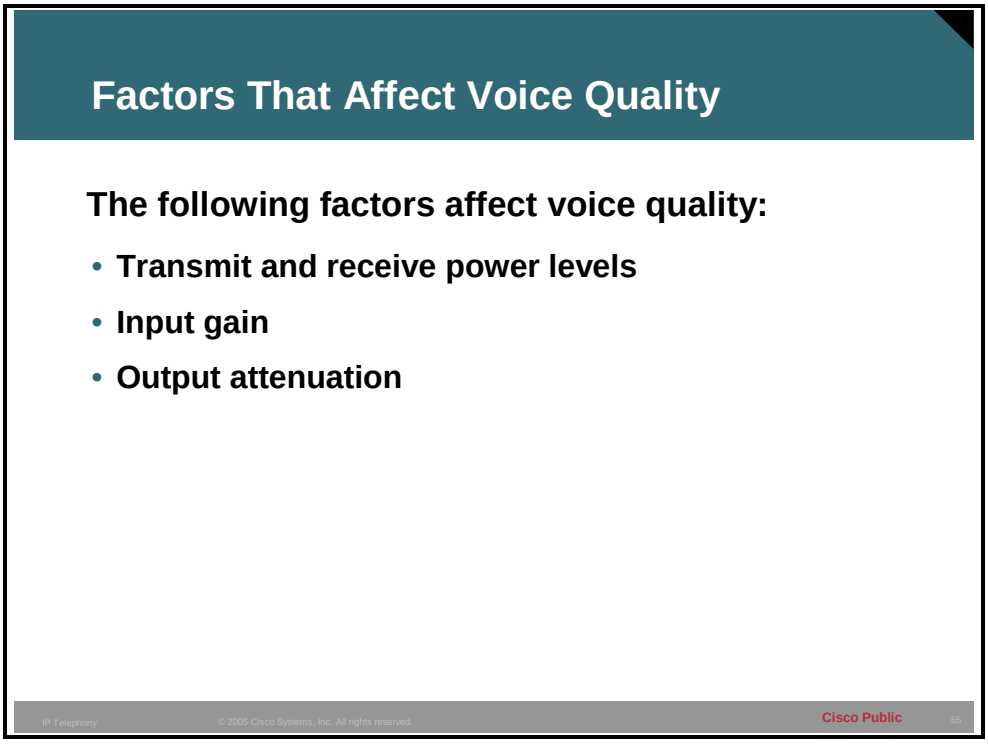
The ISDN **show** and **debug** commands in the figure are useful for viewing and troubleshooting ISDN connections.

 Copyright © 2005, Cisco Systems, Inc.

Adjusting Voice Quality

Electrical Characteristics

This topic describes the electrical characteristics of analog voice and the factors affecting voice quality.



Voice signal power in a long-distance connection must be tightly controlled. The delivered signal power must be high enough to be clearly understood, but not so strong that it leads to instabilities such as echo. In the traditional telephony network, telephone companies control the signal power levels at each analog device. Now that the IP network is carrying voice, it may be necessary to adjust signal power on a voice interface to fine-tune the voice quality.

Most initial voice signals enter the network through a two-wire local loop. Most switches connect to other switches through a four-wire connection. As voice travels through the network for delivery to the remote telephone, the voice signal must be passed from the two-wire local loop to the four-wire connection at the first switch, and from the four-wire connection at the switch to a two-wire local loop at the remote end. If the impedance at these two-wire to four-wire connections is not matched exactly, some of the voice signal reflects back in the direction of the source. As a result, originating callers hear their own voice reflected back. Sometimes, the reflected signal is reflected again, causing the destination to hear the same conversation twice.

In a traditional voice network, voice can reflect back; it usually goes unnoticed, however, because the delay is so low. In a VoIP network, echo is more noticeable because both packetization and compression contribute to delay.

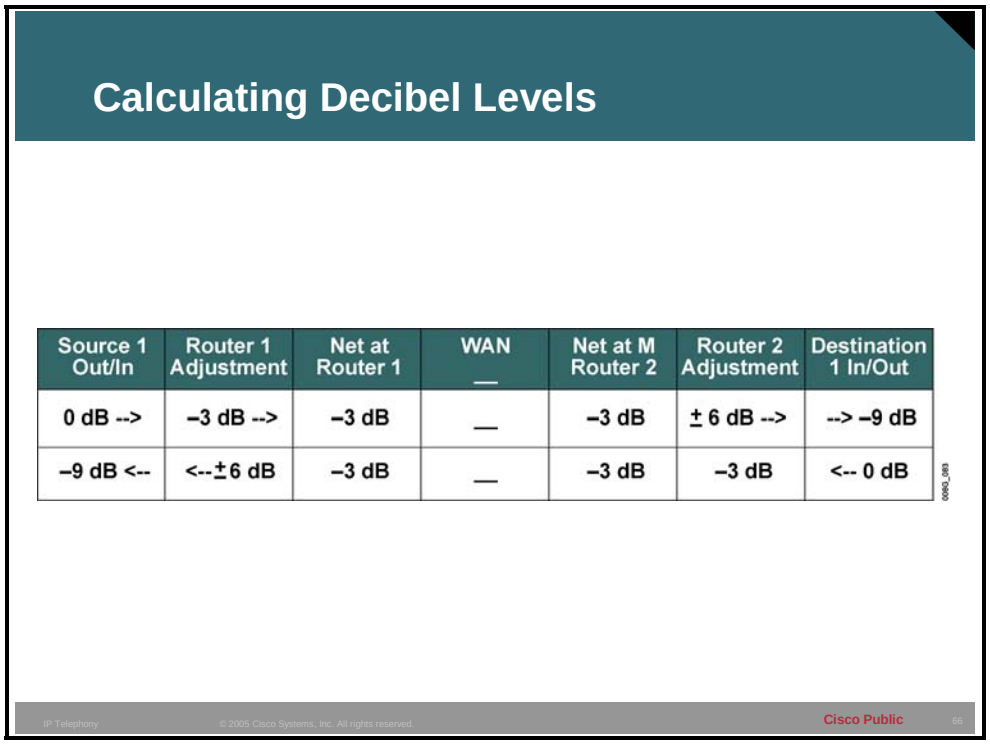
Another problem is inconsistent volume at different points in the network. Both echo and volume inconsistency may be caused by a voice port that is generating a signal level that is too high or too low. You can adjust signal strength, either in the inbound direction from an edge telephone or switch into the voice port, or in the outbound direction from the voice port to the edge telephone or switch. Echo results from incorrect input or output levels, or from an impedance mismatch. Although these adjustments are available on the Cisco voice equipment, they are also adjustable on PBX equipment.

Too much input gain can cause clipped or fuzzy voice quality. If the output level is too high at the remote router voice port, the local caller hears echo. If the local router voice port input decibel level is too high, the remote side hears clipping. If the local router voice port input decibel level is too low, or the remote router output level is too low, the remote-side voice can become distorted at a very low volume and DTMF may be missed.

Calculating Decibel Levels

Change in signal strength is measured in decibels (dBs). You can either boost the signal or attenuate it by configuring the voice port for input gain or output attenuation. You must be aware of what a voice port connects to and know at what dB level that device works best.

Calculating network dB levels is often an exercise in simple number line arithmetic. The table provides common dB levels.



Baselining Input and Output Power Levels

Considerations for baselining input and output power levels are as follows:

- Analog voice routers operate best when the receive level from an analog source is set at approximately –3 dB.
- In the United States and most of Europe, the receive (transmit) level that is normally expected for an analog telephone is approximately –9 dB. In Asian and South American

 Copyright © 2005, Cisco Systems, Inc.

countries, receive levels are closer to –14 dB. To accommodate these differences, the output levels to the router are set over a wide range.

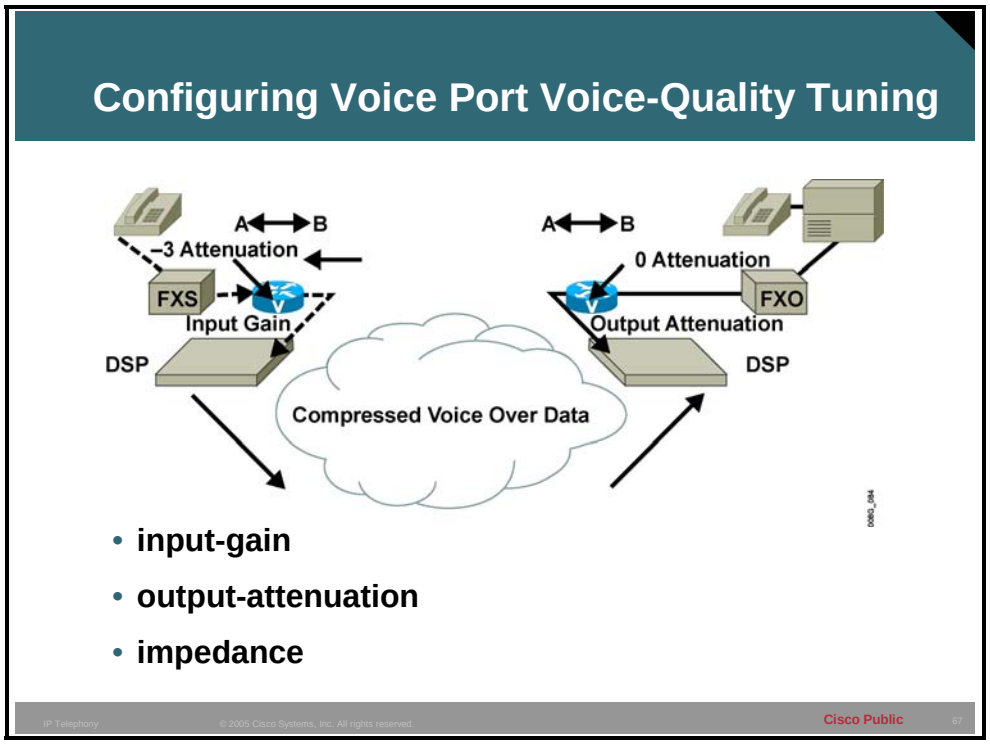
- Overdriving the circuit can cause analog clipping. Clipping occurs when the power level is above available pulse code modulation (PCM) codes, and a continuous repetition of the last PCM value is passed to the DSP.
- Echo occurs when impedance mismatches reflect power back to the source.

Example: Decibel Levels

Adjustment of decibel levels may be necessary throughout a voice network. A station connected to a PBX may experience one level of loudness when calling a local extension, a different level when dialing an outside line, and different levels when calling remote sites via VoIP. Adjustments may be necessary in this case.

Voice Quality Tuning

This topic describes voice-quality tuning configuration.



In an untuned network, a port configuration that delivers perceived good quality for a call between two dial peers might deliver perceived poor quality for a call between two other dial peers.

Voice quality adjustment is a defined, step-by-step procedure that is implemented after the network is up and running. It is ineffective for you to begin changing the default voice port configurations until full cross-network calls are established; a correctly implemented procedure results in a quality compromise between various sources that the customer accepts as good overall quality.

A variety of different factors, including input gain and output attenuation, can affect voice quality.

A loss plan looks at the required dB levels at specific interfaces, such as an analog FXS port connecting to a telephone, or an FXO port connecting to the PSTN. An analog voice router works best with a receive level of –3 dB. An analog telephone in North America and Europe works best with a receive level of –9 dB. Therefore, if the device connecting to that router provides a different level than the expected –3 dB, then input gain can be set to equalize it to –3 dB. If the output at the other end is a telephone that expects –9 dB, then the output voice port has to provide –6 dB output attenuation in addition to the –3 dB to send signaling to the telephone at the expected –9 dB levels. A systemwide loss plan looks at the dB levels of the initial input and the remote output ports and plans for the appropriate adjustments for end-to-end signal levels. You must consider other equipment (including PBXs) in the system when creating a loss plan.

 Copyright © 2005, Cisco Systems, Inc.

Configuration Parameters

Parameters for configuring voice port voice-quality tuning are as follows:

- **input-gain:** Configures a specific input gain, in decibels, to insert into the receiver side of the interface. The default value for this command assumes that a standard transmission loss plan is in effect, meaning that there must be an attenuation of –6 dB between telephones. The standard transmission plan defines country-specific dB levels and assumes that interfaces already provide the expected dB levels; for example, there must be attenuation of –6 dB between two telephones so that the input gain and output attenuation is 0, if the interfaces provide the required –6 dB attenuation.

  The gain of a signal to the PSTN can only be decreased. The gain of a signal coming into the router can be increased.

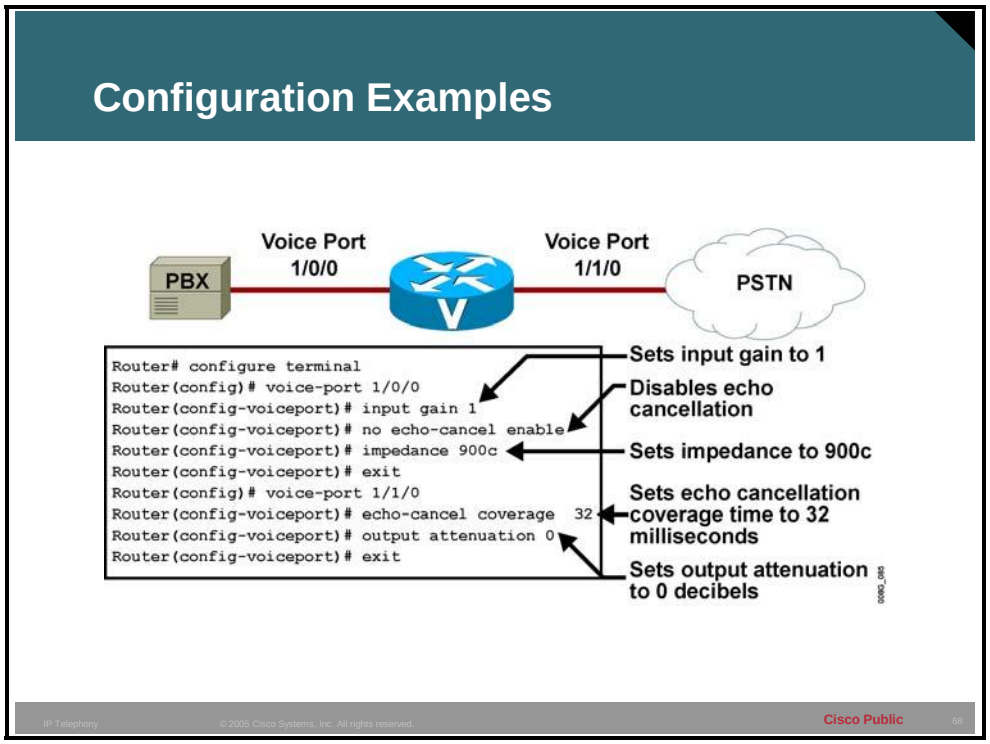
- **output-attenuation:** Configures the output attenuation value in decibels for the transmit side. The value represents the amount of loss to be inserted at the transmit side of the interface.

- **impedance:** Configures the terminating impedance of a voice port interface. The impedance value that is selected must match the setting from the specific telephony system to which it is connected. You must verify the impedance settings in the technical specifications document of the device. Impedance standards vary between countries. CO switches in the United States are predominantly 600 ohms real (600r). PBXs in the United States are normally 600r or 900 ohms complex (900c).

  Incorrect impedance settings or an impedance mismatch generates a significant amount of echo. You can mask the echo by enabling the **echo-cancel** command. In addition, gains often do not work correctly if there is an impedance mismatch.

Note	The **input-gain** and **output-attenuation** commands accommodate network equipment and are not end-user volume controls for user comfort.

Example: Voice Port Tuning



This example shows voice port tuning parameters on the E&M and FXO ports of a Cisco voice-enabled router. In the example, the PBX output is –4 dB, whereas the voice router functions best at –3 dB. Therefore, the adjustment is made in the inbound path to the router using the **input-gain** command. The impedance setting on the router needs to be changed from the default of 600r to match the 900c impedance setting for the PBX. Because this is an E&M port, echo cancellation is disabled. The FXO port connecting to the PSTN has an adjustment for echo coverage that allows for longer-distance echo cancellation.

E&M voice port parameters include:

- **input-gain:** Increases the inbound voice level by 1 dB before the voice is transmitted across the network
- **no echo-cancel enable:** Disables echo cancellation
- **impedance:** Sets the impedance to match the connecting hardware

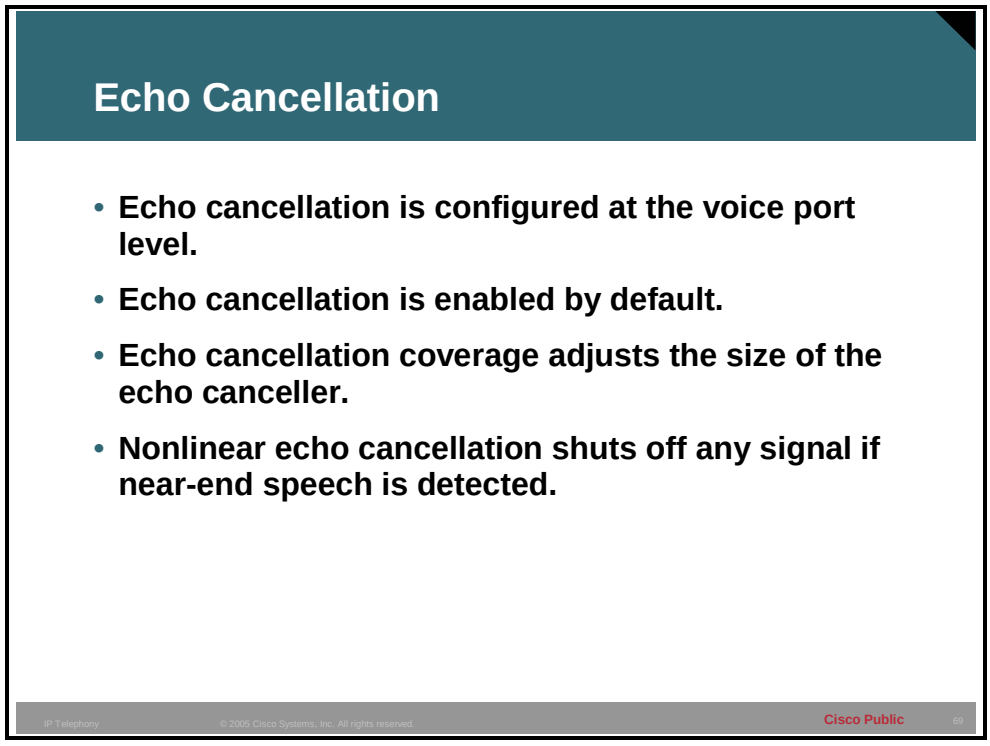
FXO voice port parameters include:

- **echo-cancel coverage:** Adjusts the cancellation coverage time to 32 ms. This allows for cancellation of echo that has greater delay.
- **output-attenuation:** Specifies that there is no attenuation as the signal is passed out of the interface to the PSTN.

 Copyright © 2005, Cisco Systems, Inc.

Echo Cancellation Commands

This topic describes echo cancellation configuration parameters.



Echo cancellation is configured at the voice port level. It is enabled by default and its characteristics are configurable. Echo cancellation commands are as follows:

- **echo-cancel enable:** Enables cancellation of voice that is sent out through the interface and received back on the same interface. Sound that is received back in this manner is perceived by the listener as echo. Echo cancellation keeps a certain-sized sample of the outbound voice and calculates what that same signal looks like when it returns as an echo. Echo cancellation then attenuates the inbound signal by that amount to cancel the echo signal. If you disable echo cancellation, it will cause the remote side of a connection to hear echo. Because echo cancellation is an invasive process that can minimally degrade voice quality, you should disable this command if it is not needed. There is no echo path for a four-wire E&M interface. The echo canceller should be disabled for this interface type.

Note	This command is valid only if the **echo-cancel coverage** command has been configured.

- **echo-cancel coverage:** Adjusts the coverage size of the echo canceller. This command enables cancellation of voice that is sent out through the interface and received back on the same interface within the configured amount of time. If the local loop (the distance from the interface to the connected equipment that is producing the echo) is longer, the configured value of this command should be extended.

  If you configure a longer value for this command, it takes the echo canceller longer to converge; in this case, the user may hear a slight echo when the connection is initially set up. If the configured value for this command is too short, the user may hear some echo for the duration of the call, because the echo canceller is not canceling the longer-delay echoes.

There is no echo or echo cancellation on the network side; for example, the non-POTS side of the connection.

Note	This command is valid only if the echo cancel feature has been enabled.

- **non-linear:** The function enabled by the **non-linear** command is also known as residual echo suppression. This command effectively creates a half-duplex voice path. If voice is present on the inbound path, then there is no signal on the outbound path. This command is associated with the echo canceller operation. The **echo-cancel enable** command must be enabled for the **non-linear** command to take effect. Use the **non-linear** command to shut off any signal if near-end speech is not detected.

  Enabling the **non-linear** command normally improves performance; however, some users encounter truncation of consonants at the ends of sentences when this command is enabled. This occurs when one person is speaking and the other person starts to speak before the first person finishes. Because the nonlinear cancellation allows speech in one direction only, it must switch directions on the fly. This may clip the end of the sentence spoken by the first person or the beginning of the sentence spoken by the second person.

Caution	Do not use the echo cancellation commands or adjust voice quality unless you are experienced in doing so. Arbitrarily adjusting these parameters could adversely affect voice quality.

ITU standard G.164 defines the performance of echo suppressors, which are the predecessors of echo cancellation technology. G.164 also defines the disabling of echo suppressors in the presence of 2100 Hz tones that precede low-bit-rate modems.

ITU standard G.165 defines echo cancellation and provides a number of objective tests that ensure a minimum level of performance. These tests check convergence speed of the echo canceller, stability of the echo canceller filter, performance of the non-linear processor, and a limited amount of double-talk testing. The signal used to perform these tests is white noise. Additionally, G.165 defines the disabling of echo cancellers in the presence of 2100 Hz signals with periodic phase reversals in order to support echo-canceling modem technology (for example, V.34), which do not work if line echo cancellation is performed in the connection.

ITU standard G.168 allows more rigorous testing and satisfies more testing requirements. White noise is replaced with a pseudo-speech signal for the convergence tests. Most echo cancellation algorithms use a least mean square algorithm to adapt the echo cancellation filter. This algorithm works best with random signals, and slows down with more correlated signals such as speech. Use of the pseudo-speech signal in testing provides a more realistic portrayal of the echo canceller's performance in real use.

Example: Echo Suppression Applied

If you speak into your telephone and hear your own voice a short time later, you are experiencing talker echo. Talker echo is caused by the remote telephony circuitry's two-wire to four-wire hybrid circuit. Enabling echo-cancellation on your voice port will eliminate the problem. Depending on the return time of the echoed voice, you can further adjust using the **echo-cancel coverage** command.

 Copyright © 2005, Cisco Systems, Inc.

Echo Canceller Comparison

This table contains echo canceller comparison information.

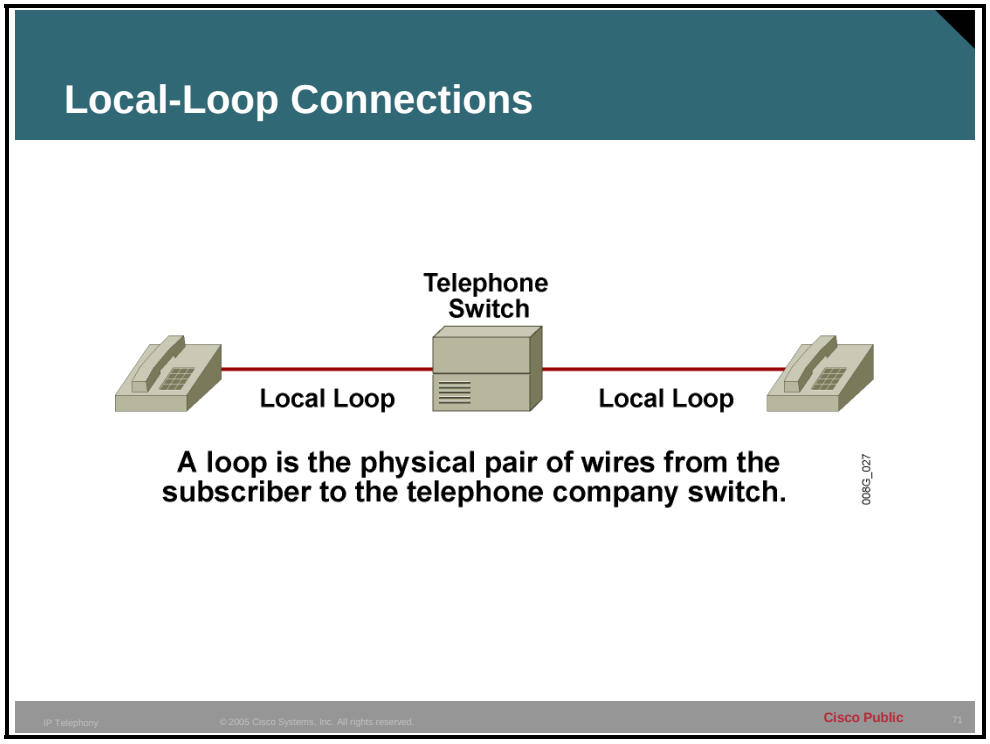
Echo Canceller Comparison

	G.165 EC	G.168 EC
Tail Coverage	Up to 32 ms	Up to 64 ms
Minimum ERL	Greater than or equal to –6 dB	Configurable to greater than or equal to –0 dB, –3 dB, or –6 dB
Echo Suppression	Up to 10 seconds	Not required due to faster convergence
Minimum Cisco IOS Software Release	12.2(11)T, 12.2(8)T5, 12.2(12), and higher	12.2(13)T, 12.2(8)YN, 12.2(15)T, 12.3(4)T, 12.3(4)XD, and higher

Analog and Digital Voice Interfaces

Local-Loop Connections

This topic describes the parts of a traditional telephony local-loop connection between a telephone subscriber and the telephone company.



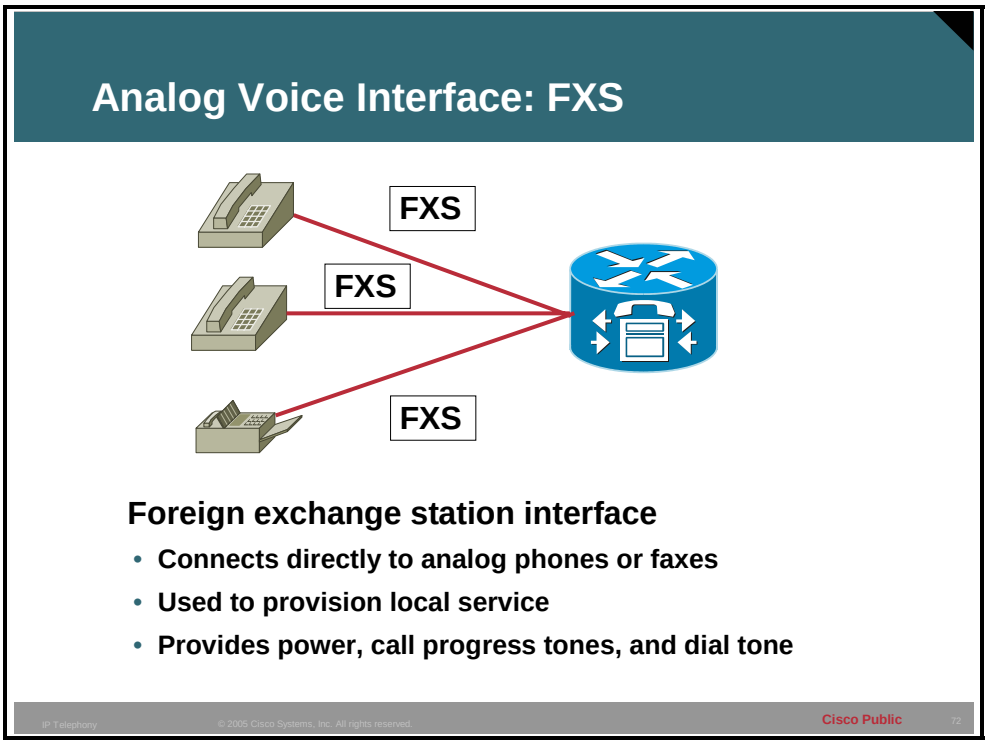
A subscriber home telephone connects to the telephone company central office (CO) via an electrical communication path called a local loop as depicted in the figure. The loop consists of a pair of twisted wires—one is called tip, the other is called ring.

In most arrangements, the ring wire ties to the negative side of a power source, called battery, while the tip wire connects to the ground. When the analog phone or fax goes to the off hook state, an electrical circuit is completed and current flows around the loop. This signals the switch that the analog phone or fax is off hook. The switch will then use a dial tone generator to send a signal that the switch is ready to receive digits. This signal is called dial tone. This wire pair which represents the local loop, along with all the others in your neighborhood, connects to the CO in a cable bundle, either buried underground or strung on poles.

 Copyright © 2005, Cisco Systems, Inc.

Analog Voice Interfaces

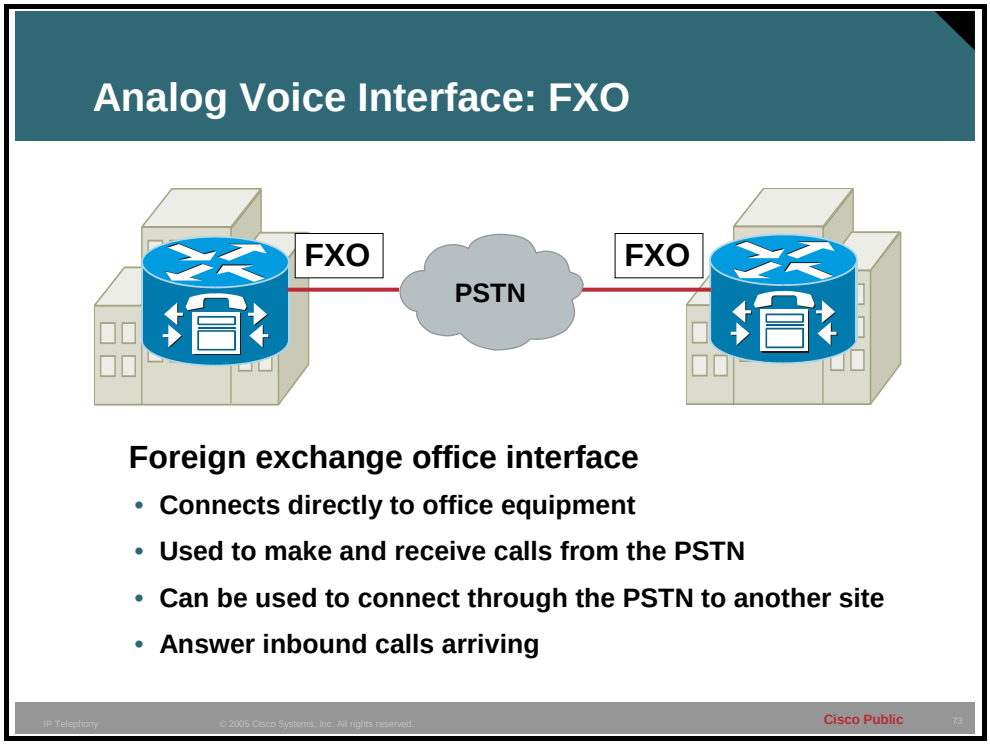
This topic defines the three analog interfaces that can be installed in a voice gateway: Foreign Exchange Station (FXS), Foreign Exchange Office (FXO), and ear and mouth (E&M). It also discusses how each of these interfaces is used.



When analog phones or fax machines are used in an IP-based environment, they will need to have a connection into this IP network. This connection takes the form of an FXS interface. The FXS interface provides a direct connection to an analog telephone, a fax machine, or a similar device. From the analog device's perspective, the FXS interface functions like a switch. Therefore, it must supply line power, ring voltage, and dial tone.

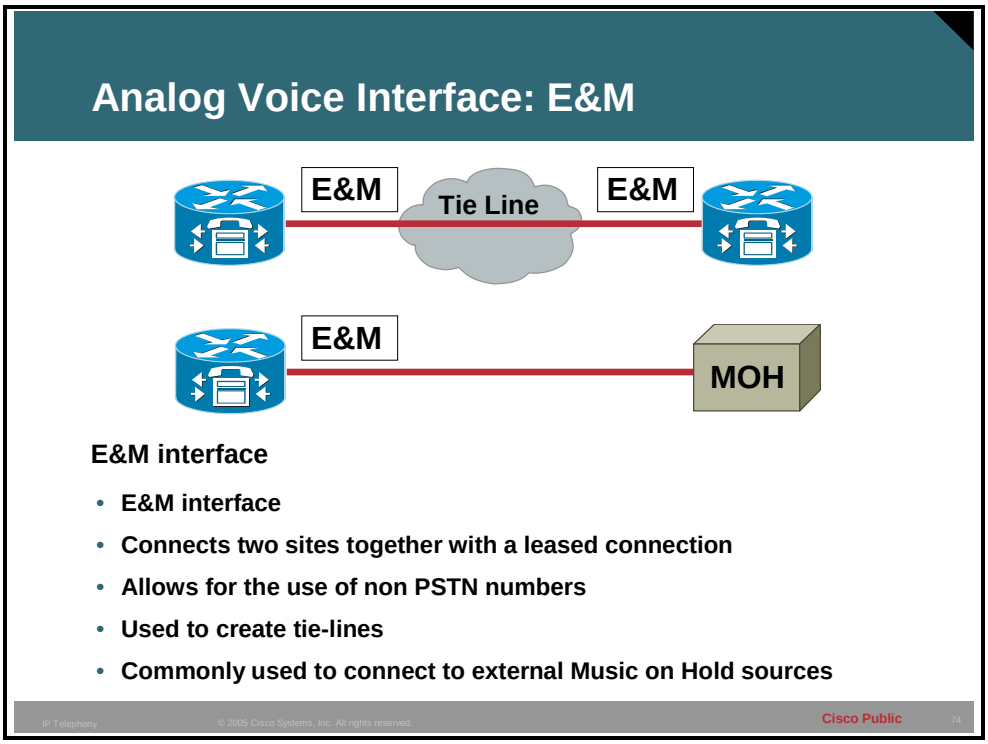
The FXS interface contains the coder-decoder (codec), which converts the spoken analog voice wave into a digital format for processing by the voice-enabled device.

Note	Analog phones plugged into an FXS port on the CallManager Express router cannot be forwarded to Unity Express voice mail. If voice mail is needed on the analog phones, use the ATA 186 or ATA 188 to connect the analog phone to the network.



For standard analog connections from the CO to enter the IP network, they will need to be terminated on an interface on a voice gateway. A Foreign Exchange Office (FXO) interface can be used for this termination of an analog line. When a call arrives, the FXO interface will answer the call and either present a second dial tone or be configured with a Private Line Auto Ringdown (PLAR). For outbound calls, the FXO interface provides either pulse or dual tone multifrequency (DTMF) digits for outbound dialing.

 Copyright © 2005, Cisco Systems, Inc.



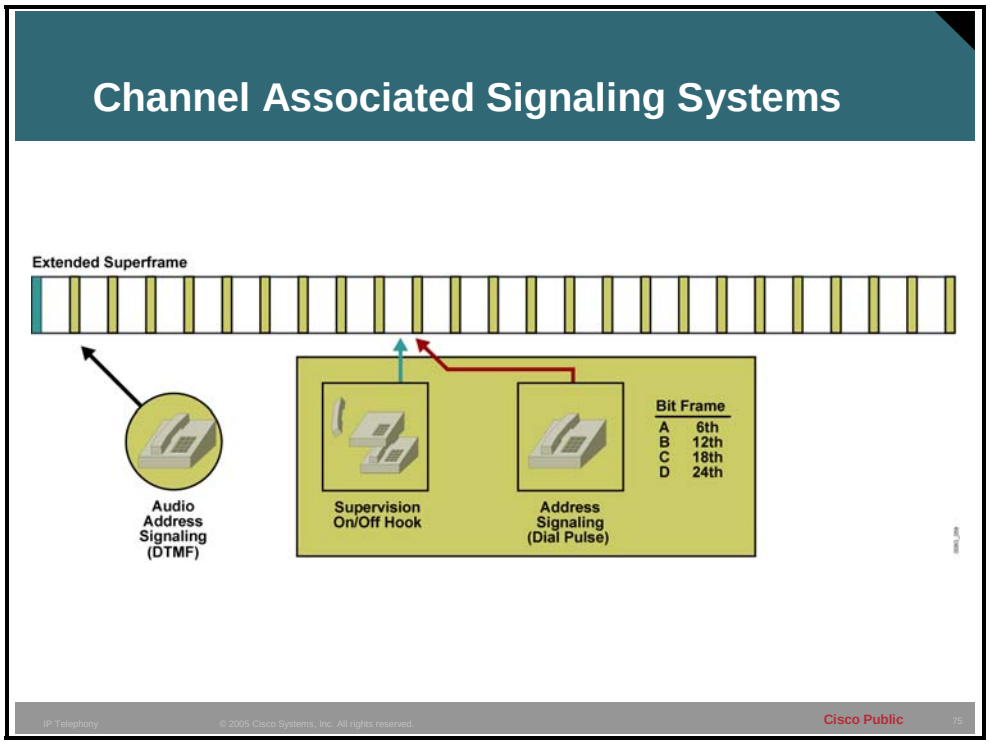
Special analog connections called tie lines can be leased from the carrier. These are typically use to tie two or mores sites together with analog connections. This tie line will terminate in an analog interface on the router so the analog communication can enter the IP network. The E&M interface on the router is where these tie lines can be terminated. E&M signaling is also referred to as “recEive and transMit,” but its origin comes from the term “earth and magneto.” Earth represents the electrical ground and magneto represents the electromagnet used to generate tone.

E&M signaling defines a trunk-circuit side and a signaling-unit side for each connection, similar to the DCE and DTE reference type. The router is usually the trunk-circuit side and the telco, CO, channel bank, or Cisco voice-enabled platform is the signaling-unit side.

Note	Many music on hold services provide an analog E&M interface that may be used to connect to the CallManager Express router.

Channel Associated Signaling Systems: T1

This topic describes CAS and its uses with T1 transmission.

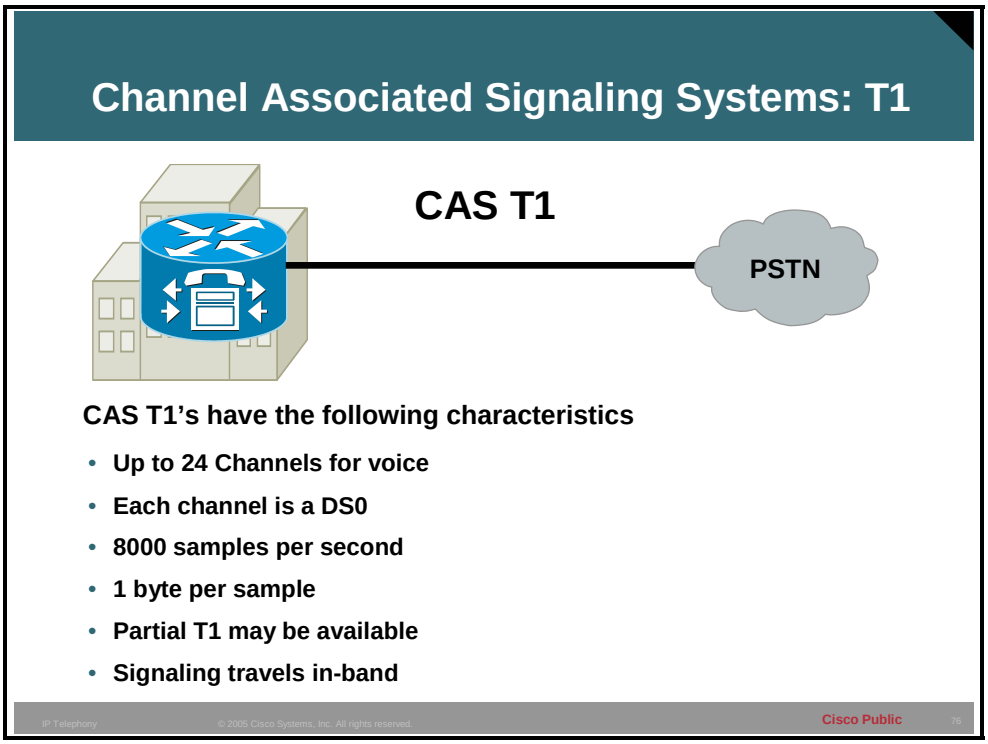


Because the signaling occurs within each DS0, it is referred to as in band. Also, because the use of these bits is exclusively reserved for signaling each respective voice channel, it is referred to as CAS.

SF has a 12-frame structure and provides AB bits for signaling. ESF has a 24-frame structure and provides ABCD bits for signaling.

Tones, such as dual tone multifrequency (DTMF) addressing or call progress, can be carried in the audio path. However, other CAS signals must be carried via the robbed bits.

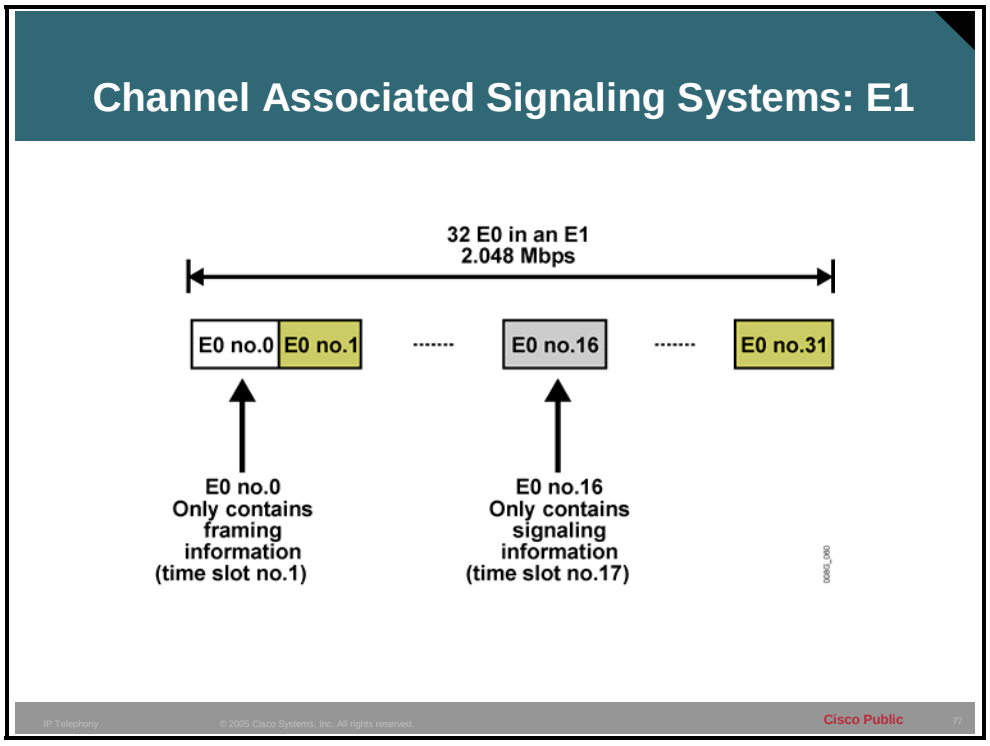
 Copyright © 2005, Cisco Systems, Inc.



CallManager Express can be connected to the PSTN through a CAS T1 connection. This will provide up to 24 channels for voice. Each channel is a 64 kb DS0.

Channel Associated Signaling Systems: E1

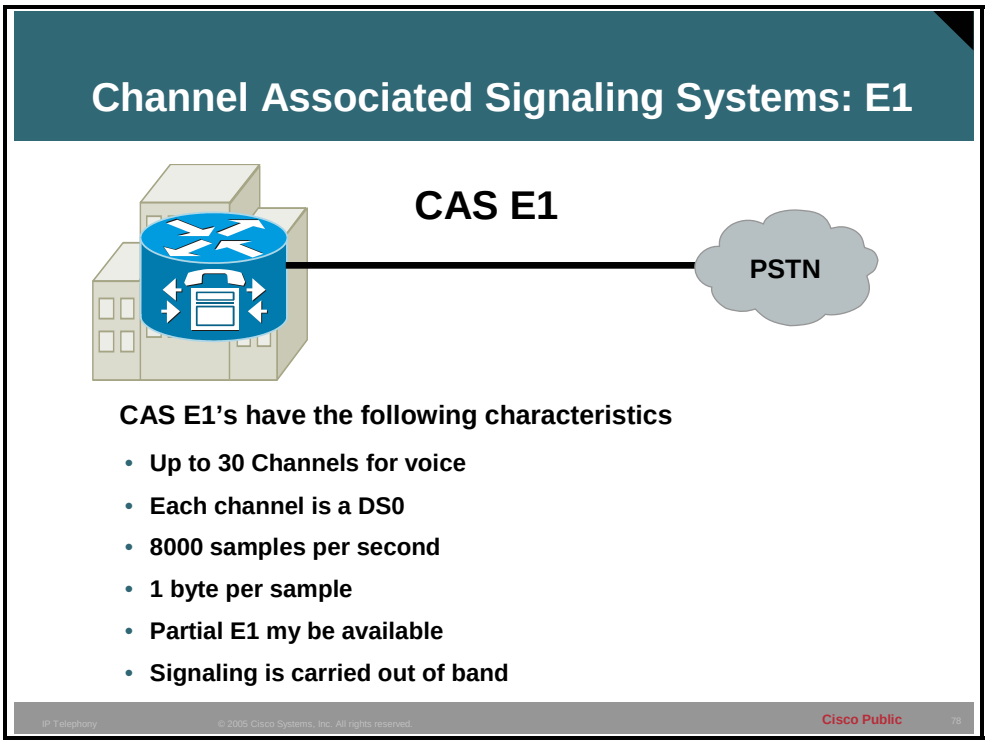
This topic describes CAS and its uses with E1 transmission.



In E1 framing and signaling, 30 of the 32 available channels, or time slots, are used for voice or data. Framing information uses time slot 1 (channel 0), while time slot 17 (channel 16) is used for signaling by all the other time slots. This signaling format is also known as CAS because each bearer channel has specific bits in the 17th timeslot assigned for signaling. However, this implementation of CAS is considered out of band because the signaling bits are not carried within the voice channel, as is the case with T1.

Note	Robbed bit signaling is not used in E1 circuits.

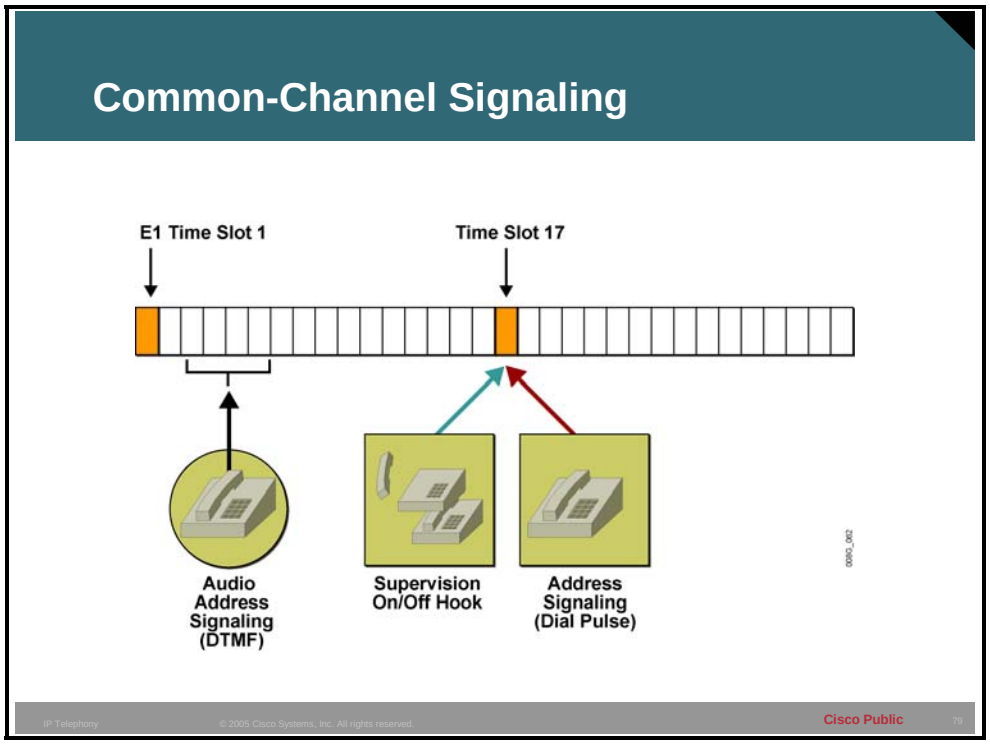
 Copyright © 2005, Cisco Systems, Inc.



CallManager Express can be connected to the PSTN and can provide up to 30 channels for voice.

Common Channel Signaling Systems

This topic describes common channel signaling (CCS) systems.



Whereas CAS uses bit time slots assigned to each specific channel, CCS uses a common channel and protocol to setup calls for all the bearer channels. Using ISDN over E1 as an example, the signaling protocol Q931 would use timeslot 17 to exchange call-setup messages for any of the 30 bearer (B) channels.

Examples of CCS signaling are as follows:

- **Proprietary implementations:** Some PBX vendors choose to implement a proprietary CCS protocol between their PBXs for T1 and E1. In this implementation, Cisco devices are configured for Transparent-Common Channel Signaling (T-CCS) because they do not understand proprietary signaling information and must simply transport the signaling without modification or interpretation.

- **ISDN:** Uses Q.931 in a common channel to signal all other channels

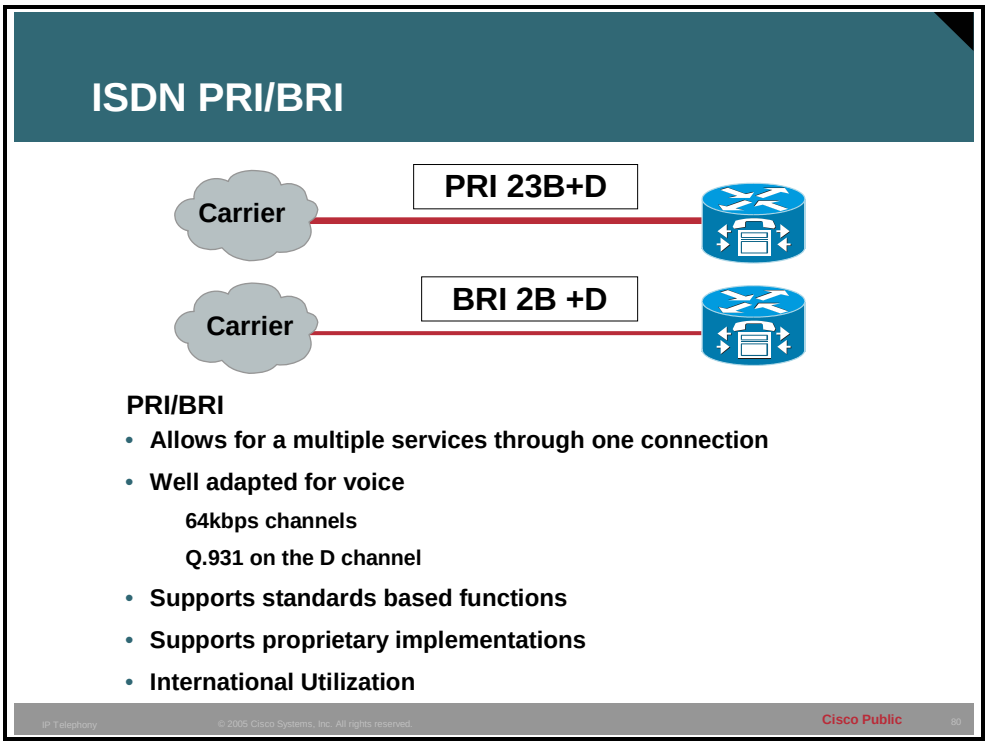
- **Digital Private Network Signaling System (DPNSS):** An open standard developed by British Telecom for implementation by any vendor who chooses to use it. DPNSS also uses a common channel to signal all other channels.

- **Q Signaling (QSIG):** Like ISDN, uses a common channel to signal all other channels.

 Copyright © 2005, Cisco Systems, Inc.

PRI/BRI

This topic describes primary rate interface and basic rate interface and how they may be used to support voice.



One form of Common Channel Signaling is Integrated Services Digital Network (ISDN). Primary rate interface (PRI) and basic rate interface (BRI) are the two ways of implementing ISDN.

Note	Because ISDN is a digital service, the time required to setup a call is significantly less than that of an analog call.

PRI supports 23 (for T1) or 30 (for E1) bearer (B) channels while BRI features two B channels. Each implementation also supports a single data (D) channel used to carry signaling information.

The following are characteristics of ISDN PRI/BRI:

- ISDN channels may carry data, voice, or video.
- Each B channel is 64 kbps, and G.711 pulse code modulation (PCM) requires 64 kbps so this is a perfect match for voice applications.
- The D channel in BRI is 16kbps and in PRI is 64kbps
- ISDN has a built-in call-control protocol known as International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Q.931 that runs on the D channel
- ISDN can support standards-based voice features, such as call forwarding and standards-based enhanced dialup capabilities, such as Group IV fax and audio channels
- ISDN may carry vendor specific PBX features

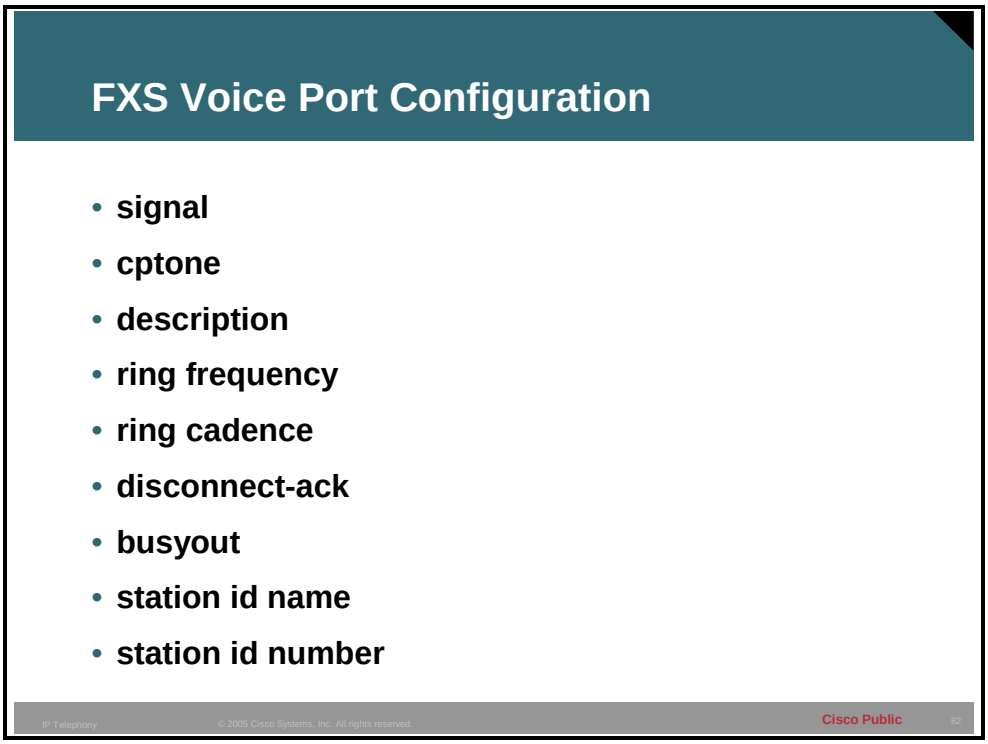
- ISDN BRI voice is commonly used in Europe; ISDN PRI voice is used worldwide.

 Copyright © 2005, Cisco Systems, Inc.

Configuring Analog and Digital Voice Interfaces

Foreign Exchange Station Ports (FXS)

FXS ports connect analog edge devices. This topic identifies the parameters that are configurable on the FXS port.



In North America, the FXS port connection functions with default settings most of the time. The same cannot be said for other countries and continents. Remember, FXS ports look like switches to the edge devices that are connected to them. Therefore, the configuration of the FXS port should emulate the switch configuration of the local PSTN.

Example

For example, consider the scenario of an international company with offices in the United States and England. The PSTN of each country provides signaling that is standard for that country. In the United States, the PSTN provides a dial tone that is different from the tone in England. When the telephone rings to signal an incoming call, the ring is different in the United States. Another instance when the default configuration might be changed is when the connection is a trunk to a PBX or key system. In that case, the FXS port must be configured to match the settings of that device.

Configuration Parameters

FXS port configuration allows you to set parameters based on the requirements of the connection if default settings need to be altered or the parameters need to be set for fine-tuning. You can set the following configuration parameters:

- **signal:** Sets the signaling type for the FXS port. In most cases, the default signaling of loopstart works well. If the connected device is a PBX or a key system, the preferred signaling is ground start. Modern PBXs and key systems do not normally use FXS ports as connections to the network, but older systems may still have these interfaces. When connecting the FXS port to a PBX or key system, you must check the configuration of the voice system and set the FXS port to match the system setting.

- **cptone:** Configures the appropriate call-progress tone for the local region. The call-progress tone setting determines the dial tone, busy tone, and ringback tone to the originating party.

- **description:** Configures a description for the voice port. You must use the description setting to describe the voice port in **show command** output. It is always useful to provide some information about the usage of a port. The description could specify the type of equipment that is connected to the FXS port.

- **ring frequency:** Configures a specific ring frequency (in Hz) for an FXS voice port. You must select the ring frequency that matches the connected equipment. If set incorrectly, the attached telephone might not ring or might buzz. In addition, the ring frequency is usually country-dependent, and you should take into account the appropriate ring frequency for your area before you configure this command.

- **ring cadence:** Configures the ring cadence for an FXS port. The ring cadence defines how ringing voltage is sent to signal a call. The normal ring cadence in North America is 2 seconds of ringing followed by 4 seconds of silence. In England, normal ring cadence is a short ring followed by a longer ring. When configured, the **cptone** setting automatically sets the ring cadence to match that country. You can manually set the ring cadence if you want to override the default country value. You may have to shut down and reactivate the voice port before the configured value takes effect.

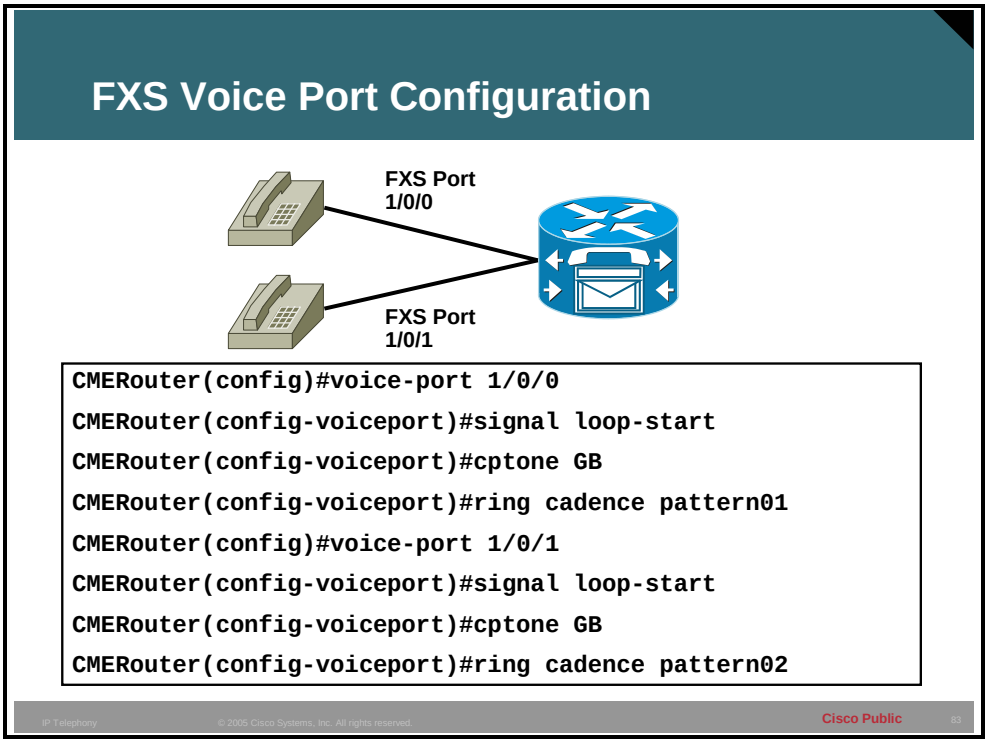
- **disconnect-ack:** Configures an FXS voice port to remove line power if the equipment on an FXS loop-start trunk disconnects first. This removal of line power is not something the user hears. Instead, it is a method for electrical devices to signal that one side has ended the call.

- **busyout:** Configures the ability to busy out an analog port.

 Copyright © 2005, Cisco Systems, Inc.

- **station id name:** Provides the station name associated with the voice port. This parameter is passed as a calling name to the remote end if the call is originated from this voice port. If no caller ID is received on an FXO voice port, this parameter will be used as the calling name. Maximum string length is limited to 15.

- **station id number:** Provides the station number that is to be used as the calling number associated with the voice port. This parameter is optional and, when it is provided, it will be used as the calling number if the call is originated from this voice port. If not specified, the calling number will be used from a reverse dial-peer search. If no caller ID is received on an FXO voice port, this parameter will be used as the calling number. Maximum string length is 15.

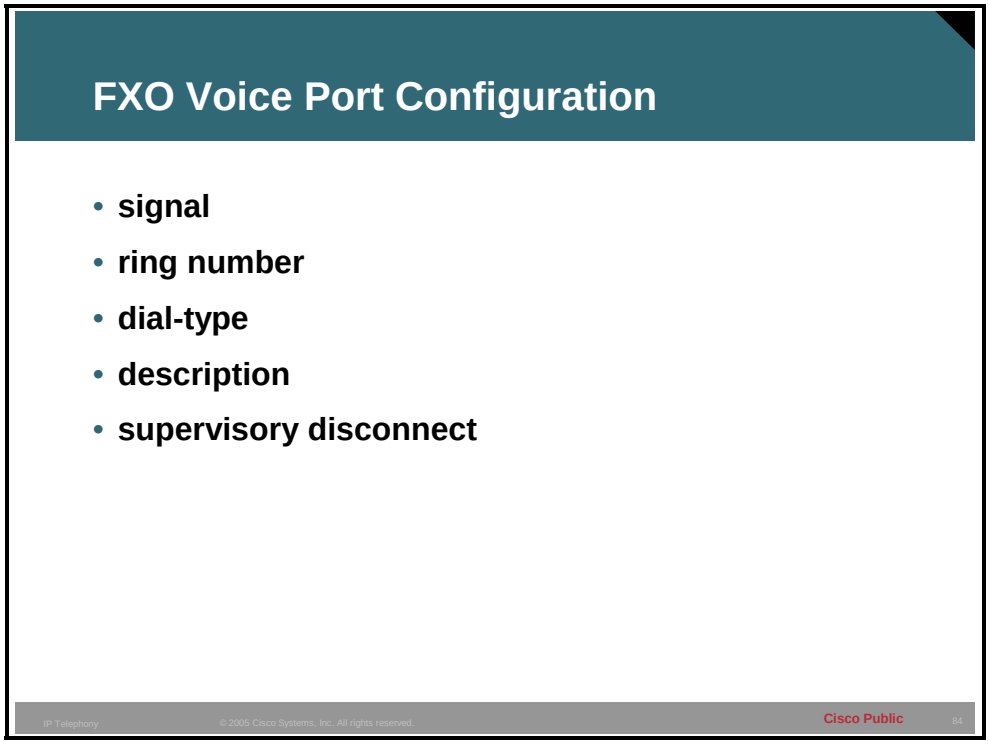


Example

The example shows how the British office is configured to enable ground-start signaling on a Cisco 2600 or 3600 series router on FSX voice port 1/0/0. The call-progress tones are set for Great Britain and ring cadence is set for pattern 1.

Foreign Exchange Office Ports (FXO)

FXO ports act like telephones and connect to central office (CO) switches or to a station port on a PBX. This topic identifies the configuration parameters that are specific to FXO ports.



Configuration Parameters

In most instances, the FXO port connection functions with default settings. FXO port configuration allows you to set parameters based on the requirements of the connection where default settings need to be altered or parameters set for fine-tuning. You can set the following configuration parameters:

- **signal:** Sets the signaling type for the FXO port. If the FXO port is connected to the PSTN, the default settings are adequate. If the FXO port is connected to a PBX, the signal setting must match the PBX.

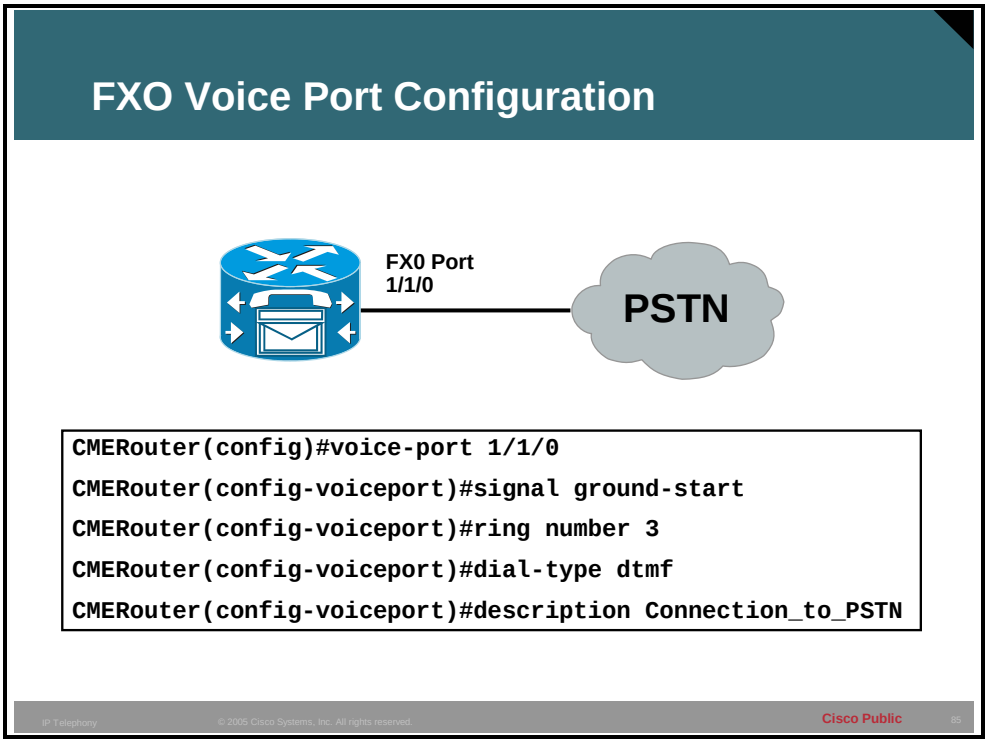
- **ring number:** Configures the number of rings before an FXO port answers a call. This is useful when you have other equipment available on the line to answer incoming calls. The FXO port answers if the equipment that is online does not answer the incoming call within the configured number of rings.

- **dial-type:** Configures the appropriate dial type for outbound dialing. Older PBXs or key sets may not support dual-tone multifrequency (DTMF) dialing. If you are connecting an FXO port to this type of device, you may need to set the dial type for pulse-dialing.

- **description:** Configures a description for the voice port. Use the description setting to describe the voice port in **show command** output.

 Copyright © 2005, Cisco Systems, Inc.

- **supervisory disconnect:** Configures supervisory disconnect signaling on the FXO port. Supervisory disconnect signaling is a power denial from the switch that lasts at least 350 ms. When this condition is detected, the system interprets this as a disconnect indication from the switch and clears the call. You should disable supervisory disconnect on the voice port if there is no supervisory disconnect available from the switch. Typically, supervisory disconnect is available when connecting to the PSTN and is enabled by default. When the connection extends out to a PBX, you should verify the documentation to ensure that supervisory disconnect is supported.

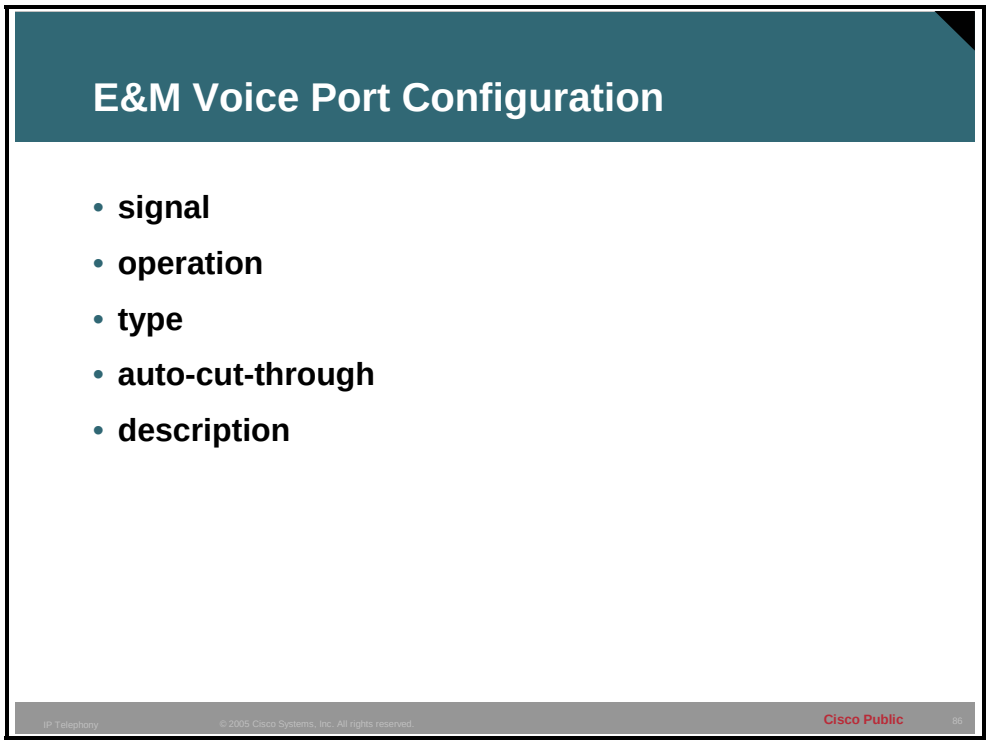


Example

The configuration in the figure enables loop-start signaling on a Cisco 2600 or 3600 series router on FXO voice port 1/1/0. The ring-number setting of **3** specifies that the FXO port does not answer the call until after the third ring, and the dial type is set to DTMF.

Ear and Mouth Ports (E&M)

E&M ports provide signaling that is used generally for switch-to-switch or switch-to-network trunk connections. This topic identifies the configuration parameters that are specific to the E&M port.



Configuration Parameters

Although E&M ports have default parameters, you must usually configure these parameters to match the device that is connected to the E&M port. You can set the following configuration parameters:

- **signal:** Configures the signal type for E&M ports and defines the signaling that is used when notifying a port to send dialed digits. This setting must match that of the PBX to which the port is connected. You must shut down and reactivate the voice port before the configured value takes effect. With **wink-start** signaling, the router listens on the M lead to determine when the PBX wants to place a call. When the router detects current on the M lead, it waits for availability of digit registers and then provides a short *wink* on the E lead to signal the PBX to start sending digits. With **delay-start**, the router provides current on the E lead immediately upon seeing current on the M lead. When current is stopped for the digit sending duration, the E lead stays high until digit registers are available. With **immediate-start**, the PBX simply waits a short time after raising the M lead and then sends the digits without a signal from the router.

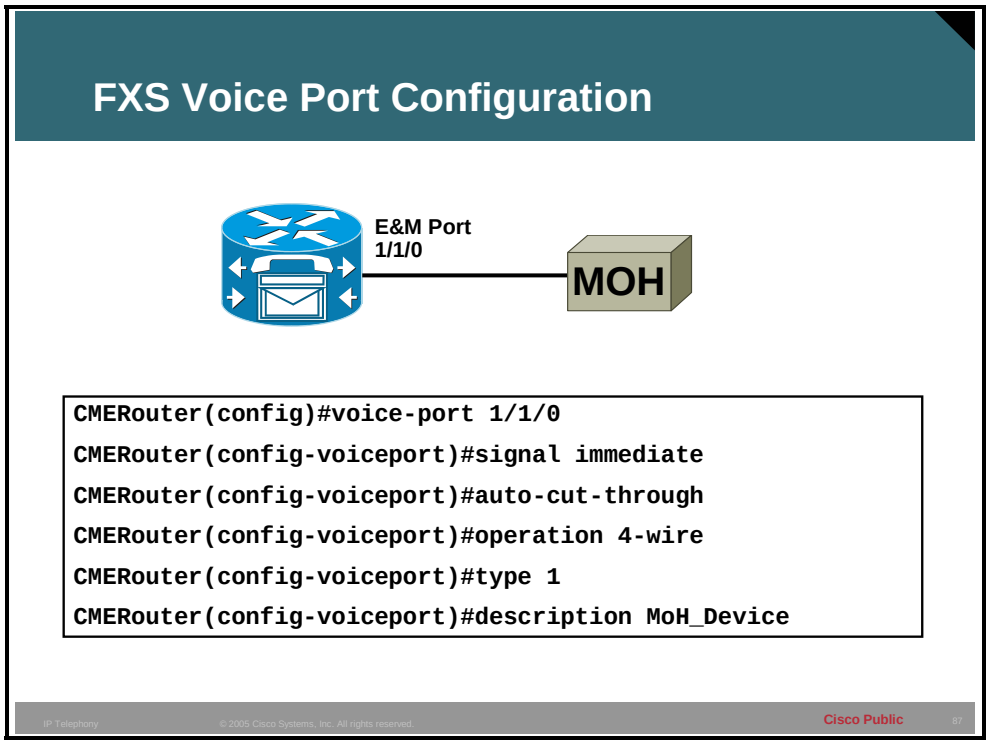
 Copyright © 2005, Cisco Systems, Inc.

- **operation:** Configures the cabling scheme for E&M ports. The **operation** command affects the voice path only. The signaling path is independent of two-wire versus four-wire settings. If the wrong cable scheme is specified, the user may get voice traffic in one direction only. You must verify with the PBX configuration to ensure that the settings match. You must then shut down and reactivate the voice port for the new value to take effect.

- **type:** Configures the E&M interface type for a specific voice port. The type defines the electrical characteristics for the E and M leads. The E and M leads are monitored for on-hook and off-hook conditions. From a PBX perspective, when the PBX attempts to place a call, it goes high (off hook) on the M lead. The switch monitors the M lead and recognizes the request for service. If the switch attempts to pass a call to the PBX, the switch goes high on the E lead. The PBX monitors the E lead and recognizes the request for service by the switch. To ensure that the settings match, you must verify them with the PBX configuration.

- **auto-cut-through:** Configures the ability to enable call completion when a PBX does not provide an M-lead response. For example, when the router is placing a call to the PBX, even though they may have the same correct signaling configured, not all PBXs provide the wink with the same duration or voltage. The router may not understand the PBX wink. The **auto-cut-through** command allows the router to send digits to the PBX, even when the expected wink is not detected.

- **description:** Configures a description for the voice port. Use the description setting to describe the voice port in **show command** output.



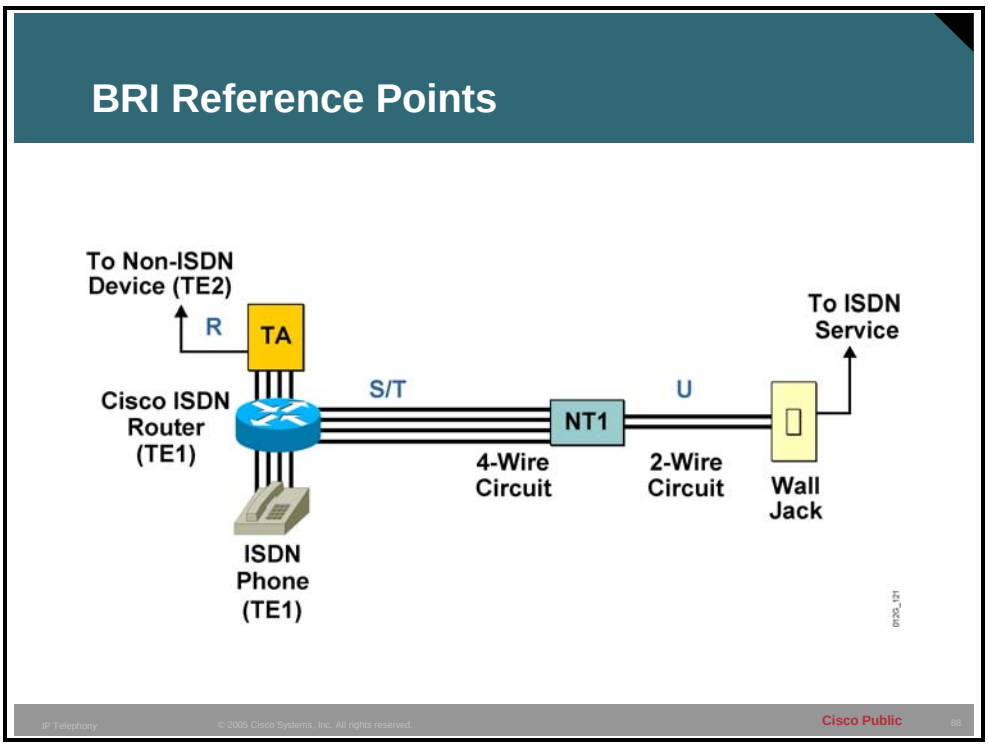
Example

The configuration in the figure enables immediate signaling with automatic cut through for an E&M connection to a Music on Hold device. This allows an external device to provide music on hold to the CallManager Express system. The **type** setting matches the E&M port setting on the MOH device as well as the number of wires used by the **operation** command.

 Copyright © 2005, Cisco Systems, Inc.

Common Channel Signaling (CCS): ISDN BRI

ISDN BRI includes various components and reference points. This topic identifies the most common components and reference points of ISDN BRI.



Given all the ISDN interface abbreviations such as T, S, U, S/T, and so on, what do all of these components and reference points look like in practice?

When creating a network, connect the network termination 1 (NT1) to the wall jack with a standard two-wire connector, then to the ISDN phone, terminal adapter, Cisco ISDN router, and maybe a fax with a four-wire connector. The S/T interface is implemented using an eight-wire connector (two pairs for data transmission and two pairs for providing optional power to the NT and TE).

Caution should be taken when connecting ISDN devices, since RJ-11 and RJ-45 connectors look similar.

The S/T reference point is:

- Four-wire interface (sending [TX] and receiving [RX])
- Point-to-point and multipoint (passive bus), as shown in the figure
- Covered by International Telecommunication Union Telecommunication Standardization Sector (ITU-T) I.430 physical layer specification for BRI interfaces, and American National Standards Institute (ANSI) T1.601 standard for the United States

The S/T interface defines the interface between a TE1 or TA and an NT. A maximum of eight devices can be daisy-chained to the S/T bus.

The U interface defines the two-wire interface between the NT1 and the ISDN cloud. The U interface is used in the United States, while in the rest of the world uses an S/T interface.

The R interface defines the interface between the TA and an attached non-ISDN device (TE2).

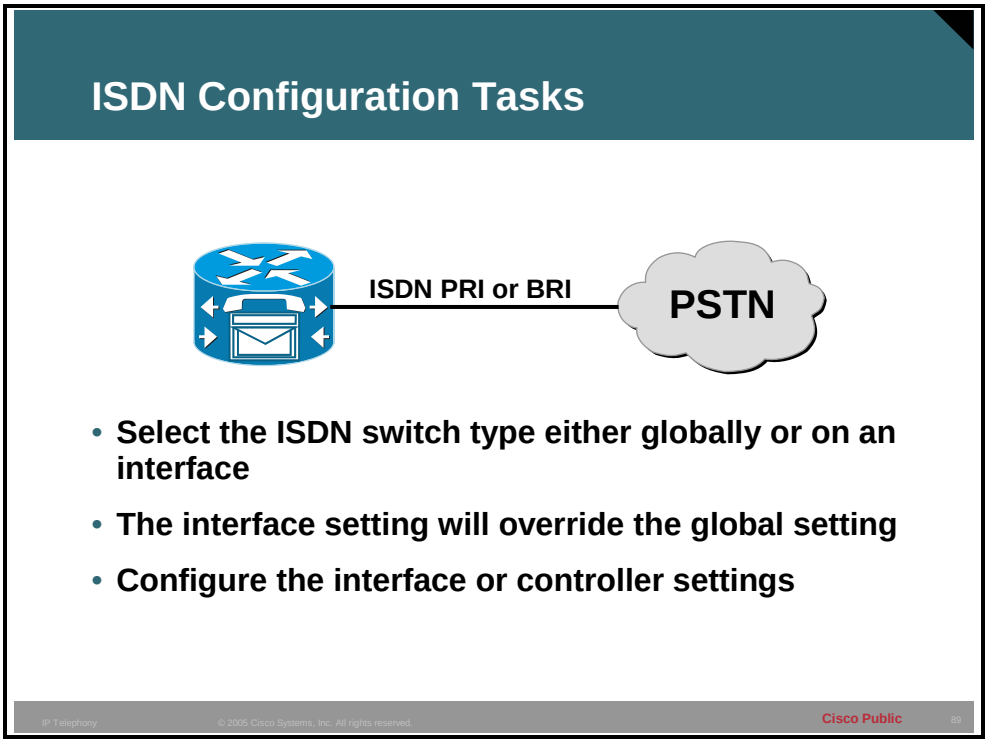
In North America, the NT1 function is commonly integrated into the ISDN device (router, TA), thus permitting a direct connection from the ISDN device to the telco jack.

An NT1 and NT2 combination device is sometimes referred to as an NTU. In most countries, the NT1/NT2 combination is provided by the service provider (telco) and customer access is only available at the S/T interface.

 Copyright © 2005, Cisco Systems, Inc.

Common Channel Signaling (CCS): ISDN Configuration Tasks

Configuring ISDN BRI requires global and interface configuration tasks. This topic provides a list of configuration tasks required to successfully configure an ISDN BRI connection.

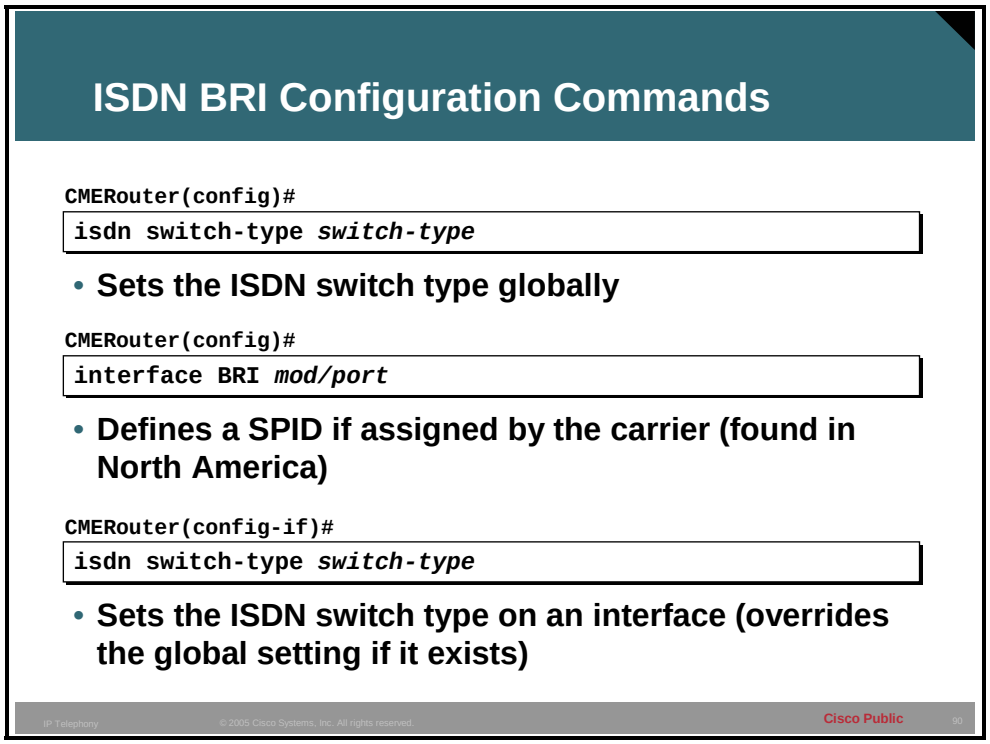


To configure an ISDN BRI interface on a router, global and interface configuration commands must be specified.

- Global configuration tasks include:
  - Select the switch type that matches the ISDN provider switch at the central office (CO).
  - Set destination details. Indicate static routes from the router to other ISDN destinations.
  - Specify the traffic criteria that initiate an ISDN call to the appropriate destination.
- Interface configuration tasks include:
  - Select the ISDN BRI port and configure an IP address and subnet mask.
  - Although the interface automatically inherits the global switch-type setting, some configurations may require a specific switch type to be configured on an interface.
  - Configure optional features, including time-to-wait for the ISDN carrier to respond to the call, and seconds of idle time before the router times out and drops the call.

Common Channel Signaling (CCS): Overview of ISDN BRI Configuration Commands

Configuring ISDN BRI requires global and interface configuration commands. This topic provides an overview of configuration commands required to successfully configure an ISDN BRI connection.



At the global level, the administrator must specify the ISDN service provider CO switch type. There are several types of switches to choose from and some of these require special parameters. Standards signaling specifics differ by region. Therefore, the switch type varies according to its geographical location. For example, the DMS-100 and National-1 require a service profile identifier (SPID) to be specified. This is optional on some switches (for example, AT&T 5ESS), or not required at all.

Although the interface configuration and selection tasks apply to all routers, this topic focuses on BRI for access routers. PRI details for Cisco routers and access servers with T1/E1 controllers are covered later in the lesson.

The **interface bri** *interface-number* command designates the interface used for ISDN on a router acting as a TE1 device.

A router without a native BRI interface is a TE2 device. It must connect to an external ISDN TA via a serial interface. On a TE2 router, the **interface serial** *interface-number* command must be used.

Use the **isdn switch-type** command to specify the CO switch to which the router connects. For BRI ISDN service, the possible switch types and their corresponding commands are shown in the table here.

 Copyright © 2005, Cisco Systems, Inc.

isdn switch-type Commands

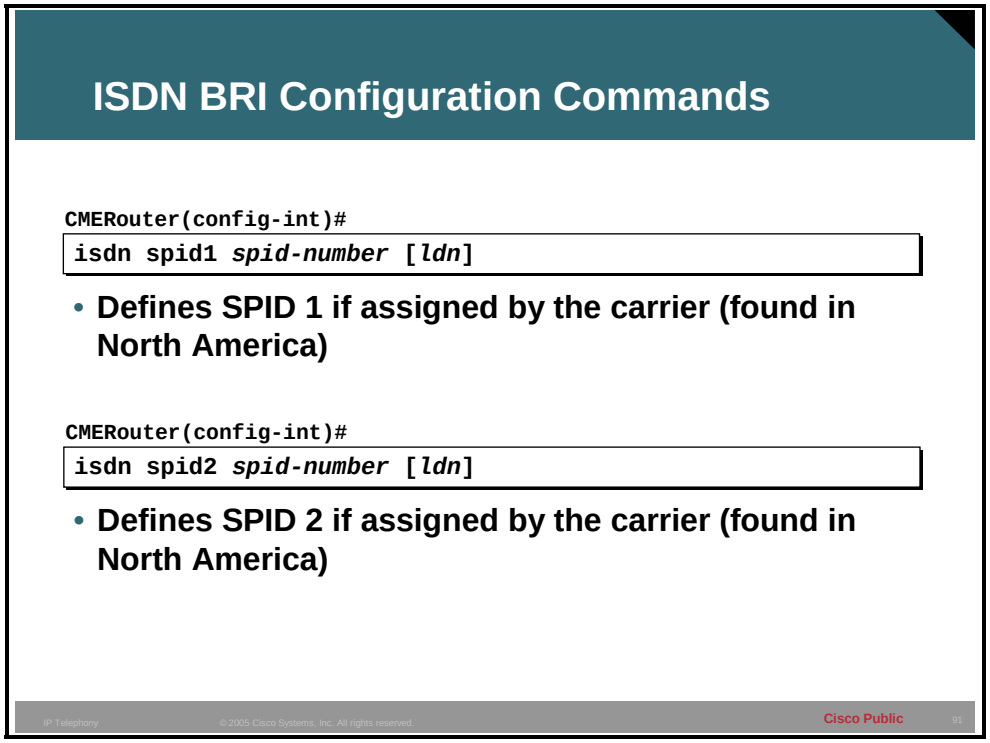
Command	Description
basic-5ess	AT&T basic rate switches (United States)
basic-dms100	NT DMS-100 (North America)
basic-ni	National ISDN-1 (North America)
basic-qsig	PINX (PBX) switches with QSIG signaling per Q.931
basic-net3	NET3 switch type for United Kingdom, Europe, Asia, and Australia
none	No switch defined

Note Other switch types are available. The list of switch types can differ based on the Cisco IOS® version used.

When the **isdn switch-type** command is used in global configuration mode, all ISDN interfaces on the router are configured for that switch type. Beginning with IOS Release 11.3T, the interface configuration mode command was introduced to allow different interfaces to be configured with different switch types. If the command is used in interface configuration mode, only the interface that is configured assumes that switch type. The interface setting always overrides the global setting.

Common Channel Signaling (CCS): ISDN BRI Configuration Commands

Selecting the correct switch type to connect is crucial when configuring ISDN BRI. This topic provides an overview of the **isdn spid** command.



Several ISDN service providers use central office switches that require dial-in numbers called service profile identifiers (SPIDs). The SPIDs are used to authenticate call requests that are within contract specifications. These switches include National ISDN and DMS-100 ISDN switches, as well as the AT&T 5ESS multipoint switch. SPIDs are used only in the United States, and are typically not required for ISDN data communications applications. The service provider supplies the local SPID numbers. If uncertain, contact the service provider to determine if the SPIDs need to be configured on your access routers.

Use the **isdn spid1** and **isdn spid2** commands to access the ISDN network when your router makes its call to the local ISDN exchange.

The **isdn spid1** command syntax is shown for the first BRI 64-kbps channel.

 Copyright © 2005, Cisco Systems, Inc.

isdn spid1 and isdn spid2 Commands

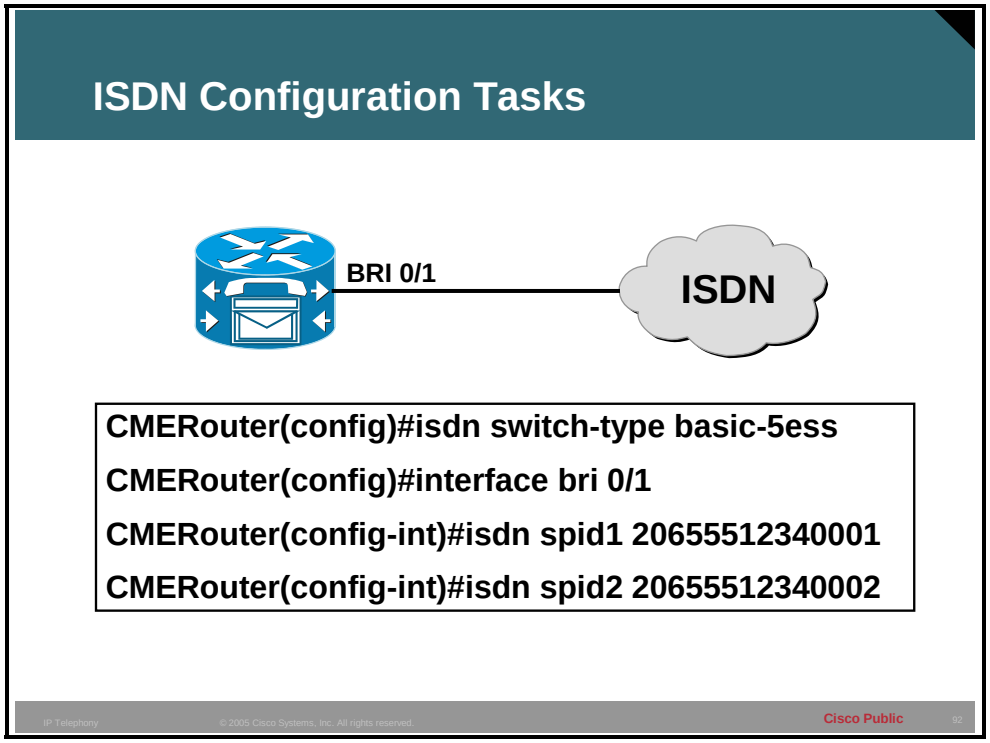
Commands	Description
spid-number	Number identifying the service to which you have subscribed. This value is usually a ten-digit telephone number followed by more digits. The ISDN service provider assigns this value.
ldn	(Optional) Seven-digit local directory number assigned by the ISDN service provider.

If you want the SPID to be automatically detected, you can specify 0 for the *spid-number* argument.

The *ldn* parameter allows you to associate up to three local directory numbers with each SPID. This number must match the called-party information coming in from the ISDN switch in order to use both B channels on most switches.

Common Channel Signaling (CCS): ISDN BRI Configuration

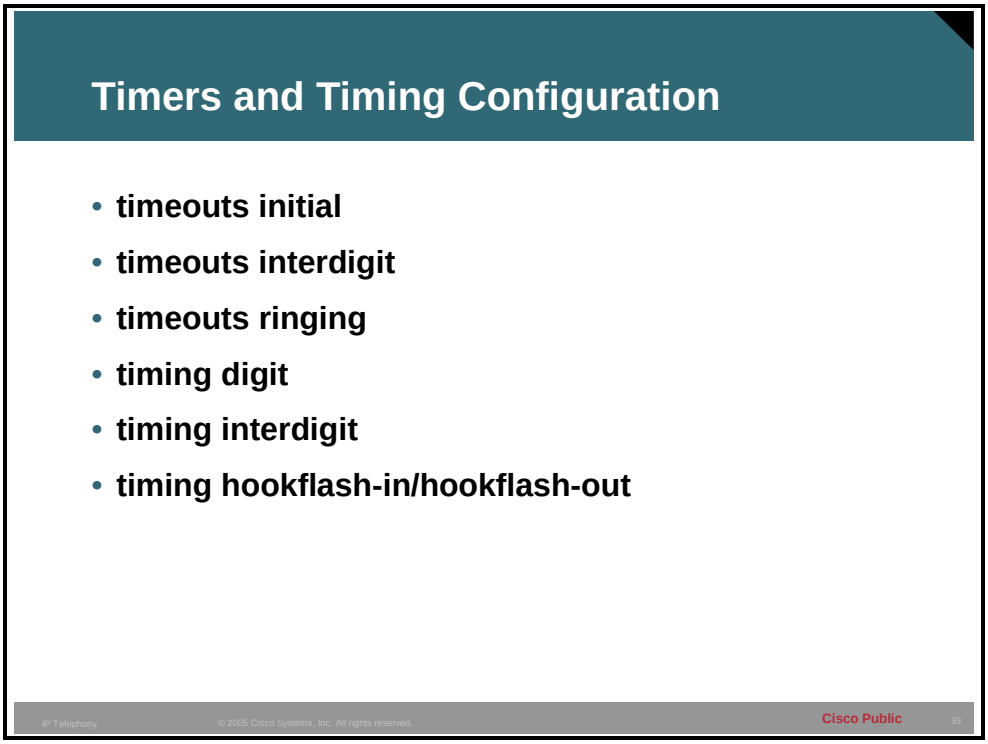
You may have to configure the Layer 2 B channel encapsulation protocol and authentication when configuring ISDN BRI.



 Copyright © 2005, Cisco Systems, Inc.

Timers and Timing

This topic identifies the timing requirements and adjustments that are applicable to voice interfaces. Under normal use, these timers do not need adjusting. In instances where ports are connected to a device that does not properly respond to dialed digits or hookflash, or where the connected device provides automated dialing, these timers can be configured to allow more or less time for a specific function.



Configuration Parameters

You can set a number of timers and timing parameters for fine-tuning the voice port. Following are voice port configuration parameters that you can set:

- **timeouts initial:** Configures the initial digit timeout value in seconds. This value controls how long the dial tone is presented before the first digit is expected. This timer typically does not need to be changed.

- **timeouts interdigit:** Configures the number of seconds for which the system will wait (after the caller has input the initial digit) for the caller to input a subsequent digit of the dialed digits. If the digits are coming from an automated device, and the dial plan is a variable length dial plan, you can shorten this timer so that the call proceeds without having to wait the full default of 10 seconds for the interdigit timer to expire.

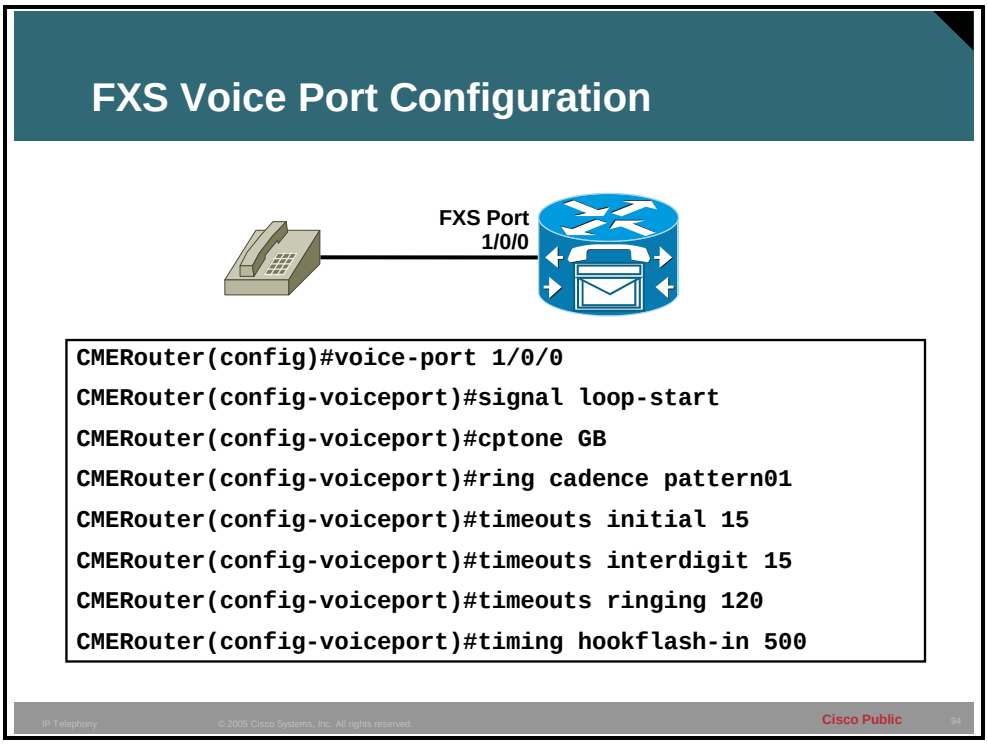
- **timeouts ringing:** Configures the length of time that a caller can continue ringing a telephone when there is no answer. You can configure this setting to be less than the default of 180 seconds so that you do not tie up the voice port when it is evident that the call is not going to be answered.

- **timing digit:** Configures the DTMF digit-signal duration for a specified voice port. You can use this setting to fine-tune a connection to a device that may have trouble recognizing dialed digits. If a user or device dials too quickly, the digit may not be recognized. By changing the timing on the digit timer you can provide for a shorter or longer DTMF duration.

- **timing interdigit:** Configures the DTMF interdigit duration for a specified voice port. You can change this setting to accommodate faster or slower dialing characteristics.

- **timing hookflash-in and hookflash-out:** Configures the maximum duration (in milliseconds) of a hookflash indication. Hookflash is an indication by a caller that the caller wishes to do something specific with the call, such as transfer the call or place the call on hold. For hookflash-in, the FXS interface processes the indication as on hook if the hookflash lasts longer than the specified limit. If you set the value too low, the hookflash may be interpreted as a hang up; the handset has to be left hung up for a longer period to clear the call if you set the value too high. For hookflash-out, the setting specifies the duration (in milliseconds) of the hookflash indication that the gateway generates outbound. You can configure this to match the requirements of the connected device.

 Copyright © 2005, Cisco Systems, Inc.

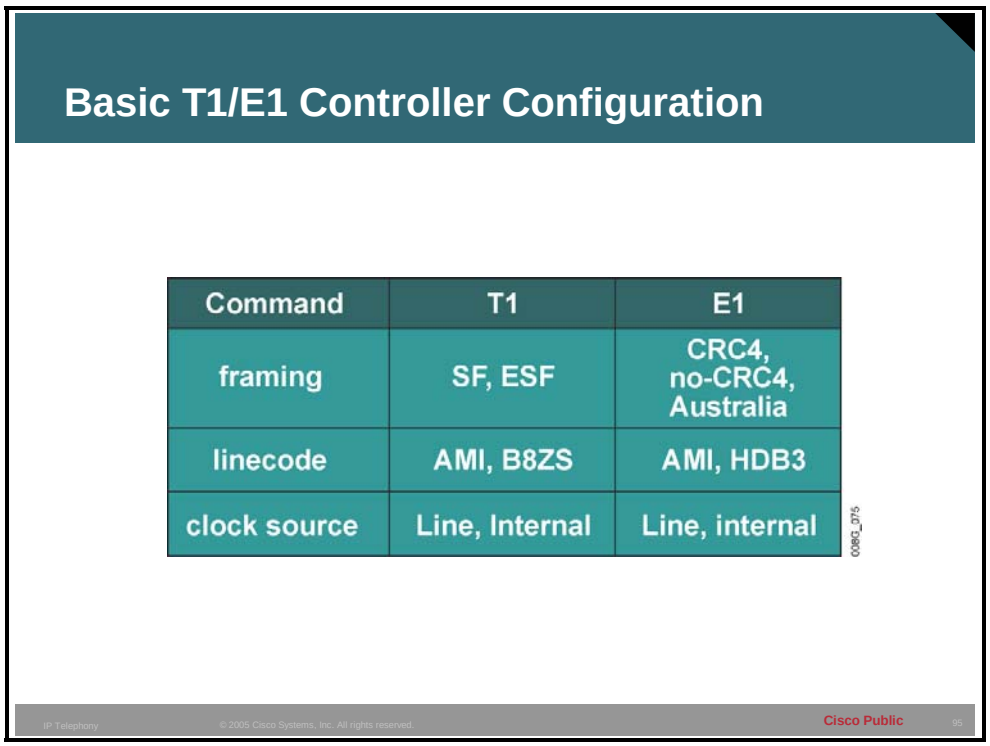


Example

The installation in the figure is for a home for the elderly where users may need more time to dial digits than in other residences. Another requirement is to allow the telephone to ring unanswered for only two minutes. The configuration in the figure enables several timing parameters on a Cisco voice-enabled router voice port 1/0/0. The initial timeout is lengthened to 15 seconds, the interdigit timeout is lengthened to 15 seconds, and the hookflash-in timer is set to 500 ms.

Digital Voice Ports

This topic identifies the configuration parameters that are specific to T1 and E1 digital voice ports.



Configuration Parameters

When you purchase a T1 or E1 connection, make sure that your service provider gives you the appropriate settings. Before you configure a T1 or E1 controller to support digital voice ports, you must enter the following basic configuration parameters to bring up the interface.

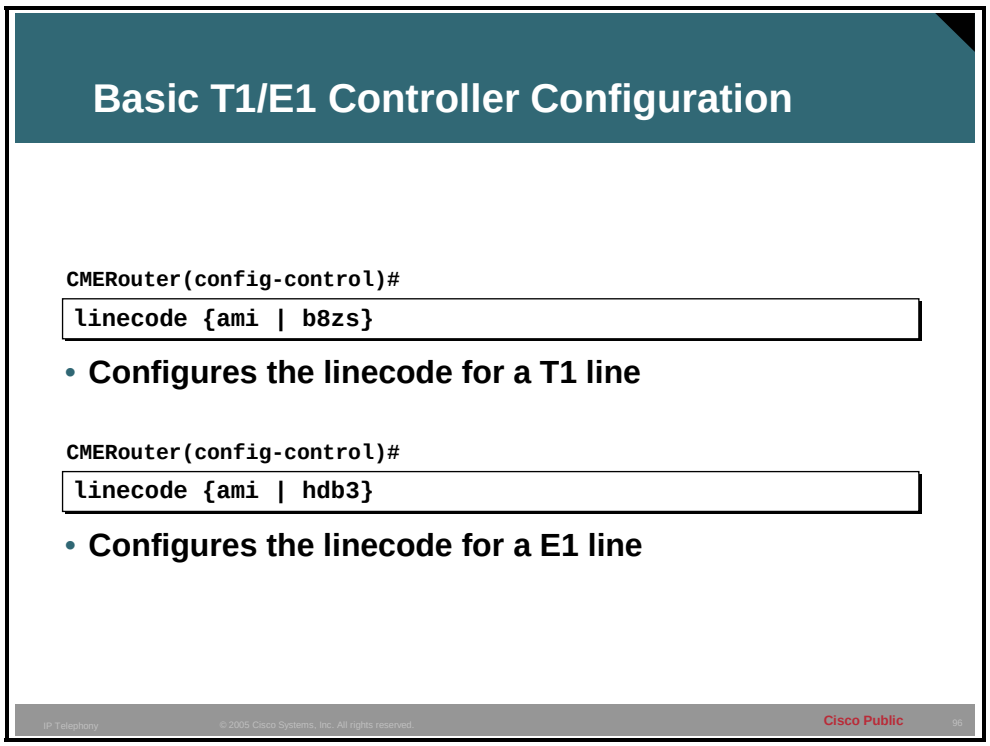
- **framing**: Selects the frame type for a T1 or E1 data line. The framing configuration differs between T1 and E1.
  - **Options for T1:** Superframe (SF) or Extended Superframe (ESF)
  - **Options for E1:** cyclic redundancy check (CRC4), no-CRC4, or Australia
  - **Default for T1:** SF
  - **Default for E1:** CRC4

 Copyright © 2005, Cisco Systems, Inc.

- **linecode:** Configures the line-encoding format for the DS1 link.
  - **Options for T1:** alternate mark inversion (AMI) or binary 8-zero substitution (B8ZS)
  - **Options for E1:** AMI or high density binary 3 (HDB3)
  - **Default for T1:** AMI
  - **Default for E1:** HDB3
- **clock source:** Configures clocking for individual T1 or E1 links.
  - **Options:** line or internal
  - **Default:** line

Channel Associated Signaling (CAS)

This topic describes the commands required to configure a Channel Associated Signaling (CAS) interface.



Use the **linecode** command to identify the physical layer signaling method to satisfy the ones density requirement on the digital facility of the provider. Without a sufficient number of ones in the digital bit stream, the switches and multiplexers in a WAN can lose their synchronization for transmitting signals. The table shows **linecode** command.

linecode Command

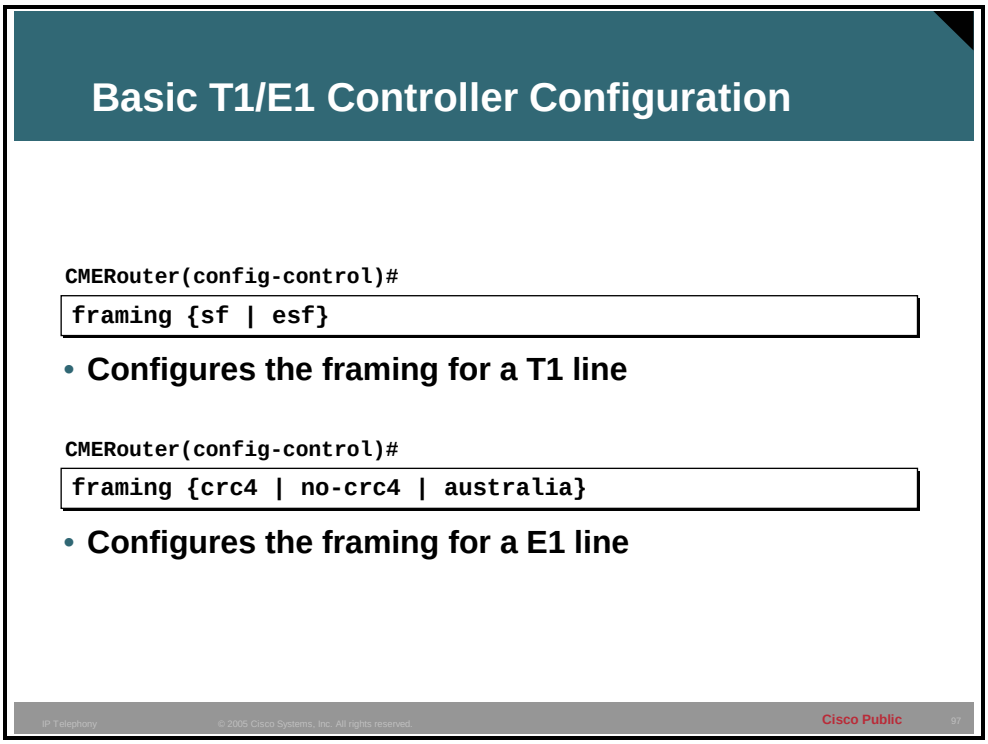
Command	Description
ami	Alternate mark inversion. Used for T1 configurations.
b8zs	Binary 8-zero substitution. Use for T1 PRI configurations.
hdb3	High density binary 3. Use for E1 PRI configurations.

Binary 8-zero substitution (B8ZS) accommodates the ones density requirements for T1 carrier facilities using special binary signals encoded over the digital transmission link. It allows 64 kbps (clear channel) for ISDN channels.

Settings for these two Cisco IOS software controller commands on the router must match the framing and line-code types used at the T1/E1 WAN central office (CO) switch of the provider.

T1 configurations typically require **framing esf** and **linecode b8zs.** E1 configurations typically require **linecode hdb3**.

 Copyright © 2005, Cisco Systems, Inc.

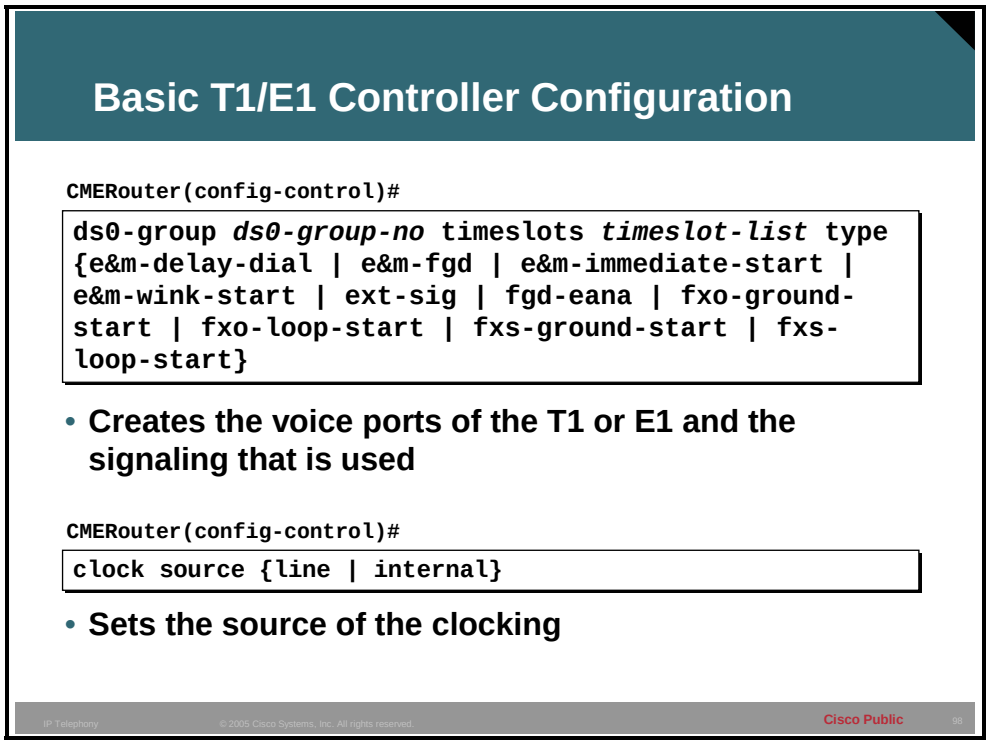


Use the **framing** controller configuration command to select the frame type used by the PRI service provider. The table shows framing commands you can use.

framing Command

Command	Description
sf	Super Frame. Use for some older T1 configurations.
esf	Extended Super Frame. Use for T1 PRI configurations.
crc4 or **no-crc4**	Cyclic redundancy check 4. Use for E1 PRI configurations.

Note Esf and crc4 are most common in new T1s or E1s



You must create a digital voice port in the T1 or E1 controller to make the digital voice port available for specific voice port configuration parameters. You must also assign timeslots and signaling to the logical voice port through configuration. The first step is to create the T1 or E1 digital voice port with the **ds0-group** *ds0-group-no* **timeslots** *timeslot-list* **type** *signal-type* command.

The **ds0-group** part of the command automatically creates a logical voice port that is numbered as *ds0-group-no*. The *dS0-group-no* parameter identifies the DS0 group (number from 0 to 23 for T1 and from 0 to 30 for E1). This group number is used as part of the logical voice port numbering scheme.

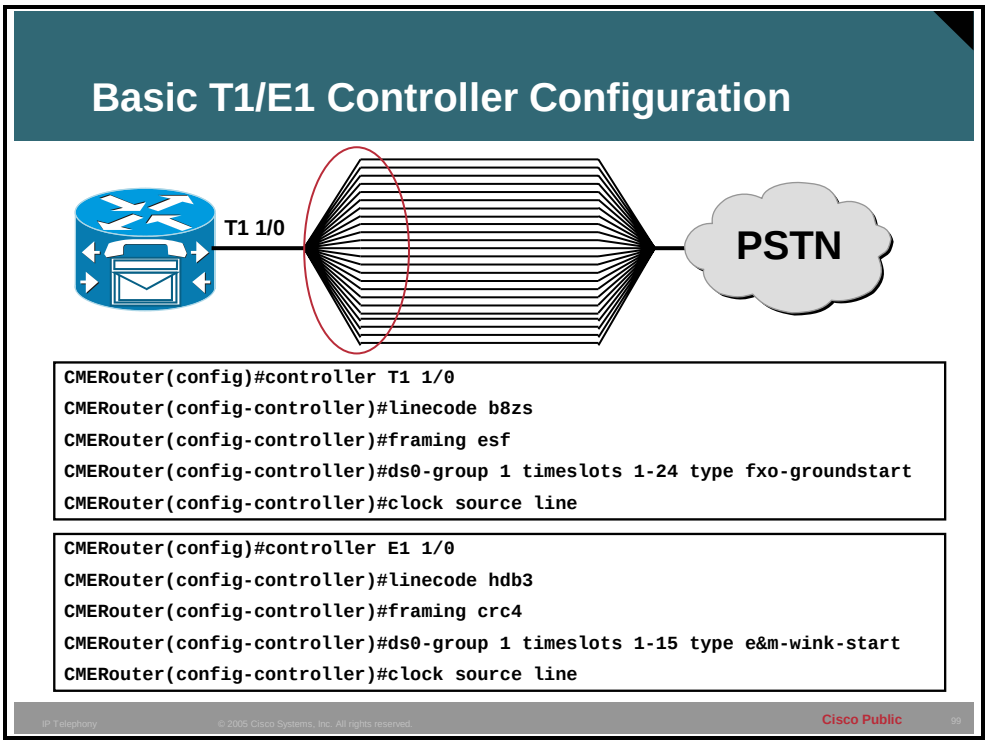
The **timeslots** part of the command allows the user to specify which timeslots are parts of the DS0 group. The *timeslot-list* parameter is a single time-slot number, a single range of numbers, or multiple ranges of numbers separated by commas.

The **type** part of the command defines the emulated analog signaling method that the router uses to connect to the PBX or PSTN. The type depends on whether the interface is T1 or E1.

To delete a DS0 group, you must first shut down the logical voice port. When the port is in shutdown state, you can remove the DS0 group from the T1 or E1 controller with the **no ds0-group** *ds0-group-no* command.

Use the **clock source** {**line** | **internal**} command to configure the T1 and E1 clock source on Cisco routers.

 Copyright © 2005, Cisco Systems, Inc.



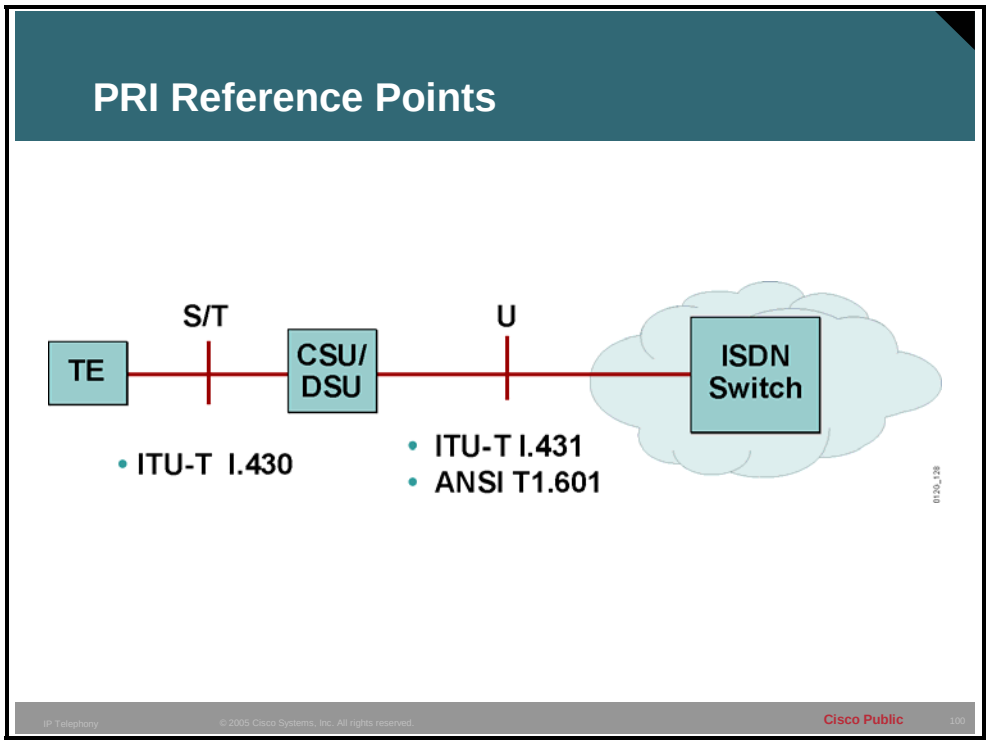
Example

This example configures the T1 controller for ESF, B8ZS linecode, and timeslots 1 through 24 with FXO ground start signaling. The resulting logical voice port is **1/0:1**, where **1/0** is the module and slot number and **:1** is the *ds0-group-no* value that was assigned during configuration.

The E1 configuration uses linecode of HDB3, framing of CRC-4, and timeslots of 1 through 15 with E&M wink start signaling. The resulting logical voice port is **1/0:1**, where the **1/0** is the module and slot number and the **:1** is the ds0-group-no value that was assigned during the configuration

Common Channel Signaling (CCS): ISDN Primary Rate Interface (PRI)

ISDN PRI includes various components and reference points. This topic identifies the most common components and reference points of ISDN PRI.



Depending on country implementation, either the ANSI T1.601 or ITU-T I.431 standard governs the physical layer of the PRI interface.

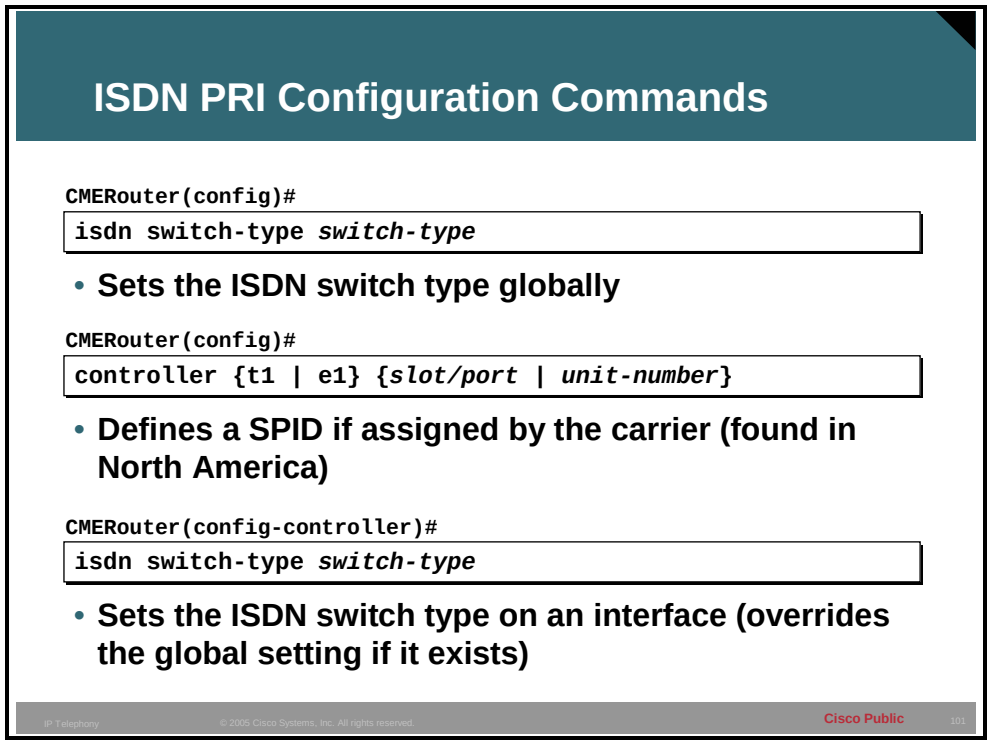
PRI technology is a bit simpler than BRI. The wiring is not multipoint, since there is only the straight connection between the channel service unit/data service unit (CSU/DSU) and the PRI interface. Multipoint refers to the ability to have multiple ISDN devices connected to the network, all of which have access to the ISDN network. Arbitration at Layer 1 and Layer 2 allows multiple devices that need to share the ISDN network to access the network without collisions or interruptions. Because there are no multiple devices, PRI does not require this arbitration.

 Copyright © 2005, Cisco Systems, Inc.

Common Channel Signaling (CCS): Overview of ISDN PRI Configuration Commands

Configuring ISDN PRI requires global and interface configuration commands.

Selecting the correct switch type to which to connect is crucial when configuring ISDN PRI. This topic provides an overview of the **isdn switch-type** command.



Use the **isdn switch-type** command to specify the central office PRI switch to which the router connects. With Cisco IOS® Release 11.3(3)T or later, this command is also available as a controller command to allow different switch types to be supported on different controllers. If configured as a global command, the specified switch type applies to all controllers, unless one is specifically configured on a controller.

An incompatible switch selection configuration can result in failure to make ISDN calls. After changing the switch type, you must reload the router to make the new configuration effective. Telco **isdn switch-type** commands are shown in the table here.

isdn switch-type Command

Command	Description
primary-4ess	AT&T Primary-4ESS switches (United States)
primary-5ess	AT&T Primary -5ESS switches (United States)
primary-dms100	NT DMS-100 switches (North America)
primary-ni	National ISDN switch type
primary-ntt	NTT ISDN PRI switches (Japan)
primary-net5	European and Australian ISDN PRI switches
primary-qsig	QSIG signaling per Q.931
None	No switch defined

Unlike BRI operation, ISDN PRIs do not use service profile identifiers (SPIDs). Therefore, there is no requirement to configure SPIDs, regardless of the ISDN switch type used by the PRI.

Use the **controller** {**t1** | **e1**} *slot/port* command in global configuration mode to identify the controller to be configured. Use a single *unit-number* to identify the AS5000 Series controller.

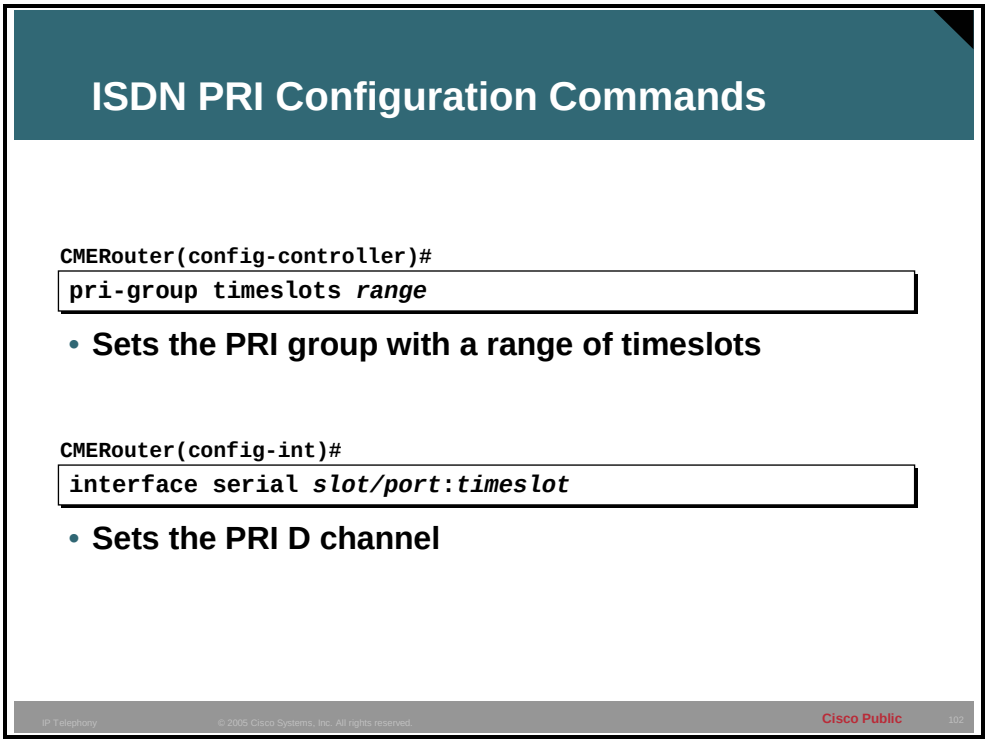
controller {t1 | e1} Command

Command	Description
t1	Specifies the controller interface for North America and Japan.
e1	Specifies the controller interface for Europe and most other countries in the world.
slot/port or *unit number*	Specifies the physical slot/port location or unit number of the controller.

 Copyright © 2005, Cisco Systems, Inc.

Common Channel Signaling (CCS): ISDN PRI Configuration Commands

Once the T1 or E1 controller is configured, the PRI channels and the corresponding D channel interface must be configured. This topic lists and explains the commands required to configure the ISDN PRI channels and D channel.



The **pri-group** command configures the specified interface for PRI operation and specifies which fixed timeslots (channels) are allocated on the digital facility of the provider.

pri-group Command

Command	Description
timeslots *range*	The range of timeslots allocated to this PRI. For T1, use values in the range of 1 to 24, and for E1, use values from 1 to 31. The speed of the PRI is the aggregate of the channels assigned.

Example #1: If using all 30 B channels on an E1 PRI (30B+D), specify **pri-group 1-31**.

Example #2: If allocated only the first eight B channels (512 kbps total data bandwidth) for a T1 PRI (23B+D), then specify **pri-group 1-8,24**. Note that the D channel must be specified.

Note	When provisioning a PRI line with less than 24 time slots (or 30 for E1), include the D channel for signaling.

Specification of the PRI group automatically creates the corresponding serial interface for the D channel: **interface serial** {*slot/port* | *unit*}**:**{**23 | 15**}. This interface is used to configure the PRI D channel. The table shows interface serial commands you can use.

interface serial Command

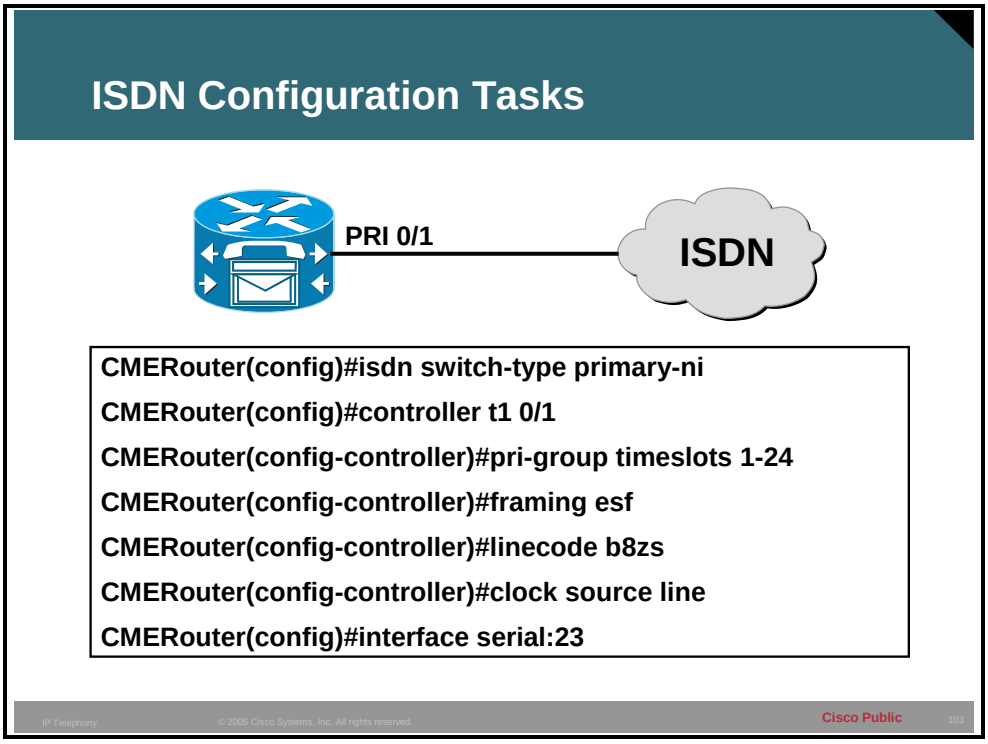
Command	Description
slot/port	The slot/port of the channelized controller.
unit	The unit number of the channelized controller on a Cisco 4000 or AS5000 Series router.
23	A T1 interface that designates channelized DS0s 0 to 22 as the B channels, and DS0 23 as the D channel.
15	An E1 interface that designates 30 B channels and timeslot 16 as the D channel.

Note In an E1 or T1 facility, the channels start numbering at 1 (1 to 31 for E1 and 1 to 24 for T1). Serial interfaces in the Cisco router start numbering at 0. Therefore, channel 16, the E1 signaling channel, is serial port subinterface 15. Channel 24, the T1 signaling channel, is serial subinterface 23.

 Copyright © 2005, Cisco Systems, Inc.

Common Channel Signaling (CCS): Sample ISND PRI Configuration

The following topic highlights a sample ISDN PRI configuration.



The table describes the commands found in the figure.

PRI Configuration Commands

Command	Description
isdn switch-type primary-ni	Selects a switch type of National ISDN
controller t1 0/1	Selects the T1 controller 0/0.
pri-group timeslots 1–24	Establishes the interface port to function as PRI with 24 timeslots (including D channel) designated to operate at a speed of 64 kbps.
framing esf	Selects Extended Superframe (ESF) framing, a T1 configuration feature.
linecode b8zs	Selects line code B8ZS for T1.
clock source line	Specifies the T1 line as the clock source for the router.
interface serial 0/0:23	Identifies the D channel on serial interface 0/0.

The **controller t1 0/1** command configures the T1 controller. In the example, the switch type selected using the national ISDN standard. This example is accurate for some operations in the United States.

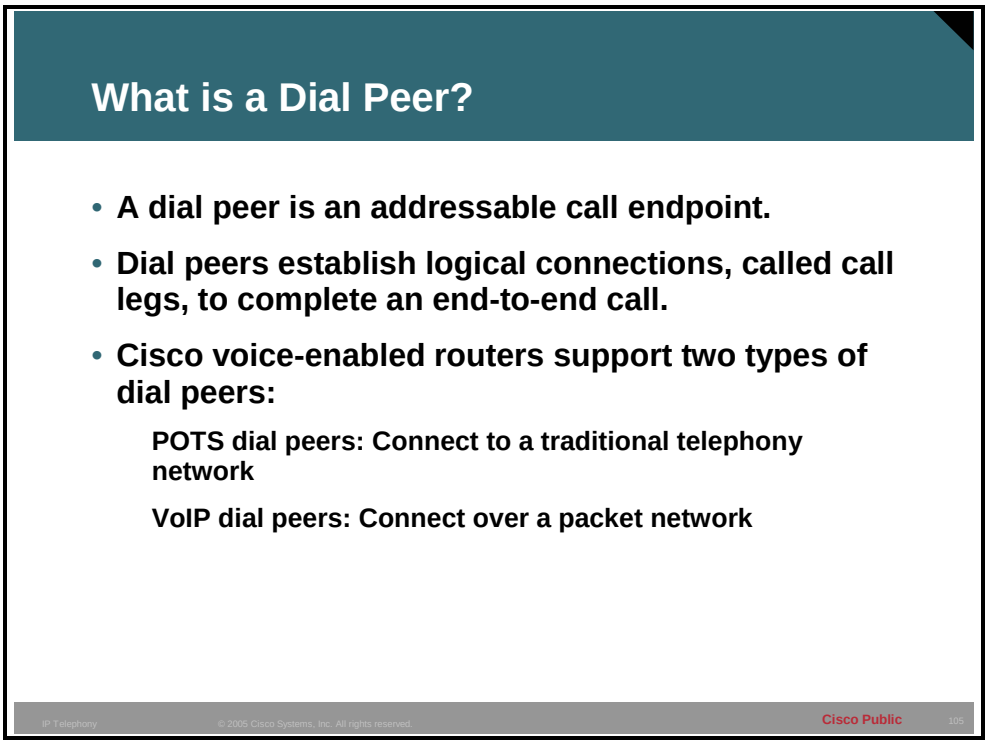
For an E1 example, the timeslot argument for the **pri-group** command would be **1–31** rather than **1–24** as shown for a T1 example, and the interface command would be **0/1:15** instead of **0/1:23**.

 Copyright © 2005, Cisco Systems, Inc.

Dial Peers

What is Dial Peer?

This topic describes dial peers and their applications.



When a call is placed, an edge device generates dialed digits as a way of signaling where the call should terminate. When these digits enter a router voice port, the router must have a way to decide whether the call can be routed, and where the call can be sent. The router does this by looking through a list of dial peers.

A dial peer is an addressable call endpoint. The address is called a *destination pattern* and is configured in every dial peer. Destination patterns can point to one telephone number only or to a range of telephone numbers. Destination patterns use both explicit digits and wildcard variables to define a telephone number or range of numbers.

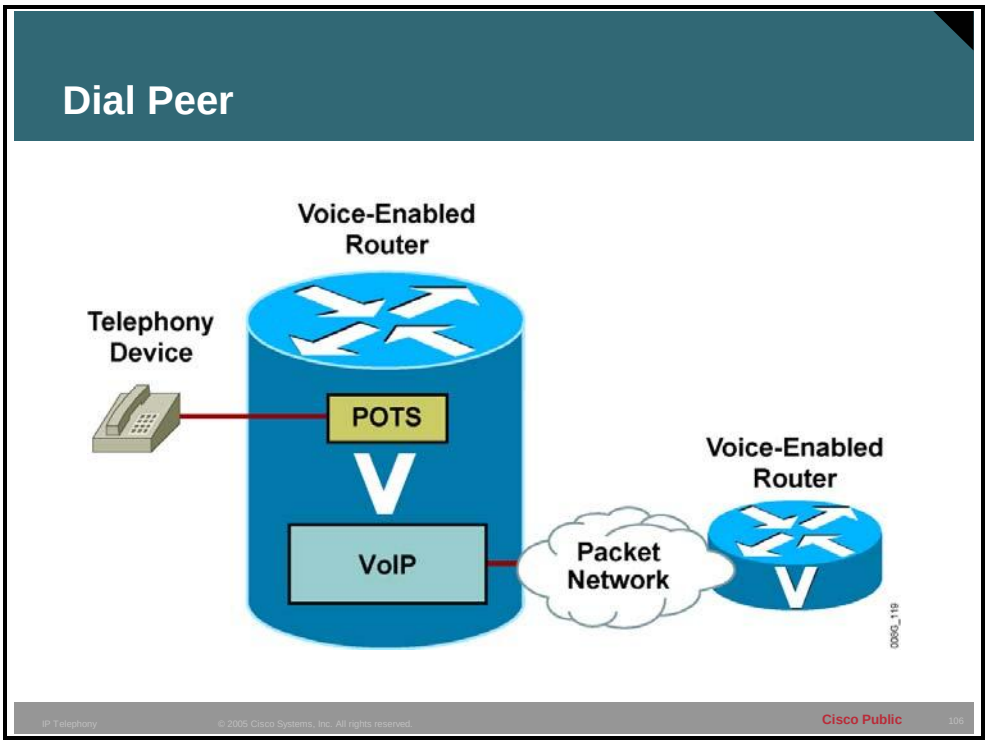
The router uses dial peers to establish logical connections. These logical connections, known as call legs, are established in either an inbound or outbound direction.

Dial peers define the parameters for the calls that they match. For example, if a call is originating and terminating at the same site, and is not crossing through slow speed WAN links, then the call can cross the local network uncompressed and without special priority. A call that originates locally and crosses the WAN link to a remote site may require compression with a specific codec. In addition, this call may require that voice activity detection (VAD) be turned on, and will need to receive preferential treatment by specifying a higher priority level.

Cisco Systems voice-enabled routers support two types of dial peers:

- **Plain old telephone service (POTS) dial peers:** Connect to a traditional telephony network, such as the public switched telephone network (PSTN) or a PBX, or to a telephony edge device, such as a telephone or fax machine. POTS dial peers perform these functions:
  - Provide an address (telephone number or range of numbers) for the edge network or device
  - Point to the specific voice port that connects the edge network or device
- **Voice over IP (VoIP) dial peers:** Connect over a packet network. VoIP dial peers perform these functions:
  - Provide a destination address (telephone number or range of numbers) for the edge device that is located across the network
  - Associate the destination address with the next hop router or destination router, depending on the technology used

 Copyright © 2005, Cisco Systems, Inc.



In the figure, the telephony device connects to the Cisco Systems voice-enabled router POTS dial. The POTS dial peer configuration includes the telephone number of the telephony device and the voice port to which it is attached. The router knows where to forward incoming calls for that telephone number.

The Cisco voice-enabled router VoIP dial peer is connected to the packet network. The VoIP dial peer configuration includes the destination telephone number (or range of numbers) and the next hop or destination voice-enabled router network address.

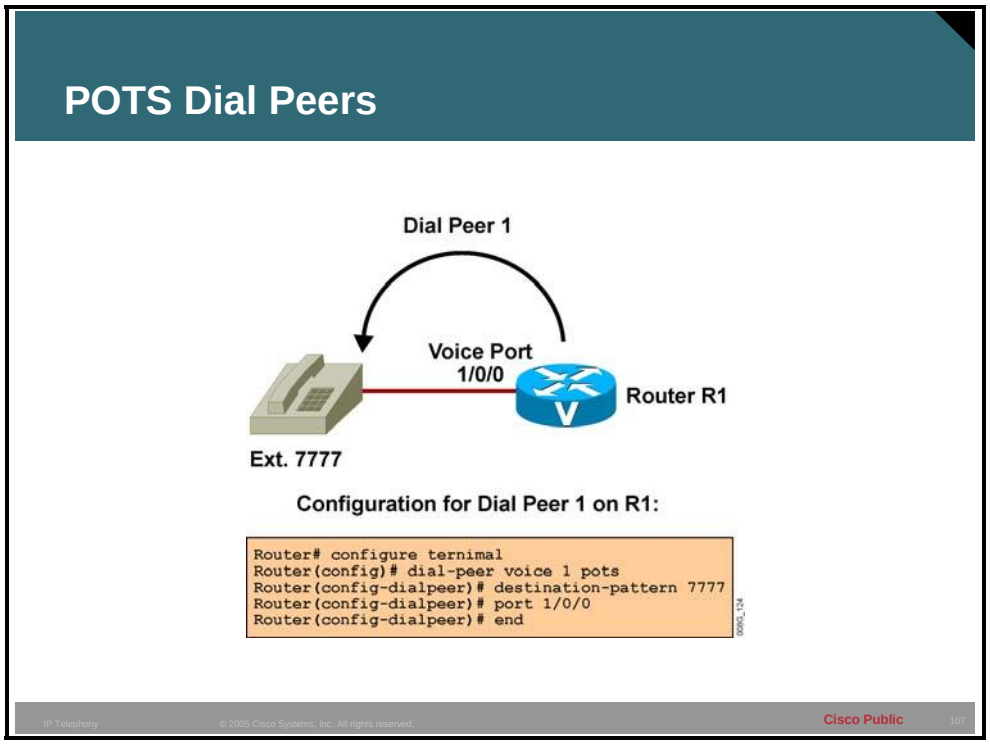
Follow the steps to place a VoIP call:

How to Place a VoIP Call

Step	Action
1	Configure the source router with a compatible dial peer that specifies the recipient destination address
2	Configure the recipient router with a POTS dial peer that specifies which voice port the router uses to forward the voice call

Plain Old Telephone Service Dial Peers

This topic describes how to configure POTS dial peers.



Before the configuration of Cisco IOS dial peers can begin, the user must have a good understanding of where the edge devices reside, what type of connections need to be made between these devices, and what telephone numbering scheme is applied to the devices.

Follow the steps to configure POTS dial peers:

How to Configure POTS Dial Peers

Step	Action
1	Configure a POTS dial peer at each router or gateway where edge telephony devices connect to the network
2	Use the **destination–pattern** command in the dial peer to configure the telephone number
3	Use the **port** command to specify the physical voice port that the POTS telephone is connected to.

The dial peer type will be specified as POTS because the edge device is directly connected to a voice port and the signaling must be sent from this port to reach the device. There are two basic parameters that need to be specified for the device: the telephone number and the voice port. When a PBX is connecting to the voice port, a range of telephone numbers can be specified.

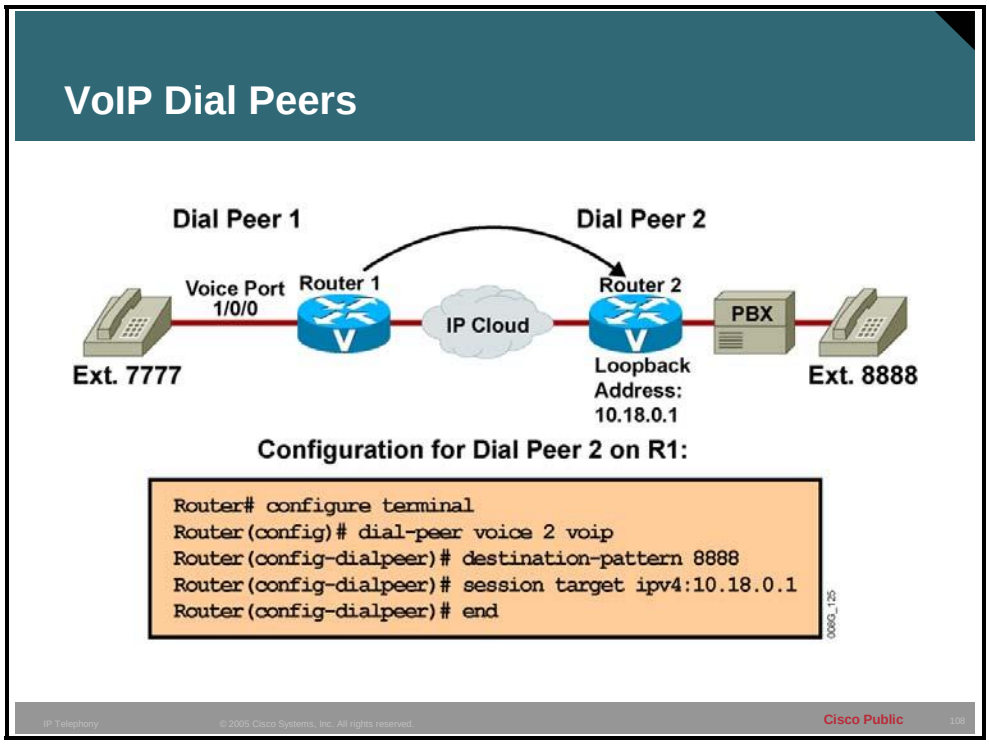
 Copyright © 2005, Cisco Systems, Inc.

Example

The figure illustrates proper POTS dial peer configuration on a Cisco voice-enabled router. The **dial-peer voice 1 pots** command notifies the router that dial peer 1 is a POTS dial peer with a tag of 1. The **destination-pattern 7777** command notifies the router that the attached telephony device terminates calls destined for telephone number 7777. The **port 1/0/0** command notifies the router that the telephony device is plugged into module 1, voice interface card (VIC) slot 0, voice port 0.

VoIP Dial Peers

This topic describes how to configure VoIP dial peers.



The administrator must know how to identify the far-end voice-enabled device that will terminate the call. In a small network environment, the device may be the IP address of the remote device. In a large environment, the device may mean pointing to a Cisco CallManager or gatekeeper for address resolution and call admission control (CAC) to complete the call.

You must follow these steps to configure VoIP dial peers:

How to Configure VoIP Dial Peers

Step	Action
1	Configure the path across the network for voice data
2	Specify the dial peer as a VoIP dial peer
4	Use the **destination-pattern** command to configure a range of numbers reachable by the remote router or gateway
5	Use the **session target** command to specify an IP address of the terminating router or gateway
6	Use the remote device loopback address as the IP address

The dial peer is specified as a VoIP dial peer, which alerts the router that it must process a call according to the various parameters that are specified in the dial peer. The dial peer must then package it as an IP packet for transport across the network. Specified parameters may include the codec used compression (VAD, for example), or marking the packet for priority service.

 Copyright © 2005, Cisco Systems, Inc.

The destination-pattern parameter configured for this dial peer is typically a range of numbers that are reachable via the remote router or gateway.

Because this dial peer points to a device across the network, the router needs a destination IP address to put in the IP packet. The session target parameter allows the administrator to specify either an IP address of the terminating router or gateway, or another device; for example, a gatekeeper or Cisco CallManager that can return an IP address of that remote terminating device.

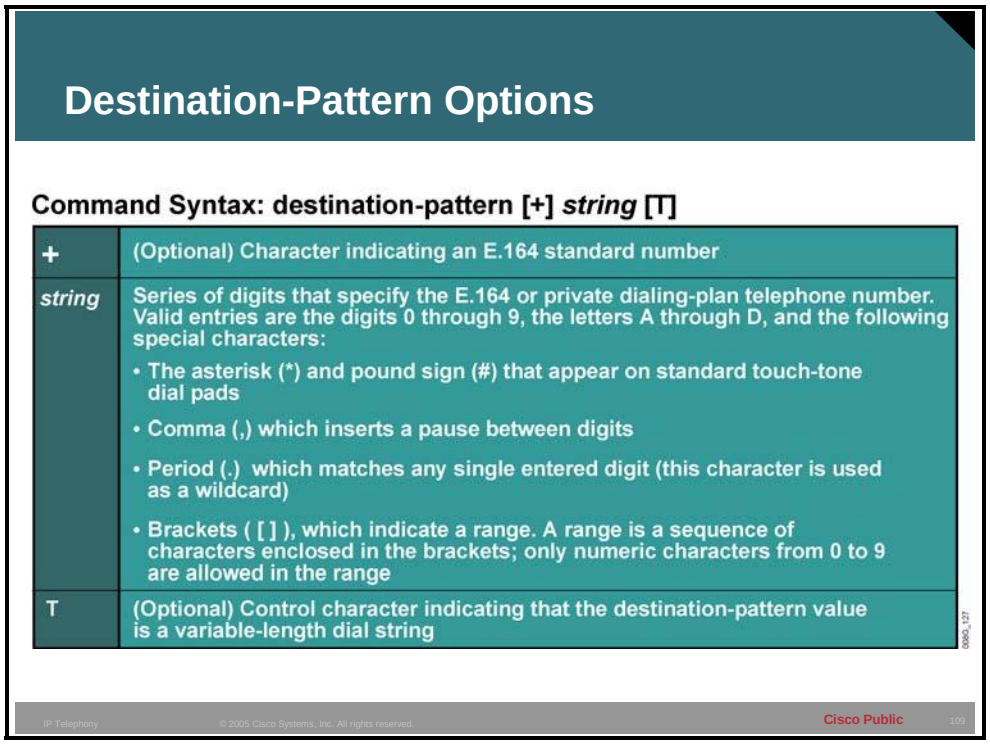
To determine which IP address a dial peer should point to, it is recommended that you use a loopback address. The loopback address is always up on a router, as long as the router is powered on and the interface is not administratively shut down. If an interface IP address is used instead of the loopback, and that interface goes down, the call will fail even if there is an alternate path to the router.

Example

The figure illustrates the proper VoIP dial peer configuration on a Cisco voice-enabled router. The **dial-peer voice 2 voip** command notifies the router that dial peer 2 is a VoIP dial peer with a tag of 2. The **destination-pattern 8888** command notifies the router that this dial peer defines an IP voice path across the network for telephone number 8888. The **session target ipv4:10.18.0.1** command defines the IP address of the router that is connected to the remote telephony device.

Destination-Pattern Options

This topic describes destination-pattern options and the applicable shortcuts.



The destination pattern associates a telephone number with a given dial peer. The destination pattern also determines the dialed digits that the router collects and forwards to the remote telephony interface, such as a PBX, Cisco CallManager, or the PSTN. You must configure a destination pattern for each POTS and VoIP dial peer that you define on the router.

The destination pattern can indicate a complete telephone number or a partial telephone number with wildcard digits; it can also point to a range of numbers defined in a variety of ways.

Destination-pattern options include:

- **Plus (+):** An optional character that indicates an E.164 standard number. E.164 is the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) recommendation for the international public telecommunication numbering plan. The plus sign in front of a destination-pattern string specifies that the string must conform to Recommendation E.164.

- ***String:*** A series of digits specifying the E.164 or private dialing-plan telephone number. The examples below show the use of special characters that are often found in destination patterns strings:

  — Asterisk (*) and pound sign (#) appear on standard touch-tone dial pads. These characters may need to be used when passing a call to an automated application that requires these characters to signal the use of a special feature. For example, when

 Copyright © 2005, Cisco Systems, Inc.

calling an interactive voice response (IVR) system that requires a code for access, the number dialed might be “5551212888#”, which would initially dial the telephone number 5551212 and input a code of 888 followed by the pound key to terminate the IVR input query.

— Comma (,) inserts a one-second pause between digits. The comma can be used, for example, where a 9 is dialed to signal a PBX that the call should be processed by the PSTN. The 9 is followed by a comma to give the PBX time to open a call path to the PSTN, after which the remaining digits will be played out. An example of this string is 9,5551212.

— Period (.) matches any single entered digit (this character is used as a wildcard). The wildcard is used to specify a group of numbers that may be accessible via a single destination router, gateway, PBX or Cisco Call Manager. Because the period (commonly referred to as a dot), indicates a single digit of 0 to 9, this limits how efficiently ranges of numbers are used. A pattern of “200.” allows for 10 uniquely addressed devices, where a pattern of “20..” can point to 100 devices. If one site has the numbers 2000 through 2049, and another site has the numbers 2050 through 2099, then the bracket notation would be more efficient.

— Brackets ([ ]) indicate a range. A range is a sequence of characters that are enclosed in the brackets. Only single numeric characters from 0 to 9 are allowed in the range. In the previous example, the bracket notation could be used to specify exactly which range of numbers is accessible through each dial peer. For example, the first site pattern would be “20[0-4].”, and the second site pattern would be “20[5-9].” The bracket notation offers much more flexibility in how numbers can be assigned.

- **T:** An optional control character indicating that the destination-pattern value is a variable-length dial string. In cases where callers may be dialing local, national or international numbers, the destination pattern must provide for a variable-length dial plan. If a particular voice gateway has access to the PSTN for local calls, and access to a transatlantic connection for international calls, then calls being routed to that gateway will have a varying number of dialed digits. A single dial peer with a destination pattern of “.T” could support the different call types. The interdigit timeout determines when a string of dialed digits is complete. The router continues to collect digits until there is an interdigit pause longer than the configured value, which by default is 10 seconds.

When the calling party finishes entering dialed digits, there is a pause equal to the interdigit timeout value *before* the router processes the call. The calling party can immediately terminate the interdigit timeout by entering the pound (#) character, which is the default termination character. Because the default interdigit timer is set to 10 seconds, users may experience a long call setup delay.

Note	Cisco IOS software does not check the validity of the E.164 telephone number; it accepts any series of digits as a valid number.

Example

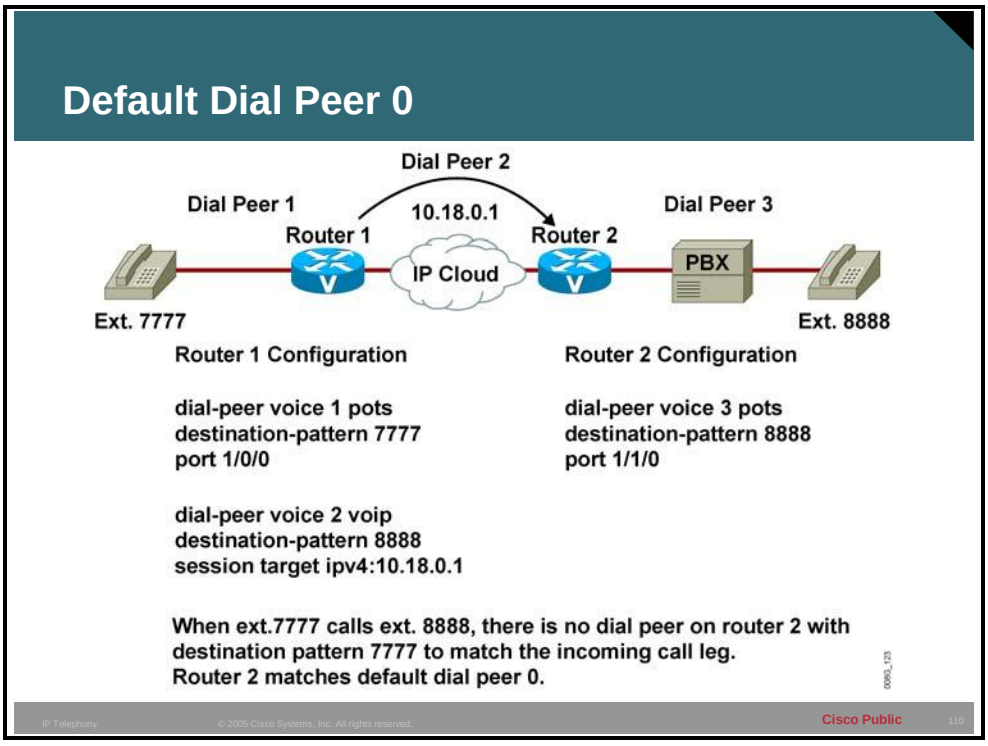
Example: Destination-Pattern Options

Destination Pattern	Matching Telephone Numbers
5551234	Matches one telephone number exactly, 5551234. This is typically used when there is a single device, such as a telephone or fax, connected to a voice port.
555[1-3]…	Matches a seven-digit telephone number where the first three digits are 555, the fourth digit can be a 1, 2, or 3, and the last digits can be any valid digits. This type of destination pattern is used where telephone number ranges are assigned to specific sites. In this example, the destination pattern is used in a small site that does not need more than thirty numbers assigned.
.T	Matches any telephone number that has at least one digit and can vary in length from 1 to 32 digits total. This destination pattern is used for a dial peer that services a variable-length dial plan, such as local, national, and international calls. It can also be used as a default destination pattern so that any calls that do not match a more specific pattern will match this one and can be directed to an operator.

 Copyright © 2005, Cisco Systems, Inc.

What is the Default Dial Peer?

This topic describes the default dial peer.



When a matching inbound dial peer is not found, the router resorts to the default dial peer.

Note	Default dial peers are used for inbound matches only. They are not used to match outbound calls that do not have a dial peer configured.

The default dial peer is referred to as *dial-peer 0*.

Example

In the figure, only one-way dialing is configured. The caller at extension 7777 can call extension 8888 because there is a VoIP dial peer configured on router 1 to route the call across the network. There is no VoIP dial peer configured on router 2 to point calls across the network towards router 1. Therefore, there is no dial peer on router 2 that will match the calling number of extension 7777 on the inbound call leg. If no incoming dial peer matches the calling number, the inbound call leg automatically matches to a default dial peer (POTS or VoIP).

Note	There is an exception to the previous statement. Cisco voice and/or dial platforms, such as the AS53*xx* and AS5800, require that a configured inbound dial peer be matched for incoming POTS calls to be accepted as voice calls. If there is no inbound dial peer match, the call is treated and processed as a dial-up (modem) call.

Dial peer 0 for inbound VoIP peers has the following configuration:

- any codec
- ip precedence 0
- vad enabled
- no rsvp support
- fax-rate service

Dial peer 0 for inbound POTS peers has the following configuration:

- no ivr application

You cannot change the default configuration for dial peer 0. Default dial peer 0 fails to negotiate non-default capabilities or services. When the default dial peer is matched on a VoIP call, the call leg that is set up in the inbound direction uses any supported codec for voice compression, based on the requested codec capability coming from the source router. When a default dial peer is matched, the voice path in one direction may have different parameters than the voice in the return direction. This may cause one side of the connection to report good-quality voice, while the other side reports poor-quality voice. For example, the outbound dial peer has VAD disabled, but the inbound call leg is matched against the default dial peer, which has VAD enabled. In this example, VAD is *on* in one direction and *off* in the return direction.

When the default dial peer is matched on an inbound POTS call leg, there is no default IVR application with the port; as a result, the user gets a dial tone and proceeds with dialed digits.

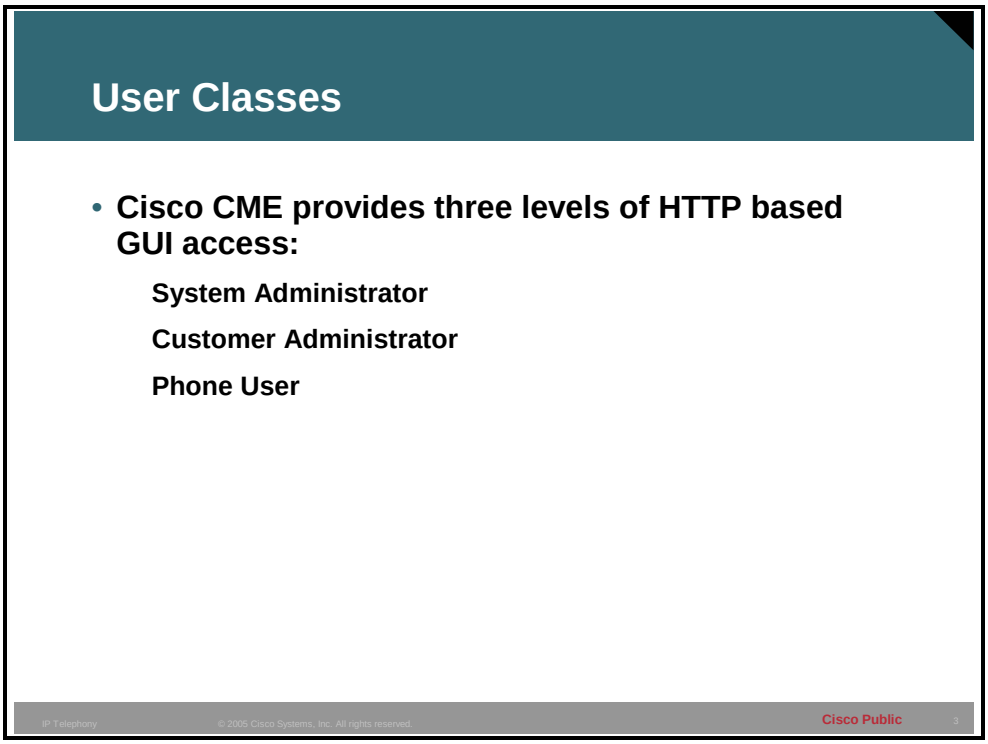
The use of a catch all dial peer that will match all calls can prevent the use of the default dial peer and send any matches to a default location like the operator or an automated attendant (AA).

 Copyright © 2005, Cisco Systems, Inc.

Cisco CME GUI Features

User Classes

This topic describes the three user classes for HTTP based GUI access.



The Cisco CME GUI provides a Web-based interface to manage most system-wide and phone-based features. In particular, the GUI facilitates the routine adds and changes associated with employee turnover, allowing these changes to be performed by non-technical staff.

The GUI provides three levels of access to support the following user classes:

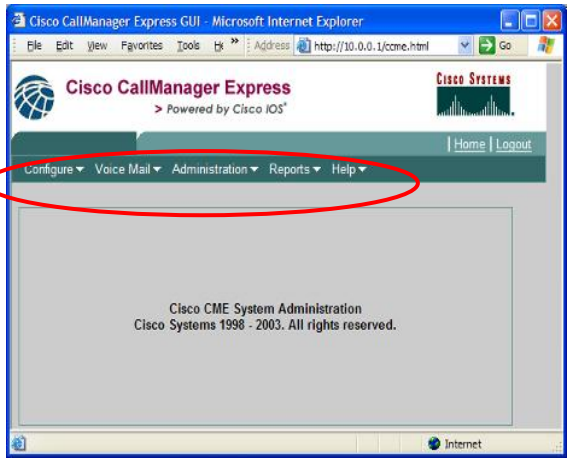
- System Administrator - Able to configure all system wide and phone-based features. This person is familiar with Cisco IOS software and VoIP network configuration.
- Customer Administrator - Able to perform routine phone adds and changes without having access to system wide features. This person does not have to be trained in Cisco IOS software.
- Phone User - Able to program a small set of features on his or her own phone and search the Cisco CME directory.

Note The System Administrator account must initially be configured through the CLI.

User Classes (Cont.)

HTTP://*ip_address*/ccme.html

System and Customer Administrator Web-based GUI interface



IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 4

The system administrator and the customer administrator by default will have the same level of access. The customer administrator can be customized to have a subset of the objects in the menus. This will be covered later in the lesson. The objects that will be seen are the following drop down menus:

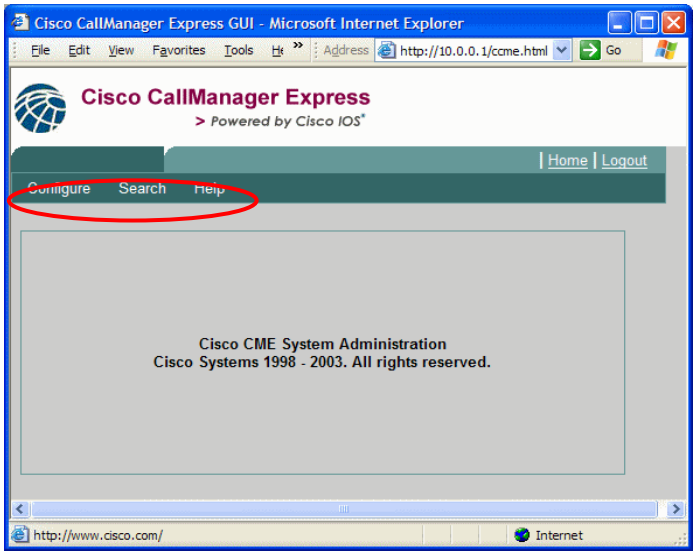
- **Configure** – Settings dealing with ephones, ephone-dns, and system settings
- **Voice Mail** – Settings dealing with voice mail settings and integrations
- **Administrator** – Where the backup and restore, saving of the changes, and reloading the router can be done
- **Reports** – Where various reports can be run and viewed
- **Help** – Links to versions information and the help file

Note	The System Administrator username and password may be changed from System Administrator GUI.

 Copyright © 2005, Cisco Systems, Inc.

User Classes (Cont.)

Phone User GUI Web interface



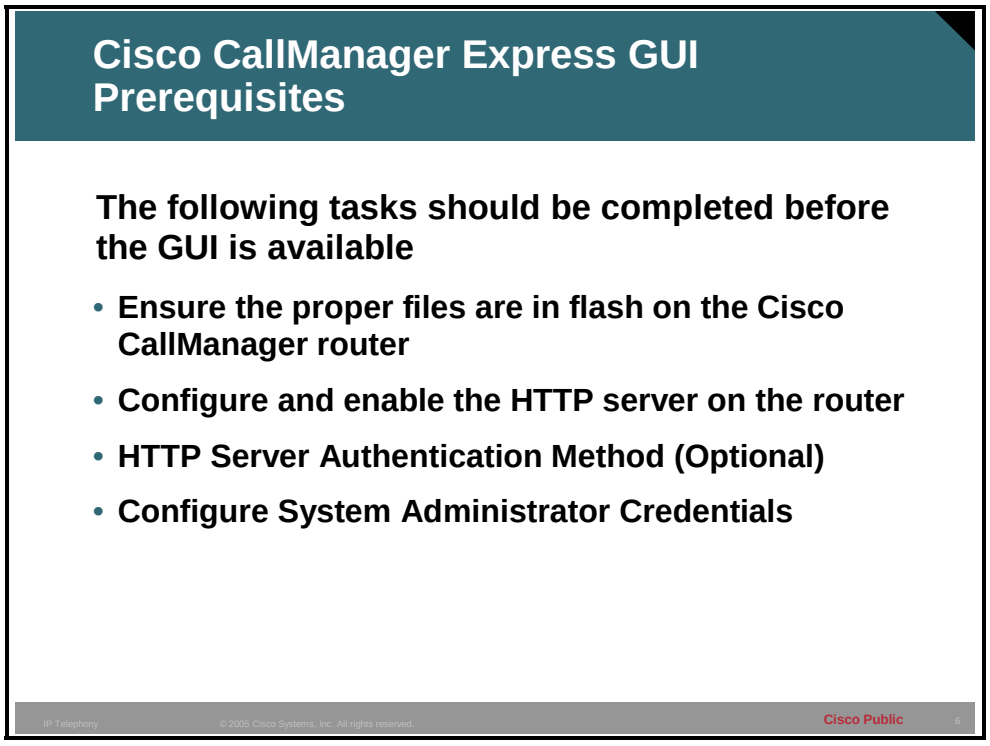
IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 5

The phone user GUI Web interface looks similar to the system and customer administrator GUI Web interfaces. The phone users can make some basic changes to the configuration of their phones, as well look up entries in the Cisco CME directory. The menus visible to the system users will include very limited options under the following drop down menus.

- **Configure** – Where some limited settings about the users associated phone can be made
- **Search** – Where the user can search the directory of Cisco CME
- **Help** – Links to the version information and help file for the users

Cisco CallManager Express GUI Prerequisites

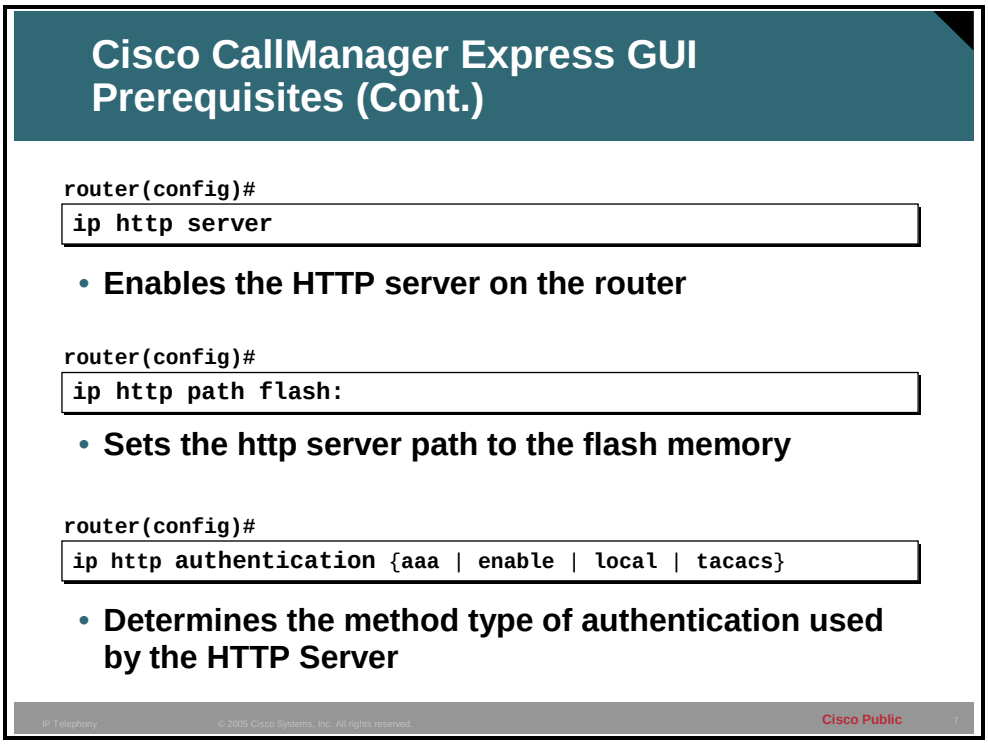
This topic describes the GUI prerequisite tasks to be completed.



The Cisco CME GUI uses HTTP to transfer information from the Cisco CME router to the PC of an administrator or phone user. The router must be configured as an HTTP server and have the proper Web files in flash locally to serve up to the browser. In addition an initial system administrator username and password must be defined from the router command-line interface (CLI). Customer administrators and phone users can be added from the Cisco CME router using CLI commands or from a PC using GUI Web pages. The GUI Web page functions for Customer Administrators can be restricted and customized with support in Cisco CME for XML cascading style sheets (files with a .css suffix).

Note	In order to access the GUI interface, Internet Explorer (IE) 5.5 or greater is required.

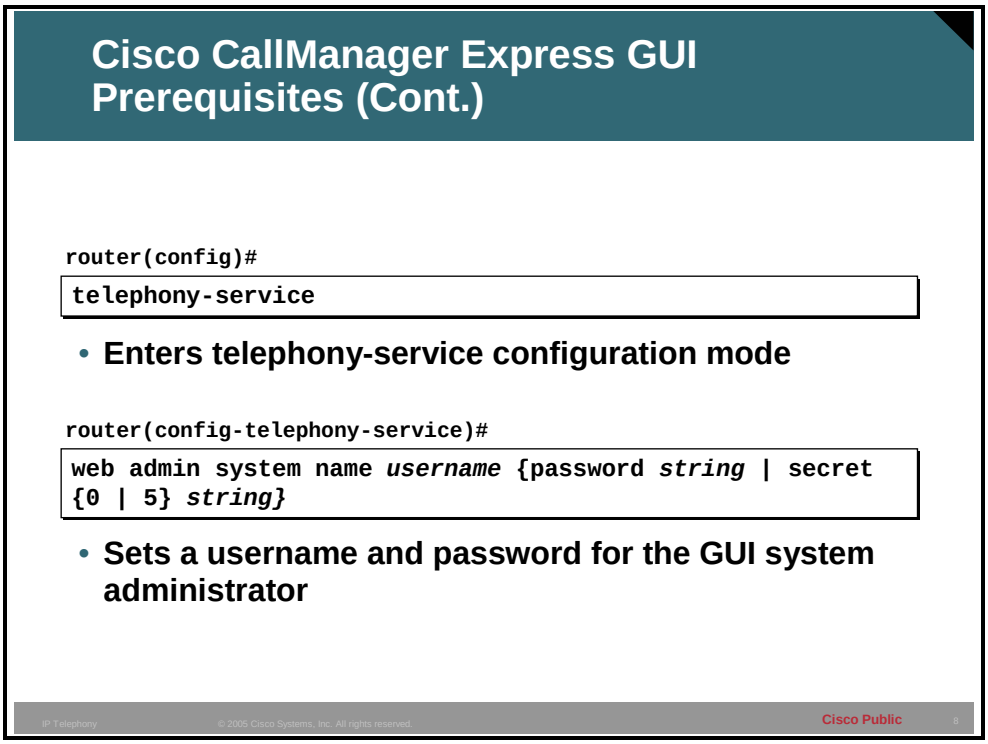
 Copyright © 2005, Cisco Systems, Inc.



The GUI Web interface files must be installed in flash memory on a Web server that runs locally on the Cisco CME router. The HTTP server on the Cisco CME router is disabled by default. In order to enable it, enter **ip http server** from global configuration mode. While this starts the HTTP service, it does not define where the files are that will be served up by the local routers Web server will reside. To configure the location of the files to be served by the Web server enter the command **ip http path flash:** from global configuration mode. Authentication is set to use the enable password by default. It is recommended that authentication be configured to use AAA or a local username and password pair. The **ip http authentication** command is used to configure the authentication method that is desired.

Command	Purpose
ip http server Example: Router(config)#ip http server	Enables the Cisco Web server on the local Cisco CME router
ip http path flash: Example: Router(config)# ip http path flash:	Sets the base HTTP path for HTML files to Flash memory on the router.
ip http authentication {aaa | enable | local |tacacs} Example: Router(config)# ip http authentication aaa This command has no effect for customer administrator and phone users.	Specifies method of authentication to use for the system administrator when accessing the HTTP server. Default is the enable keyword. • aaa - Indicates that the authentication method used for the AAA login service should be used for authentication. The AAA login service method is specified by the aaa authentication login command. • **enable** -Uses the enable password. This is the default if this command is not used. • **local** - Uses login user name, password, and privilege level access combination specified in the local system configuration (by the username global configuration command). • **tacacs** - Uses TACACS (or XTACACS) server.

 Copyright © 2005, Cisco Systems, Inc.



To configure the system administrator credentials, from global configuration mode, enter the **telephony-service** command. From the telephony service sub mode enter **web admin system name *username* password *password*** command. This defines an initial username and password for the system administrator to access the GUI. Once you have created this account you can log in to the GUI. While in the GUI as the system administrator, the customer administrator and phone users may be defined. Alternatively, you can continue to use router CLI to create the customer administrator and phone users' credentials.

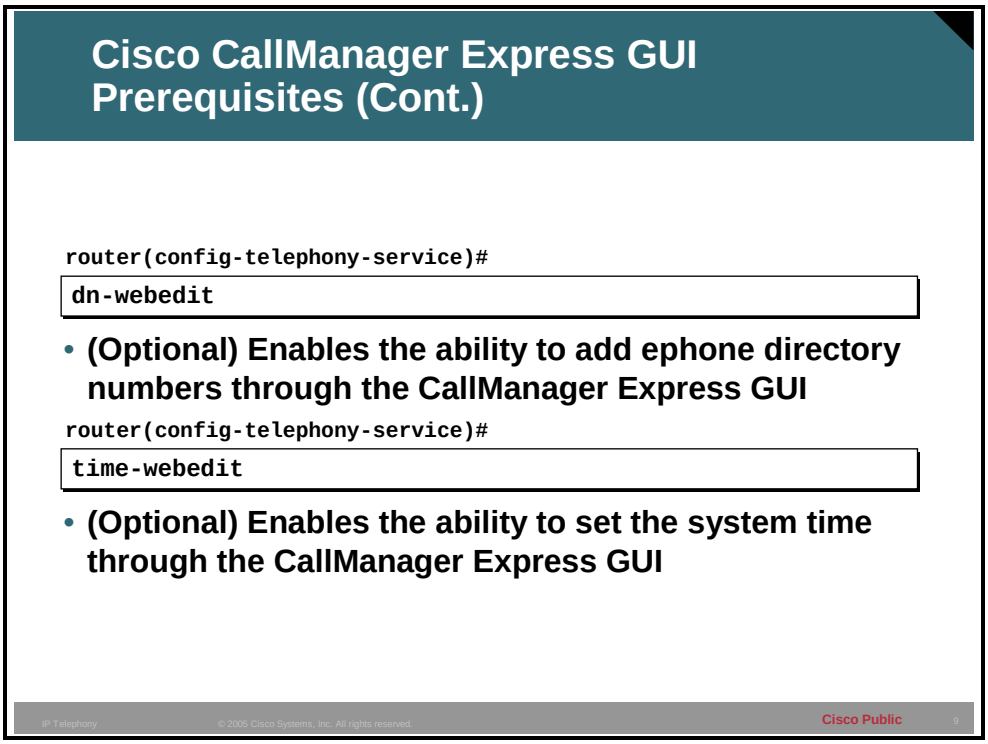
The password will not be encrypted if the **0** options is used and will be clearly visible in the configuration. If the password is set with the **5** option the password will be shown as a MD5 hash.

Note	There is only one system administrator set of credentials.

Command	Purpose
telephony-service **Example:** `Router(config)#` telephony-service	**Enters telephony-service configuration mode.**
web admin system name username {password string | secret {0 | 5} string} **Example:** Router(config-telephony-service)# web admin system name pwa3 secret 0 wp78pw	Defines a username and password for a system administrator. The default username is Admin. There is no default password. • name username – System administrator username. • password string – String to verify system administrator identity. Default is empty string. • secret {0 | 5} string – Password should be encrypted. The digit specifies state of encryption of the string that follows, as explained here: – 0 – Password that follows is not yet encrypted. – 5 – Password that follows is encrypted using MD5.

Note	The secret 5 keyword pair is used in the output of show commands when encrypted passwords are displayed and it indicates that the password that follows is encrypted.

 Copyright © 2005, Cisco Systems, Inc.



By default, ephone-dns can only be created through the CLI of the Cisco CME router. The ability to add ephone-dns through the GUI Web interface can be enabled if desired. To enable this functionality, use the **dn-webedit** command.

Similarly, the ability to set the system time of the Cisco CallManager router in the GUI Web interface, which ultimately sets the time which is displayed on the display of the IP phones, has to be enabled and by default will not be available in the GUI Web interface. To enable the setting of the time in the GUI Web interface, use the **time-webedit** command.

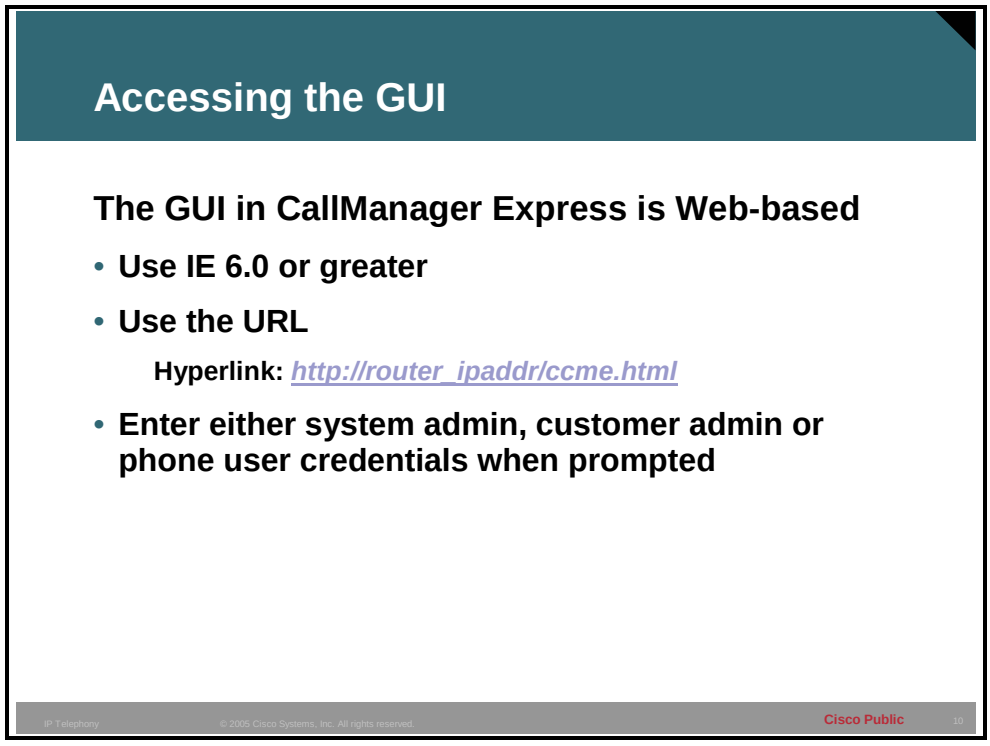
These settings provide a way to allow the non technical administrator to create new ephone-dns and modify the time through the GUI Web-based interface instead of the CLI that the non-technical administrator may not be comfortable in.

Command	Purpose
dn-webedit **Example:** `Router(config-telephony-service)#` dn-webedit	(Optional) Enables the ability to add directory numbers through the Web interface. The **no** form of this command disables the ability to create IP phone extension telephone numbers. That ability could disrupt the network-wide management of telephone numbers. If this command is not used, the ability to create directory numbers is disabled by default.
time-webedit **Example:** `Router(config-telephony-service)#` time-webedit	(Optional) Enables the ability to set the phone time for the Cisco CME system through the Web interface. **Note** Cisco discourages this method for setting network time. The router should be set up to automatically synchronize its router clock from a network-based clock source using Network Time Protocol (NTP). In the rare case that a network NTP clock source is not available, the **time-webedit** command can be used to allow manual setting and resetting of the router clock through the GUI.

 Copyright © 2005, Cisco Systems, Inc.

Accessing the GUI

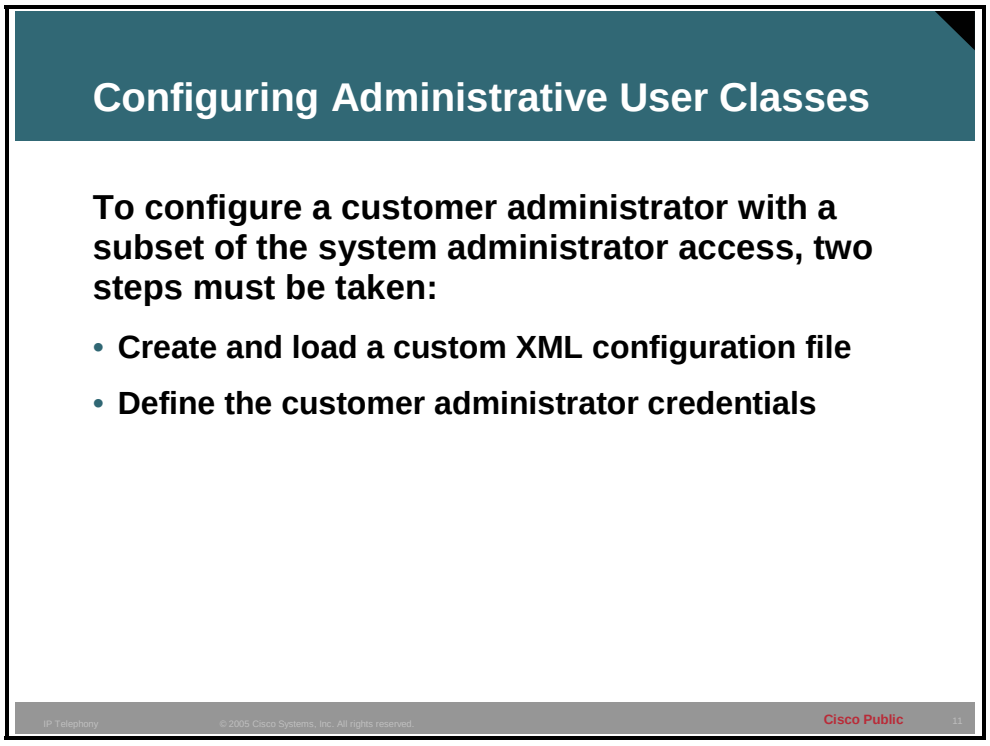
This topic describes how to access the GUI.



To access the Administrative Web site to make changes use the URL http://*router_ipaddr*/ccme.html in your IE 5.5 browser. When prompted for credentials, use the administrative credentials previously defined in the CLI. Based on the credentials presented to the Cisco CME router, the router will display the appropriate Web page for either the system administrator, customer administrator or a phone user.

Configuring Administrative User Classes

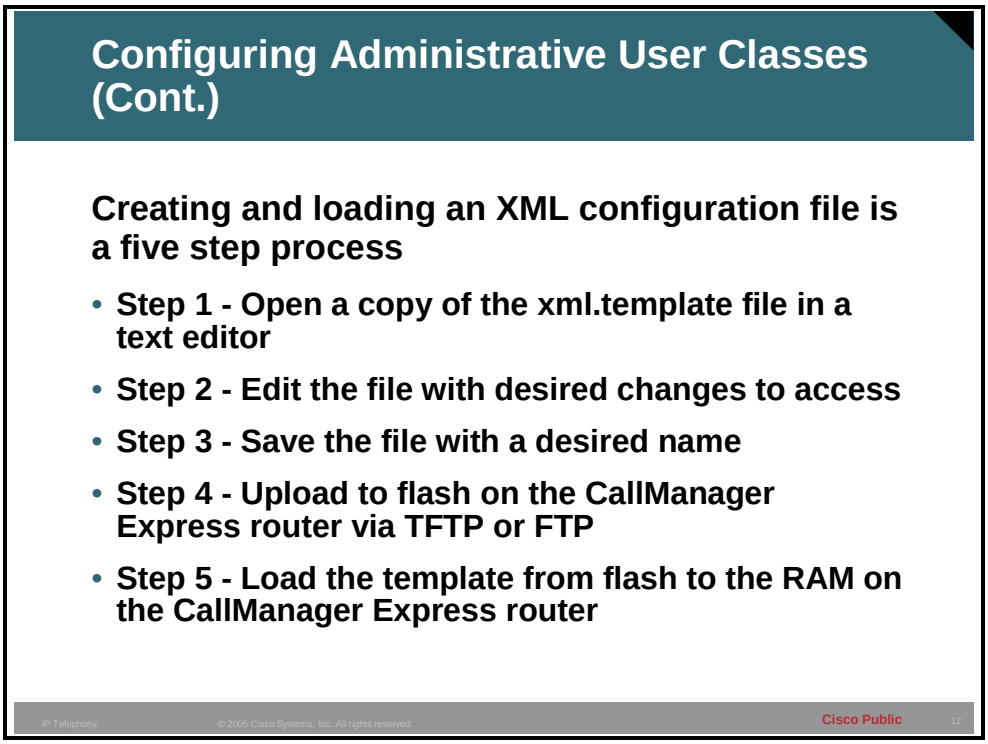
This topic describes how to configure a customer administrator.



In the Cisco CME system there is a system administrator that has full control of the system. It may be desirable to create another custom level of access to the system by configuring what is known as a customer administrator. This customer administrator can have a subset of the full level of access enjoyed by the default system administrator. The end result will be the existence of two levels of administrators one with full access and the customer administrator with some defined subset of full access.

Creating and defining the level of access for the customer administrator to log in to the GUI Cisco CME interface is a two-step process. The first step is to create the XML file that will define the level of access to objects in the Cisco CallManager GUI Web interface. The second step is to create the user credentials that will be used by the customer administrator. This may be done by either using the CLI or the system administrator GUI Web interface.

 Copyright © 2005, Cisco Systems, Inc.



The xml.template file is included in both the .tar and .zip that Cisco CME was installed with. First open the xml.template file with a text editor. Then delete either the “Hide” word or “Show” word, as well as the pipe symbol and the brackets, leaving only “Hide” or “Show” remaining whichever level of access is desired for that object. Save the file with a name that has significance and an .xml extension. This file will then need to be uploaded to the flash of the Cisco CME router. Finally the file will be loaded into RAM from flash.

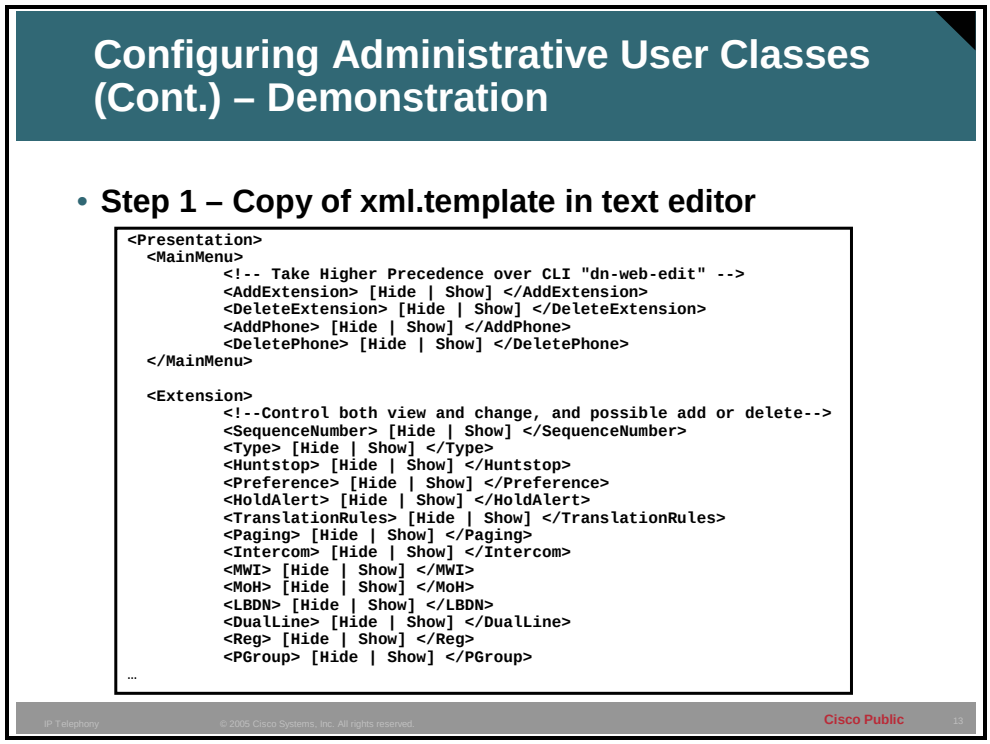
Step	Action	Notes
1.	Open a copy of the xml.template file	The xml.template file is included in both the tar and the zip file that the Cisco CME files came in
2.	Modify the xml file	Leave only the “Hide” or “Show” word, whichever action is desired, deleting the other word and any brackets or pipe symbols
3.	Save the file with the desired name `Example:CustomerAdmin.xml`	The name of the file can be anything desired as long as it is a known value
4.	Upload the xml file to flash memory on the Cisco CME router `copy ftp flash`	TFTP or FTP can be used to move the new xml file to flash memory
5.	Load the template from flash to RAM on the Cisco CME router `web customize load` *`filename`*	This command will be executed if saved to the startup-config at boot up

Example

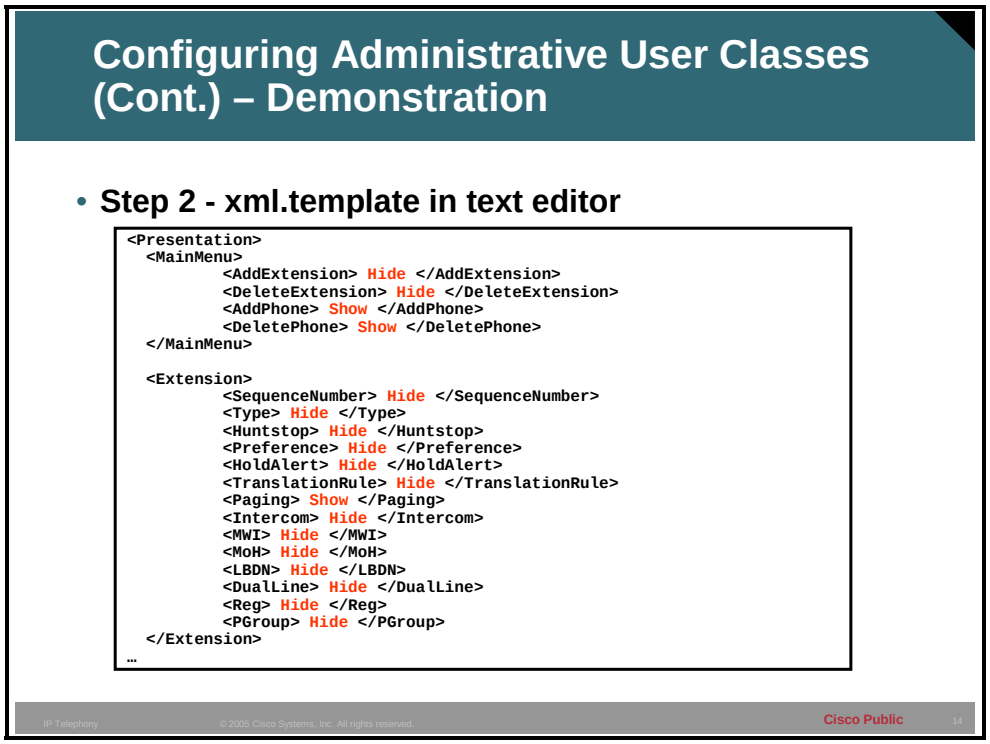
Changing a line in the xml.template file that controls the ability to add a new phone in Cisco CME GUI Web interface.

"<AddPhone> **[Hide | Show]** </AddPhone**>"** becomes "<AddPhone> **Hide** </AddPhone>" and would prevent the Customer Administrator from adding a phone through the Web-based interface.

 Copyright © 2005, Cisco Systems, Inc.



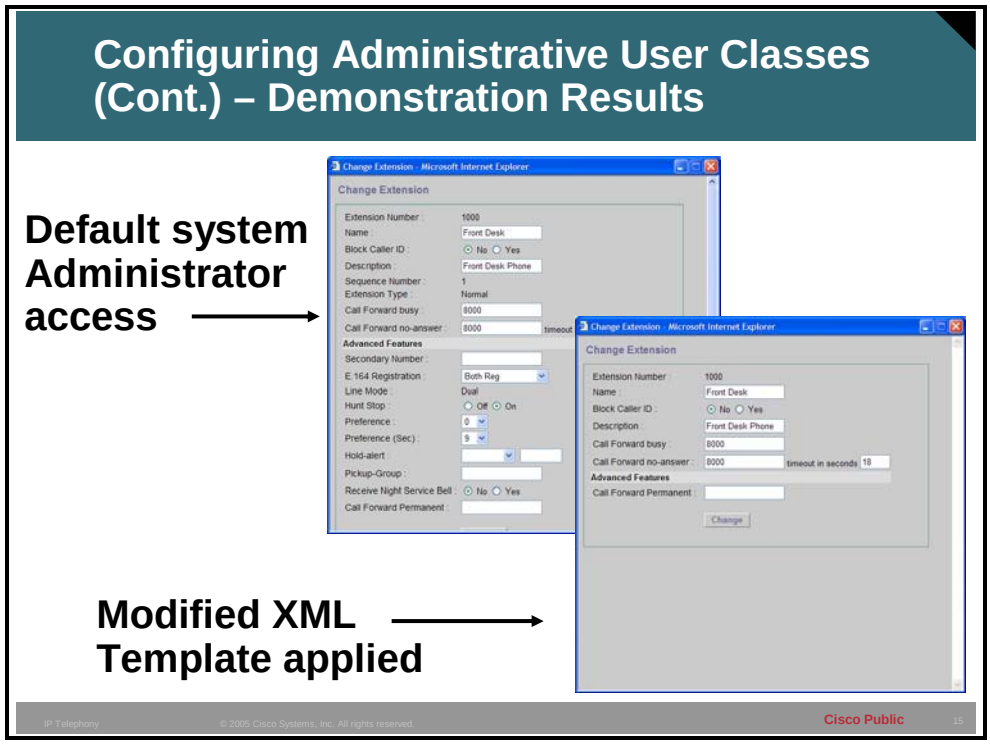
This is an example of the xml.template that comes with Cisco CME 3.1. Notice the **[Hide | Show].** This needs to be edited to leave only the desired action.



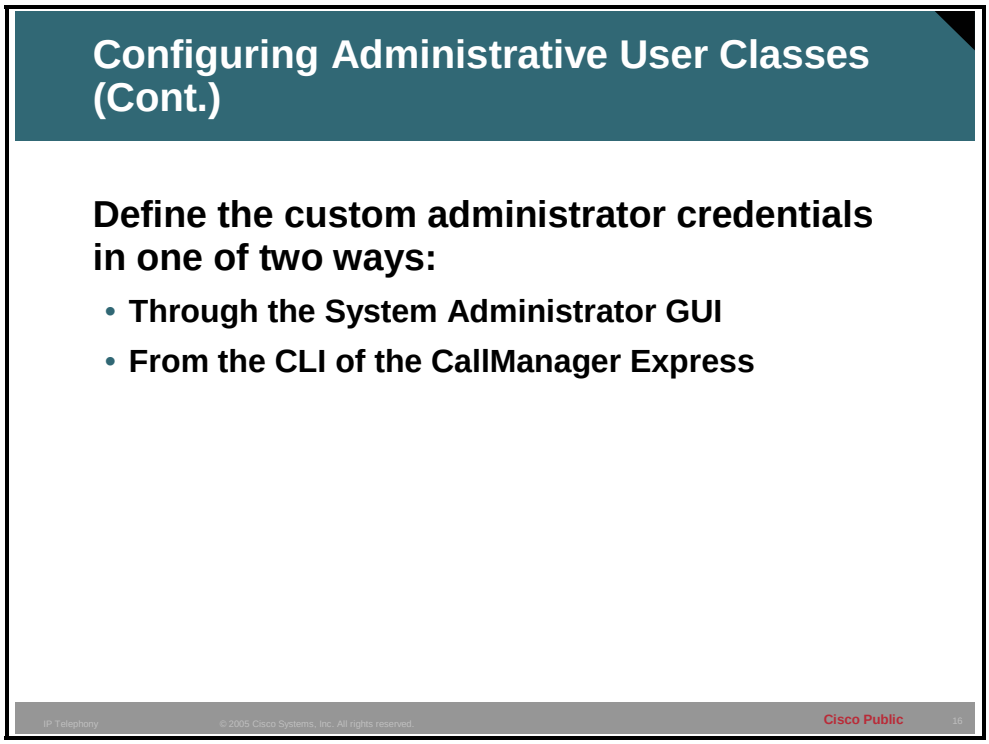
This example XML file shows the proper syntax for an XML file. Notice that this XML file would allow the customer administrator to add and delete a phone but not an extension. Once the desired changes to access have been made, save the file (step 3) and put it on an ftp or tftp server that the Cisco CME router can communicate with. Next in step 4, use the **copy ftp flash** or **copy tftp flash** command to move the file to flash on the Cisco CME router. The last step is step 5 and uses the command **web customize load *filename*** from telephony service mode to load the file into RAM on the Cisco CME router. Any syntax errors that exist in this step will cause the process to fail, which will then cause the Cisco CME router to output a syslog message.

Command	Purpose
web customize load *filename* **Example:** `Router(config-telephony-service)#` web customize load myxmlfile.xml	Used to load and parse an eXtensible Markup Language (XML) file in router Flash memory to customize a Cisco CME GUI for a customer administrator.

 Copyright © 2005, Cisco Systems, Inc.



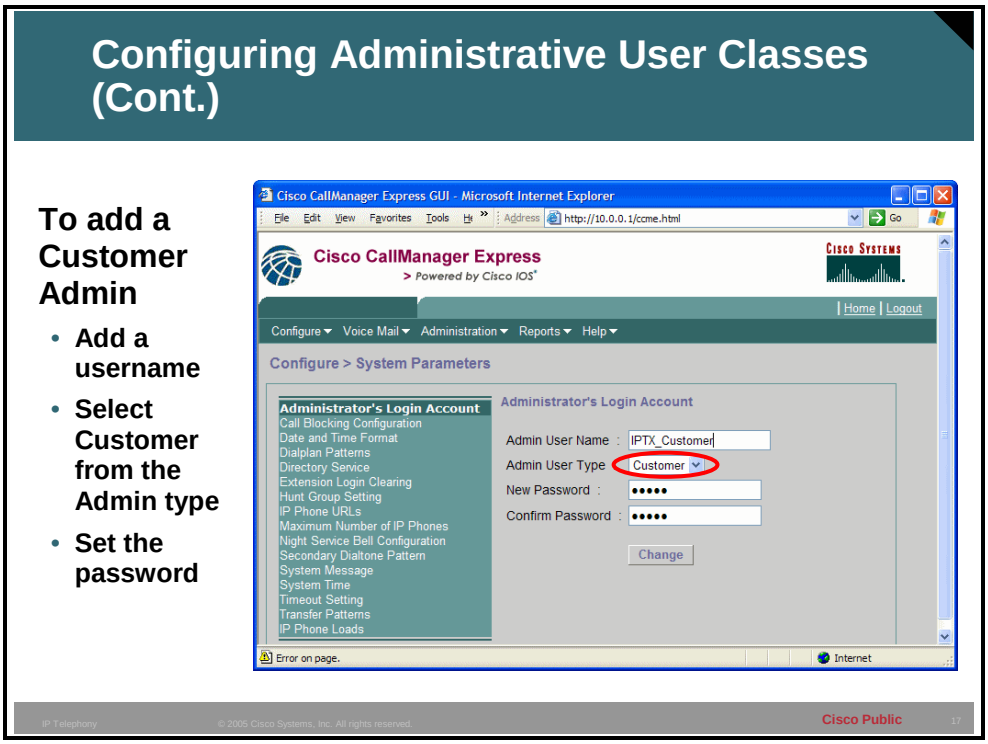
This slide shows the results of the previous XML configuration file. The difference in access to the GUI Web interface is a direct result of the <Extensions> section in the previous slide.



Defining the Custom Administrator Credentials

After the XML file is configured and loaded into RAM, the system administrator can set up the credentials for the customer administrator. There are two different ways to achieve this. The first is through the system administrator Web pages, and the second is from the CLI.

 Copyright © 2005, Cisco Systems, Inc.

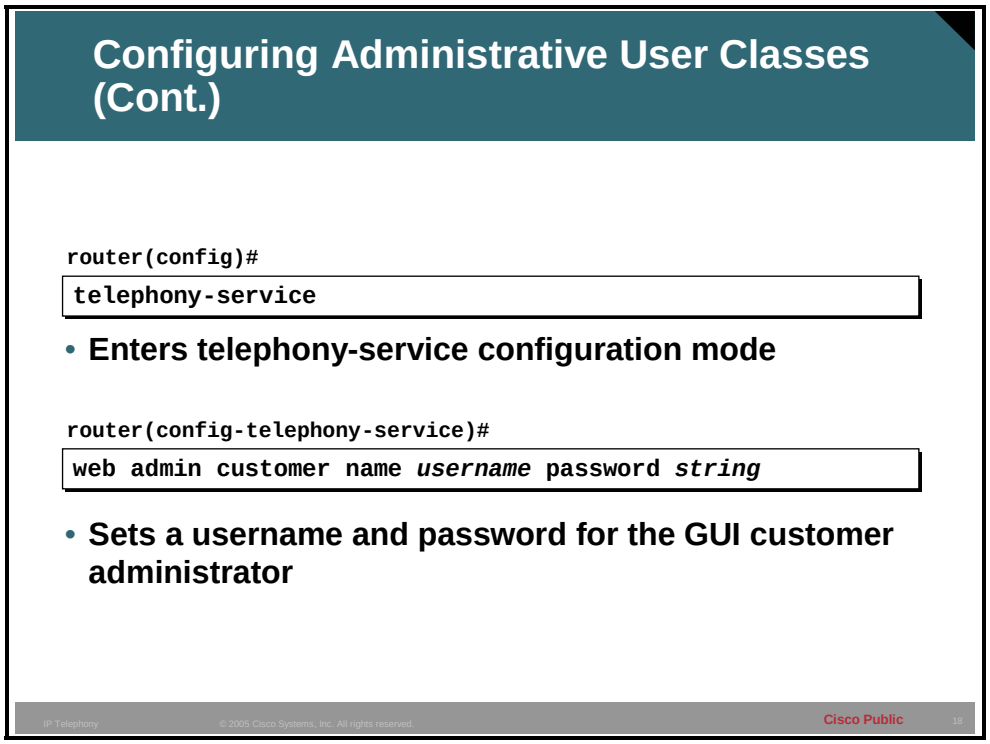


Defining the Custom Administrator Credentials in the GUI

This slide shows the creation of the Customer Administrator by the System Administrator. Access to this page is through the “Configure” drop-down menu, then selecting System Parameters.

The end result will be that there will now be a system administrator and a customer administrator.

Note	Only one set of customer administrator credentials may be defined. Any subsequent changes will simply overwrite the initial configuration.



Defining the Custom Administrator Credentials in the CLI

To create the customer administrator from the CLI first enter the **telephony-service** command from global configuration mode. Then, enter the **web admin customer name *username* password *password*** command to create the credentials to be used by the customer administrator.

Note	Only one set of customer administrator credentials may be defined. Any subsequent changes will simply overwrite the initial configuration.

Command	Purpose
telephony-service **Example:** `Router(config)#` telephony-service	**Enters telephony-service configuration mode.**
web admin customer name username {password string | secret {0 | 5} string} **Example:** Router(config-telephony-service)# web admin customer name user44 password w10293847	Defines a username and password for a customer administrator. The default username is Customer. There is no default password. • name username—Username of customer administrator. • password string—String to verify customer administrator

 Copyright © 2005, Cisco Systems, Inc.

Configuring Administrative User Classes (Cont.)

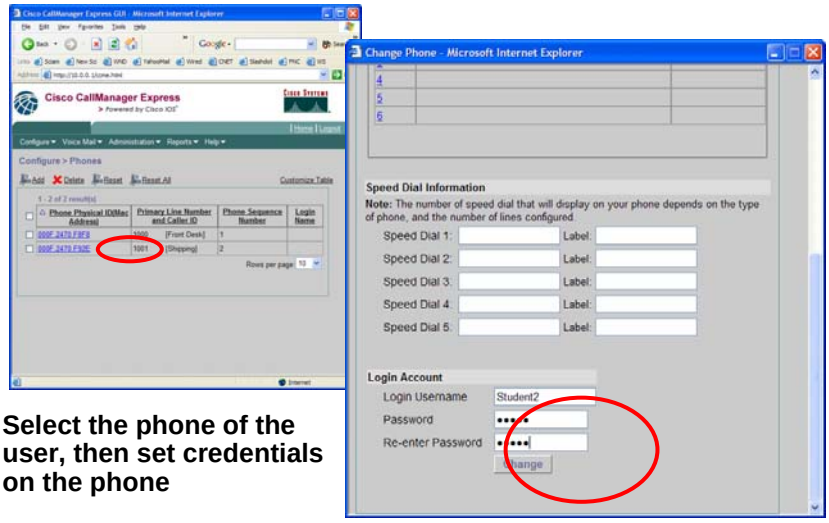
Two ways to define phone users:

- **Through the System Administrator GUI**
- **From the CLI of the CallManager Express**

© 2005 Cisco Systems, Inc. All rights reserved.

Like the customer administrator, phone users can also be configured from either the GUI or the CLI. One set of credentials may be defined per phone.

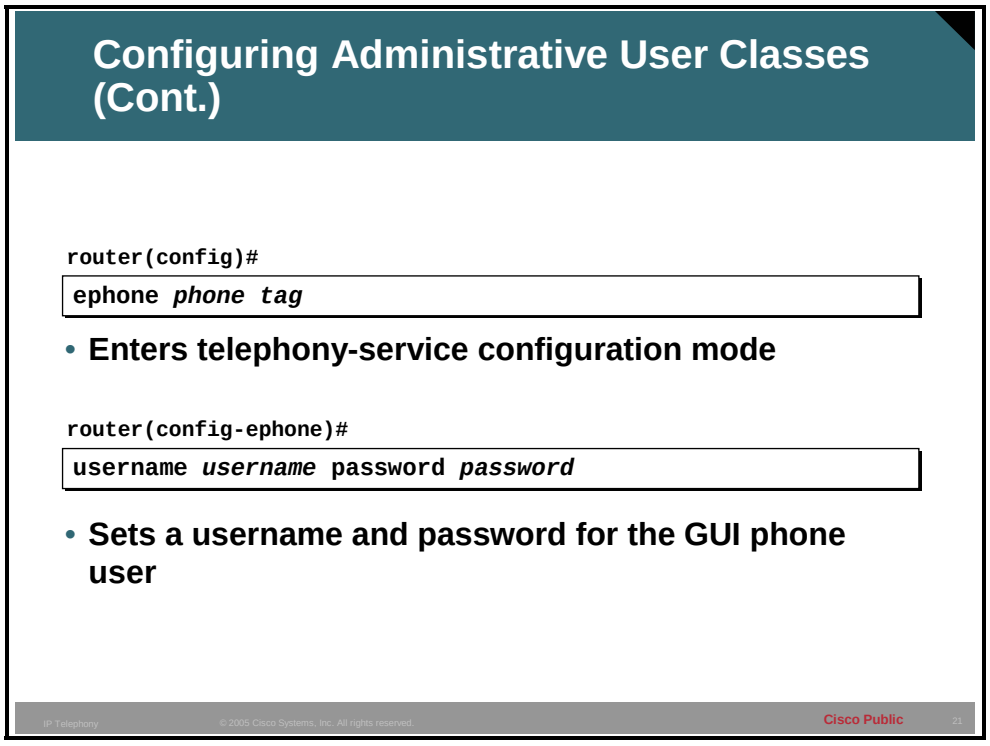
Configuring Administrative User Classes (Cont.)



Select the phone of the user, then set credentials on the phone

© 2005 Cisco Systems, Inc. All rights reserved.

To set phone user credentials from the phone user Web pages, go to the “Configure” drop-down menu and select “Phones.” Either add a new phone or change an existing phone by selecting it. Scroll to the bottom of the page and in the “Login Account” area, define the user and password. Select the “Change” button to commit the changes.



To configure the phone user credentials for a phone, enter the ephone sub configuration mode by entering the **ephone *phone*** tag from global configuration mode. Then enter the **username *username* password *password*** command. This will be used by the phone users to log into the GUI Web interface and for any TAPI lite connections.

Note	The password will be shown in clear text in the router configuration.

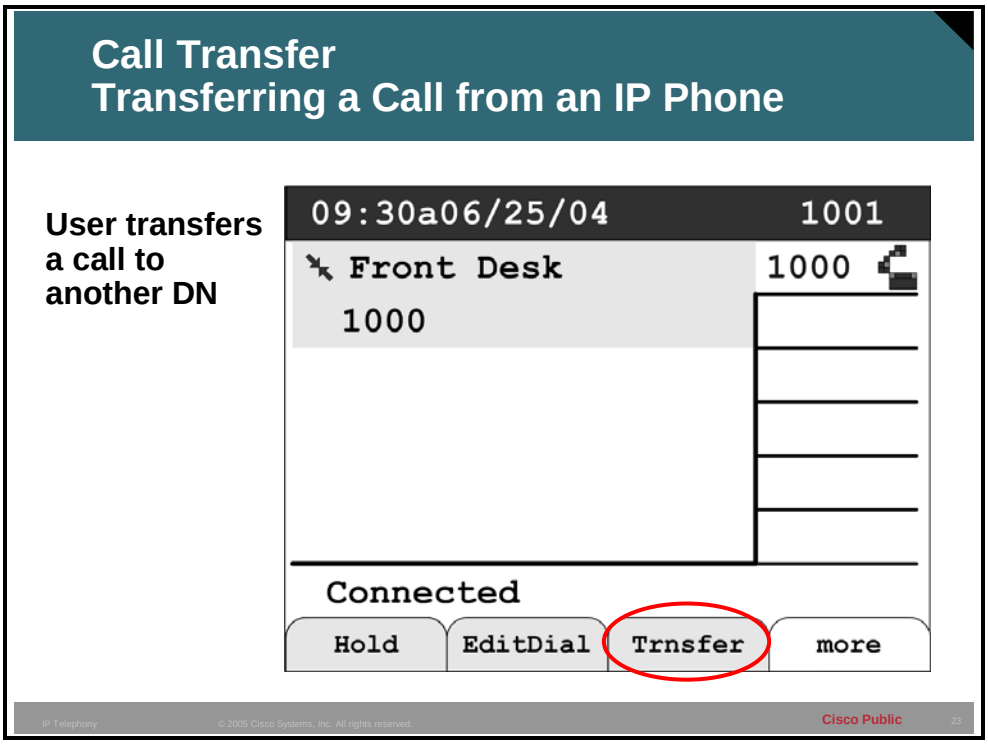
Command	Purpose
ephone *phone tag* **Example:** `Router(config)#` ephone 44	**Enters ephone configuration mode to register Cisco IP phones.**
username *username* password *password* **Example:** Router(config-ephone)# username prx password pk59wq .	Assigns a phone user login account name and password. This allows individual phone users to log in to the Cisco CME router through a Web interface to change a limited number of personal settings.

 Copyright © 2005, Cisco Systems, Inc.

Configuring Phone Features

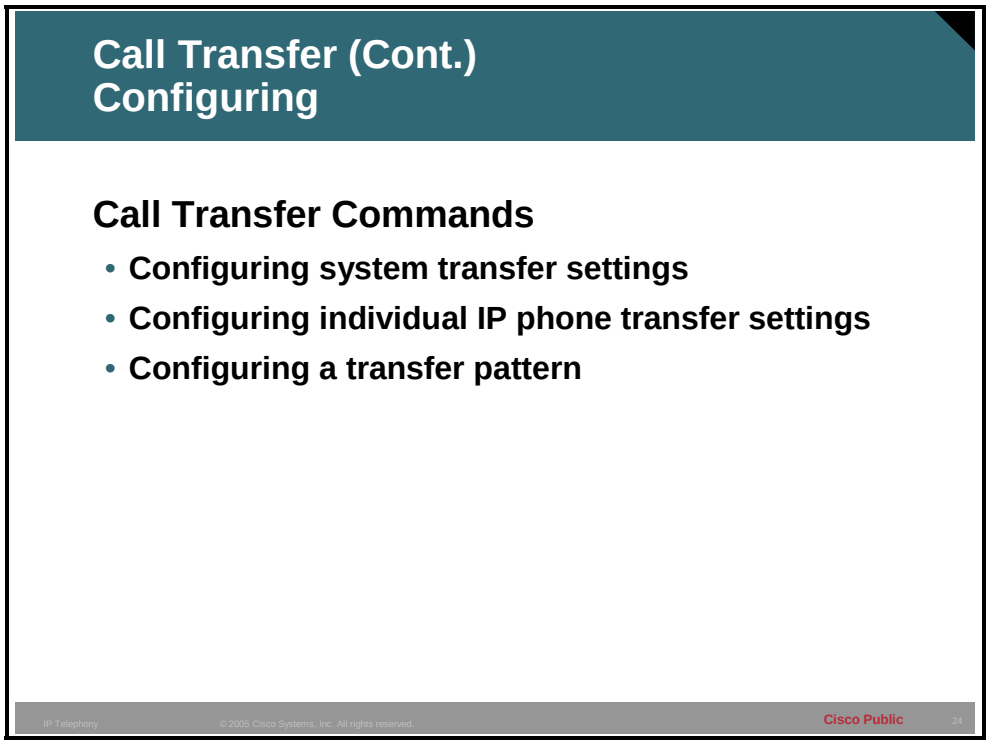
Call Transfer

This topic describes the Cisco CME transfer commands.



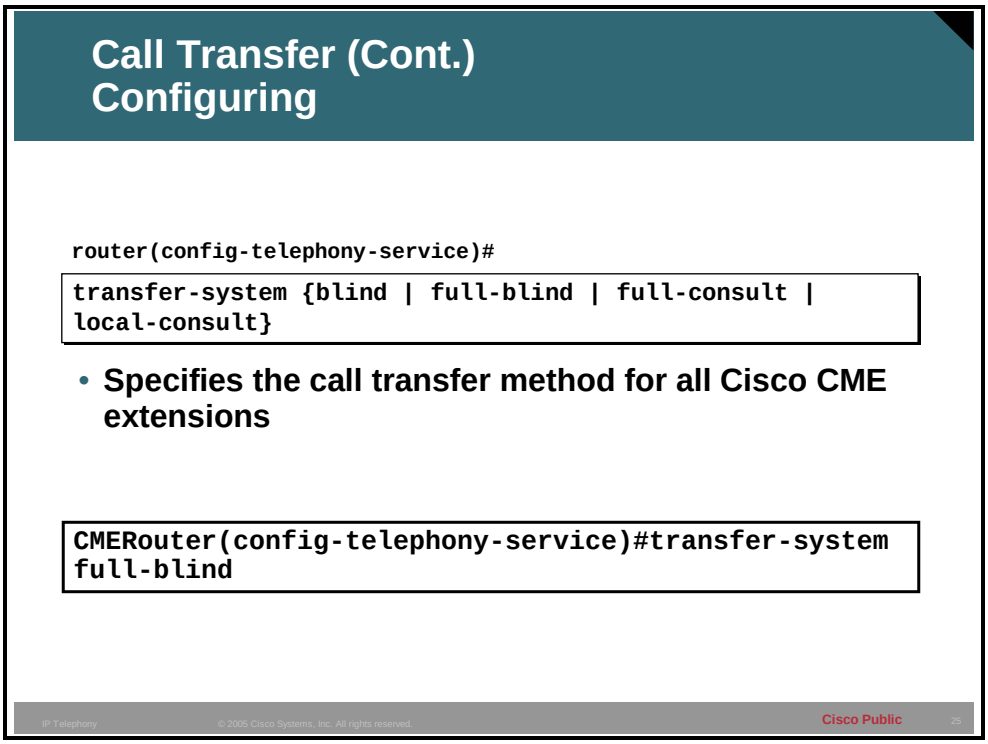
Transferring a caller to another directory number is a very common occurrence in the enterprise. The person on the IP phone can initiate a transfer by using the functions displayed on the IP phone display. To transfer a caller the user can initiate the transfer by pressing the “Trnsfer” softkey button and dialing the number that the call will be transferred to.

Depending on the configuration deployed on the Cisco CME system the call will either be blindly transferred or transferred with a consultation first. A blind transferred occurs when the transferor does not know if the extension that the call was transferred to will answer the call. The extension may be busy, ring no answer, or the extension may be answered. A consultative transfer differs in that the transferor is connected to the transfer target extension and then if satisfied finalizes the transfer which will connect the caller and the transfer target together.



Call transfer is a function that can be configured in various ways, depending on the supported protocols. These call transfer commands include system-wide settings that can be overridden with phone specific settings, which can be overridden by settings on the transfer pattern.

 Copyright © 2005, Cisco Systems, Inc.



Transfer System

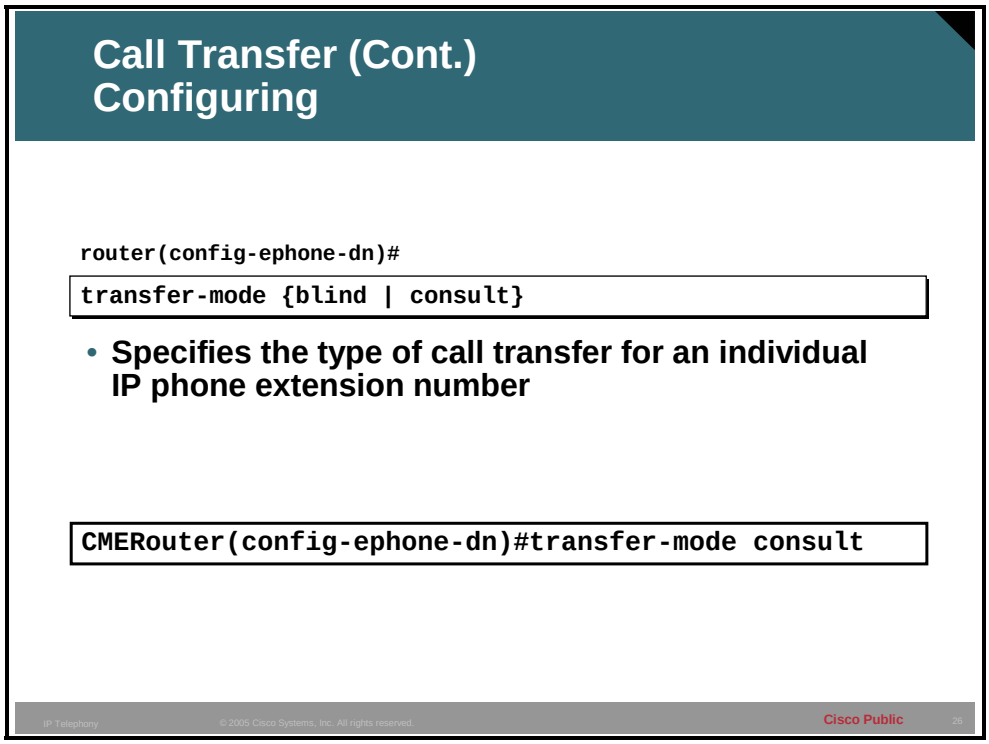
To specify the call transfer method for IP phone extensions system-wide that use the ITU-T H.450.2 standard, use the **transfer-system** command in telephony-service configuration mode. To disable the call transfer method, use the **no** form of this command.

When H.450.2 call transfer is selected using the **full-blind** blind keyword the call is transferred without consultation using the H.450.2 standard. When a call is transferred using the **blind** keyword (the default) the call is blindly transferred using a single line and a Cisco proprietary method. When the **full-consult** keyword is used the call is transferred with consultation using the H.450.2 standard. The **local-consult** uses consultation with local calls and blindly transfers for non-local calls. The **local-consult** uses a proprietary transfer mechanism and is not commonly used.

Note	Cisco CME 3.1 provides full call-transfer and call-forwarding interoperability with call processing systems on the network that support H.450.2, H.450.3, and H.450.12 standards. For call processing systems that do not support H.450 standards, Cisco CME 3.1 provides VoIP-to-VoIP hairpin call routing without requiring the use of the special Tool Command Language (Tcl) script that was needed in earlier releases of Cisco CME.

Transfer System Command

Command	Description
transfer-system {blind | full-blind | full-consult | local-consult} **Example:** Router(config-telephony-service)# transfer-system full-consult	Defines the call transfer method to allow call transfer with consultation for all lines served by the router. • **blind**—Calls are transferred without consultation with a single phone line using the Cisco-proprietary method. • **full-blind**—Calls are transferred without consultation using H.450.2 standard methods. • **full-consult**—Calls are transferred with consultation using H.450.2 standard methods and a second phone line if available. The calls fall back to full-blind if the second line is unavailable. • **local-consult**—Local calls are transferred with local consultation using a second phone line if available. The calls fall back to blind for non-local consultation or non-local transfer target.



Transfer Mode

To specify the type of call transfer for an individual IP phone extension that uses the ITU-T H.450.2 standard, use the **transfer-mode** command in ephone-dn configuration mode. To remove this specification, use the **no** form of this command.

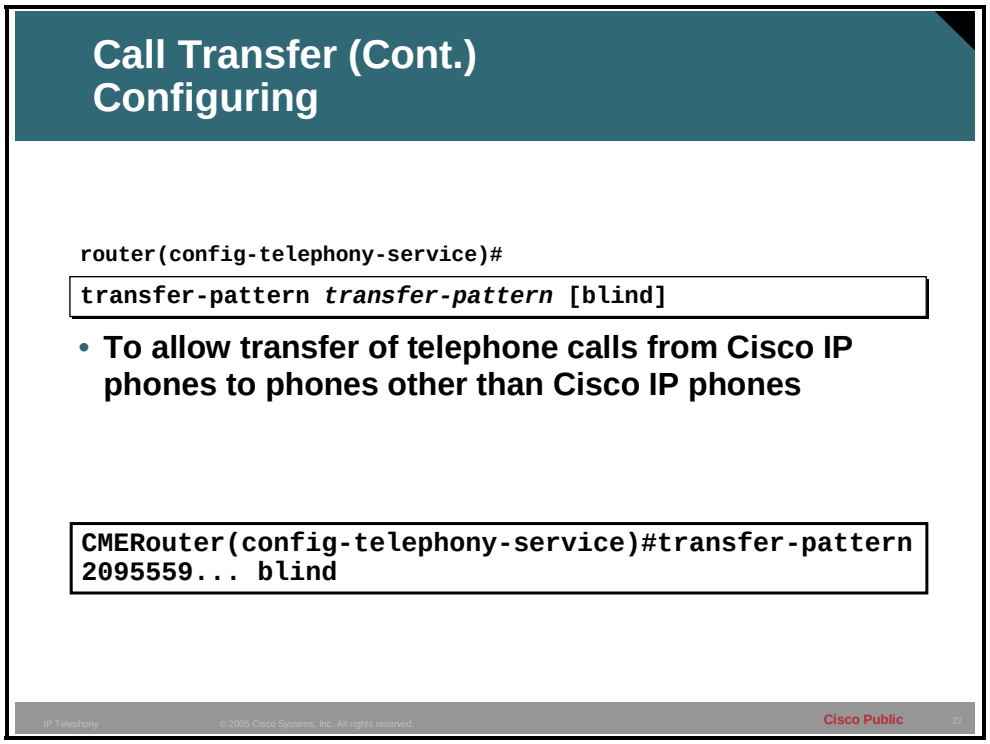
The **transfer mode** command specifies the type of call transfer for an individual Cisco IP phone extension that is using the ITU-T H.450.2 protocol. It allows you to override the system default **transfer-system** setting (full-consult or full-blind) for that ephone-dn extension. For example, in a Cisco CME network that is set up for consultative transfer, a specific extension

 Copyright © 2005, Cisco Systems, Inc.

with an auto-attendant that automatically transfers incoming calls to specific extension numbers can be set to use blind transfer because auto-attendants do not use consultative transfer.

Transfer Mode Command

Command	Description
transfer-mode {blind | consult} **Example:** Router(config-ephone-dn)#transfer-mode blind	This command specifies the type of call transfer for an individual Cisco IP phone extension that is using the ITU-T H.450.2 protocol. It allows you to override the system default transfer-system setting (full-consult or full-blind) for that extension. • **blind** — Transfers calls without consultation using a single phone line. • **consult** — Transfers calls with consultation using a second phone line, if available. .



Transfer Pattern

To allow the transfer of telephone calls from CallManager IP phones to non-local destinations, use the **transfer-pattern** command in telephony-service configuration mode. To disable these transfers, use the **no** form of this command.

The **transfer-pattern** command allows you to transfer calls to destinations other than local IP Phones. This includes non-IP phones and external destinations. A call is then established between the transferred party and the new recipient. By default, all Cisco IP phone extension numbers are allowed as transfer targets. The default is that all transfers will be consultative in nature. The optional **blind** keyword forces calls that are transferred to numbers that match the transfer pattern to be executed as blind or full-blind transfers, overriding any settings made using the **transfer-system** and **transfer-mode** commands. When defining transfers to non-local numbers, it is important to note that transfer-pattern digit matching is performed before translation-rule operations. Therefore, you should specify in this command the digits actually entered by phone users before they are translated.

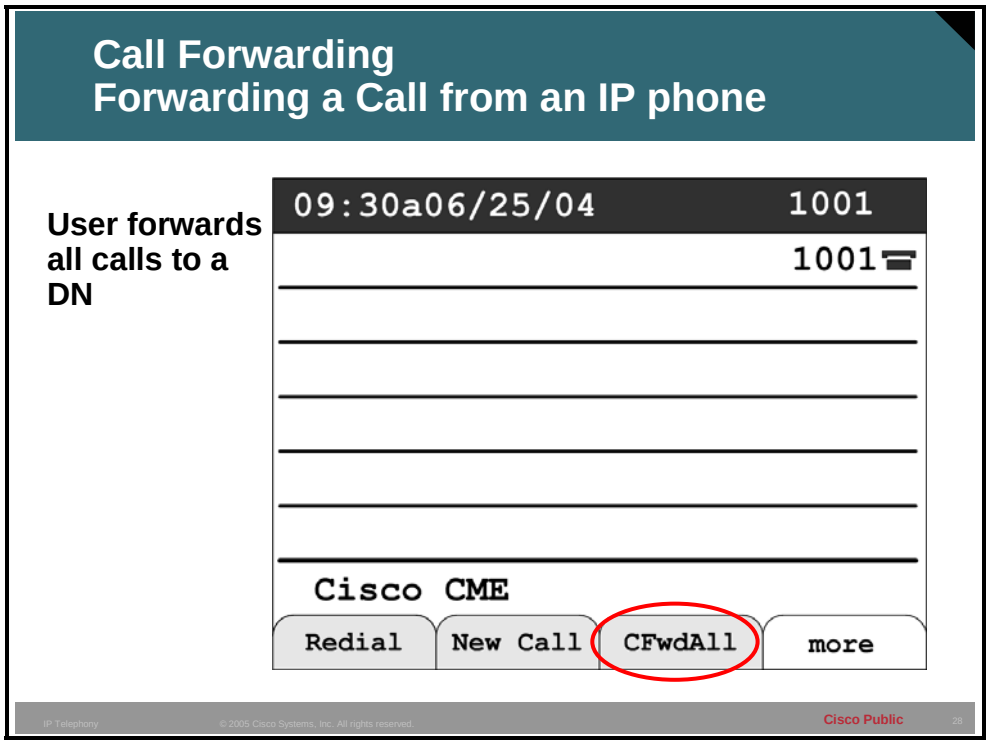
 Copyright © 2005, Cisco Systems, Inc.

Transfer Pattern Command

Command	Description
transfer-pattern *transfer-pattern* [blind] **Example:** Router(config-telephony-service)# transfer-pattern .T	Allows transfer of telephone calls by Cisco IP phones to specified phone number patterns. If no transfer pattern is set, the default is that transfers are permitted only to other local IP phones. *transfer-pattern*—String of digits for permitted call transfers. Wildcards are allowed. A pattern of .T transfers all calling parties using the H.450.2 standard. • **blind**—(Optional) When H.450.2 consultative call transfer is configured, forces transfers that match the pattern specified in this command to be executed as blind transfers. Overrides settings made using the transfer-system and transfer-mode commands. Note When defining transfers to non-local numbers, it is important to note that transfer-pattern digit matching is performed before translation-rule operations. Therefore, you should specify in this command the digits actually entered by phone users before they are translated.

Call Forwarding

This topic describes the Cisco CME call forwarding commands.



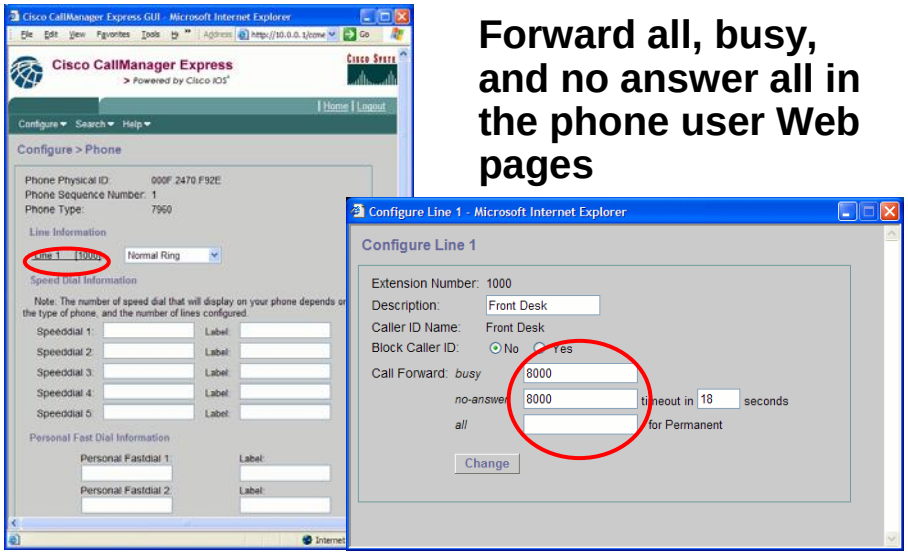
Forwarding call settings govern the behaviors and destinations that the calls will be forwarded to in various situations that may occur such as the destination is busy, or the phone rings but no one answers, or all calls may be desired to be forwarded. On a users phone the ring no answer and busy settings usually will be set by the administrator to go to the voice mailbox of that user. Other type of extensions may not have the same behavior and might have no settings or may forward to another extension constructing something like a hunt group.

The forward all setting can be set on the IP phone by the user. For example a user may be going on vacation and wishes all calls to be handled by another employee. This is a very common situation that occurs in many deployments.

Using the phone to set the forward all setting is done by pressing the “CFwdAll” softkey button and entering the number to which all calls will be forwarded, followed by the # key to tell the system you are done entering digits. The forward destination will be displayed on the bottom of the IP phone screen. To remove the forward all, press the “CFwdAll” softkey button again. This turns off the forward all. The user or administrator can also use the GUI Web interface of Cisco CME to configure the call forward options.

 Copyright © 2005, Cisco Systems, Inc.

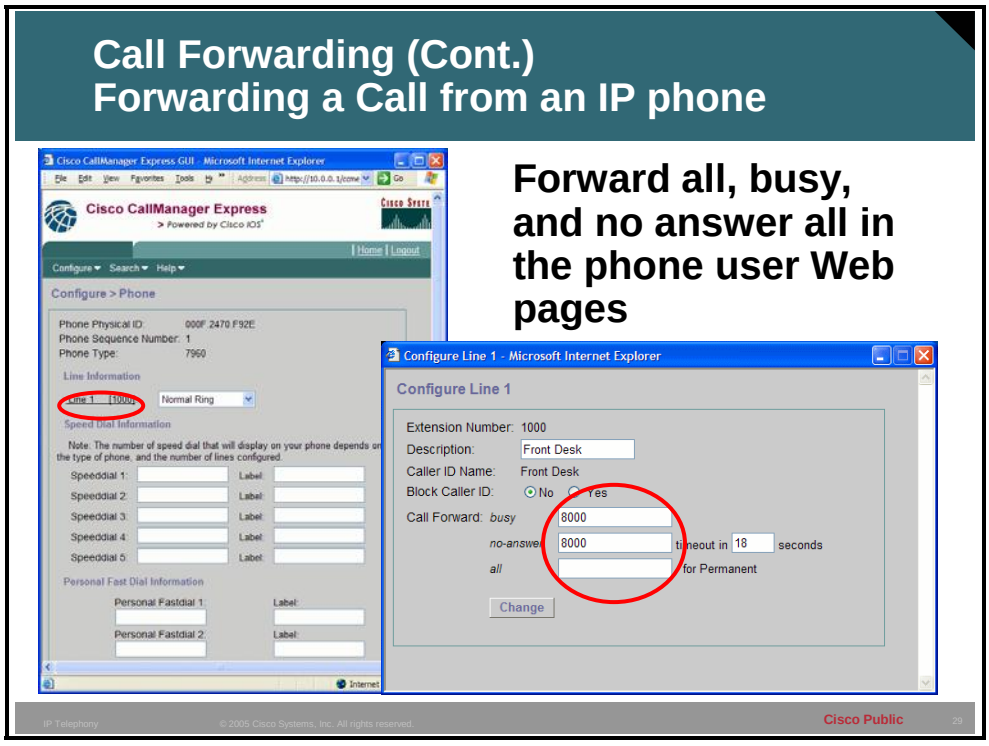
Call Forwarding (Cont.)
Forwarding a Call from an IP phone



Forward all, busy, and no answer all in the phone user Web pages

© 2005 Cisco Systems, Inc. All rights reserved.

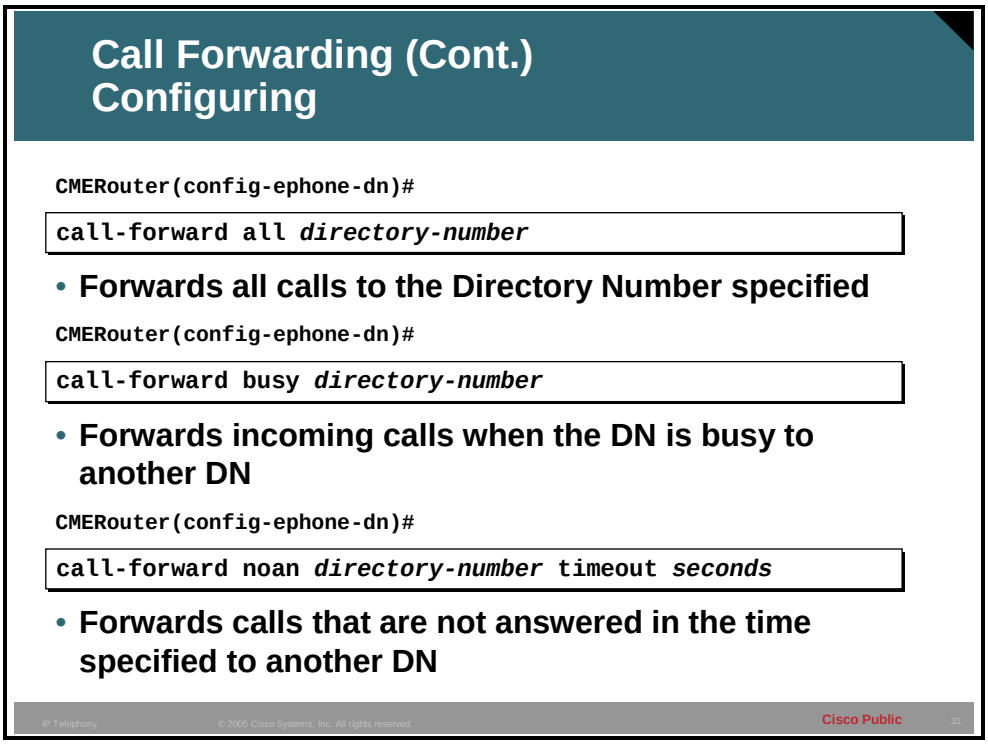
From the phone user Web interface, the user is able to configure a line on the phone to forward all, forward busy and forward no answer. A user is only able to configure the phone on which he/she has credentials defined.



There are five call forwarding commands that can be configured from the command line of the Cisco CME router. These commands are the following:

- Call forward all (CLI, GUI, Phone)
- Call forward busy (CLI, GUI)
- Call forward no answer (CLI, GUI)
- Call forward max-length (CLI)
- Call forward pattern (CLI)

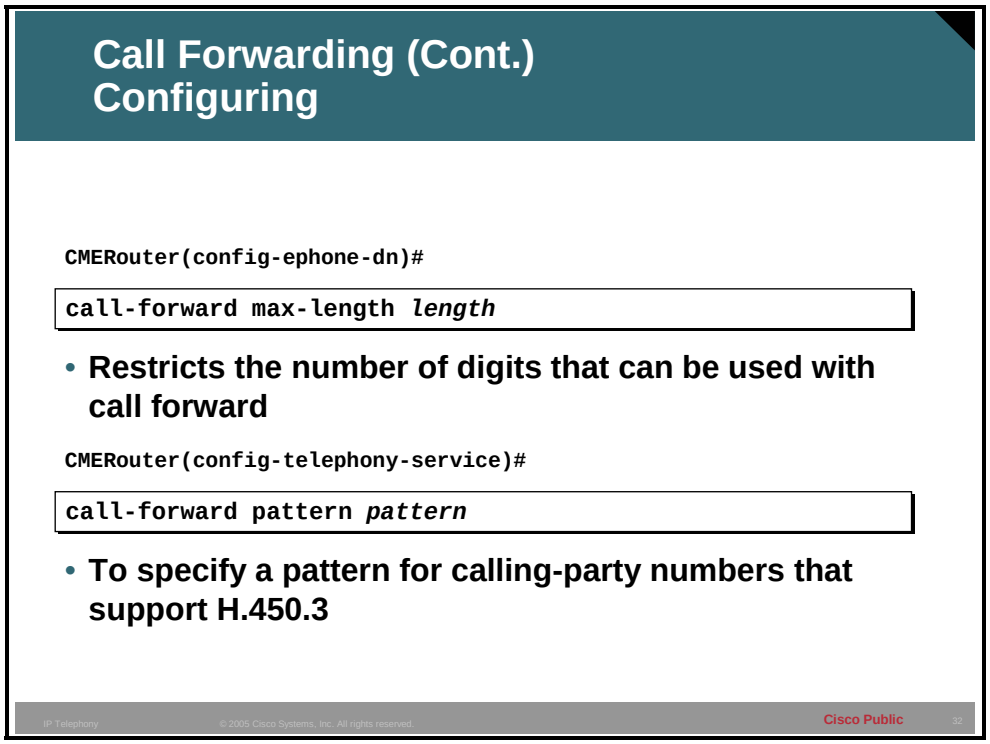
 Copyright © 2005, Cisco Systems, Inc.



Call Forward All, Call Forward Busy and Call Forward No Answer

The **call-forward all** command can be configured from the CLI, this setting can also be made from GUI interface, or the IP phone. The **call-forward busy** command can be configured from the CLI and this setting can also be configured in the GUI interface. The **call-forward noan** command can be configured from the CLI and this setting can also be defined from the GUI interface.

Command	Purpose
call-forward all *directory-number* Example: Router(config-ephone-dn)#call-forward all 1001	To configure call forwarding so that all incoming calls to an extension (ephone-dn) are forwarded to another extension.
call-forward busy *directory-number* Example: Router(config-ephone-dn)# call-forward busy 8000	To configure call forwarding so that incoming calls to a busy extension (ephone-dn) are forwarded to another extension.
call-forward noan *directory-number* timeout *seconds* Example: Router(config-ephone-dn)# call-forward noan 8000 timeout 15	To configure call forwarding so that incoming calls to an extension (ephone-dn) that does not answer are forwarded to another extension.



Call Forward Maximum Length and Call Forward Pattern

The **call-forward max-length** command is used to restrict the number digits that a user can enter for the forwarding calls. This is important to prevent a user from forwarding calls to destinations that might incur toll charges. This command can only be configured from the command line. If the **call-forward max-length 0** is configured the call forward softkey will be grayed out and not available through the IP phone. However it is important to realize that the phone user can still set the forward setting in the GUI Web interface even if the max length is set to 0.

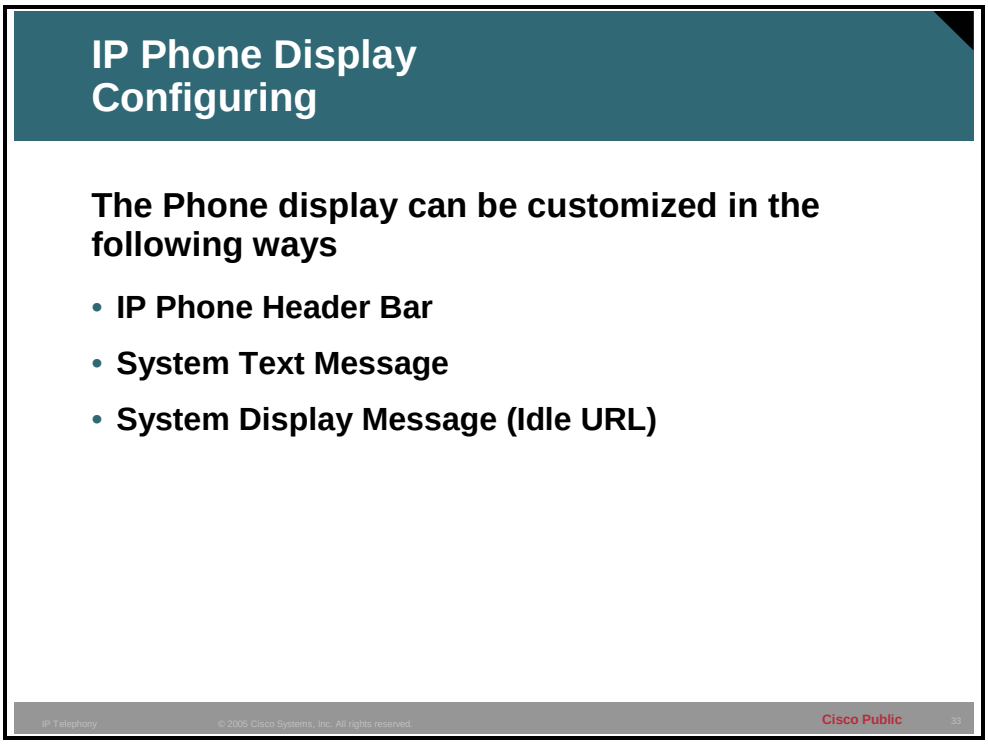
The **call-forward pattern** command attaches a pattern against the phone number of the calling party. When an extension number has forwarded its calls, and an incoming call is received for that number, the router sends an H.450.3 response back to the original calling party to request that the call be placed again using the forward-to destination. Calling numbers that do not match the patterns defined using this command are forwarded using Cisco-proprietary call forwarding for backward compatibility. Configuring this for numbers that do not support H.450.3 could result in dropped calls. This command should be configured to match only calling numbers that support H.450.3 protocol.

Command	Purpose
call-forward max-length *length* Example: Router(config-ephone-dn)#call-forward max-length 5	Restricts the number of digits that can be entered using the CfwdAll soft key on an IP phone..
call-forward pattern *pattern* Example: Router(config-telephony-service)#call-forward pattern 9.T	Specifies a pattern for calling-party numbers that are able to support the ITU-T H.450.3 standard for call forwarding,.

 Copyright © 2005, Cisco Systems, Inc.

IP Phone Display

This topic describes the IP phone display options.



The display of the IP phone can be customized to reflect the needs and identity of the enterprise that the CallManager system and phones are being deployed for.

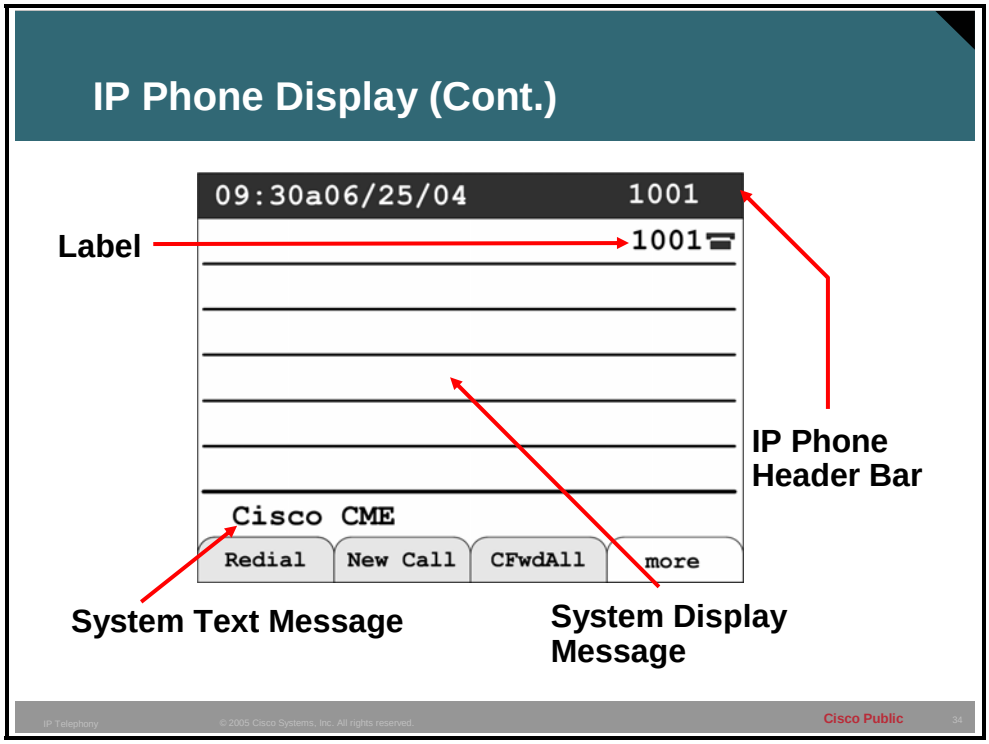
Normally, the IP phone header bar, or top line, of a 7940 or 7960 phone replicates the text that appears next to the first line button. The header bar can, however, contain a user-definable message instead of the extension number. For example, the header bar can be used to display a name or the full E.164 number of the phone. If no description is specified, the header bar replicates the extension number that appears next to the first button on the phone.

The system text message replaces the default “Cisco CallManager Express” message towards the bottom of the phone. There is room for about 30 characters to be displayed. The message will appear when the phone is idle. This occurs when one of the following three conditions is met:

- A busy phone goes on-hook
- A phone receives a keepalive
- The phone restarts

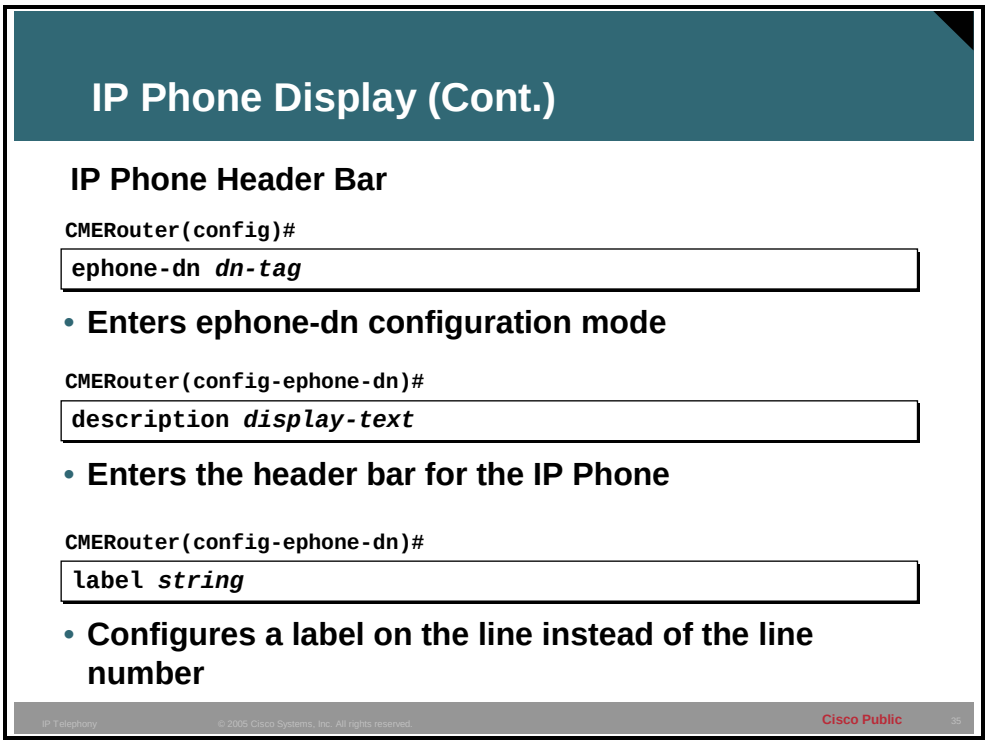
The system display message feature allows you to specify a file to display on 7940 and 7960 Cisco IP phones when they are not in use. You can use this feature to provide the phone display with a system message that is refreshed at configurable intervals, similar to the way that the system text message feature provides a message. The difference between the two is that the system text message feature displays a single line of text at the bottom of the phone display, whereas the system display message feature can use the entire display area and contain graphic images.

The system display message feature requires a back-end Web server to serve the browser page to the phone display, as the Cisco CME system only provisions the URL. The system display message display can also provide soft keys for the phone and thereby take input from the phone user for interactive services.



This graphic shows the different areas that will be present on the display of a Cisco CME controlled phone. Theses features can be customized for the current implementation.

 Copyright © 2005, Cisco Systems, Inc.



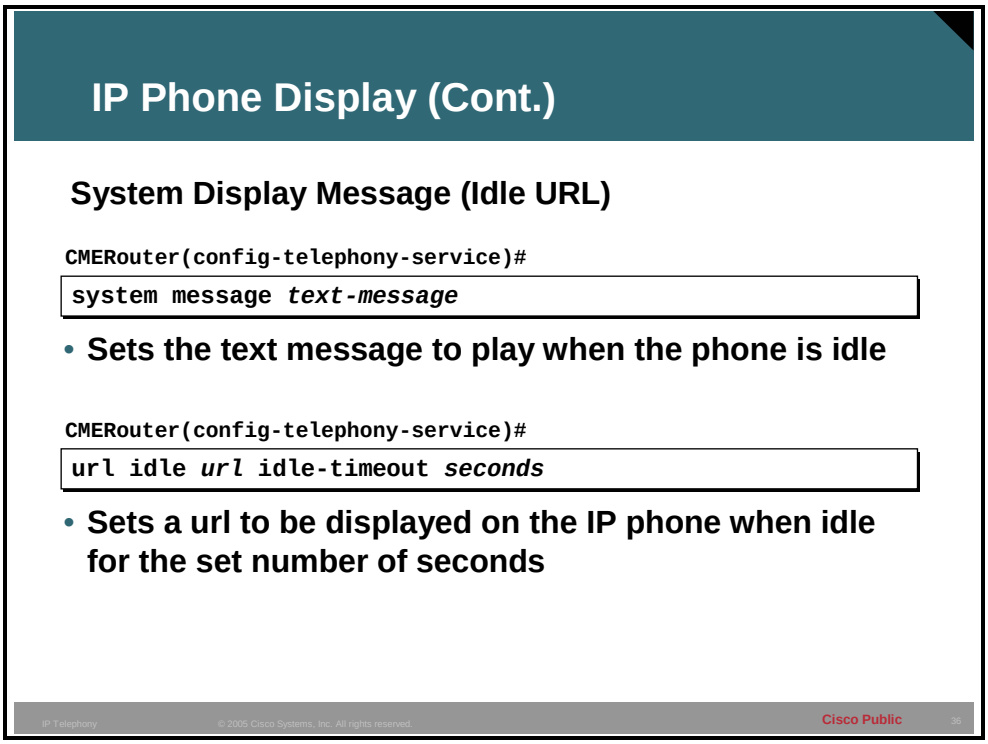
The **description** command is use to change the IP header bar of a phone. A common use of this command is to enter the DID (if there is one) of the first line. This allows users to easily see the number that someone on the PSTN could use to call them on the current phone. However, any text or numbers could be displayed here.

To create a text identifier instead of a phone-number display for an extension on an IP phone console uses the **label** command.

Note	The phone must be reset to have any changed to the header bar appear

Command	Purpose
ephone-dn *dn-tag* Example: Router(config)#ephone-dn 5	Enters ephone-dn configuration mode. • dn-tag—The unique sequence number that identifies the ephone-dn for which the description should be in effect.
Description *display-text* Example: Router(config-ephone-dn)#description 206-295-7561	Defines a description for the header bar of a Cisco IP Phone 7940 or Cisco IP Phone 7960 that has the specified ephone-dn associated with its first line button. • display-text—Alphanumeric character string, up to 40 characters. String is truncated to 14 characters in the display.
Label *string* Example: Router(config-ephone-dn)#label user10	To create a text identifier instead of a phone-number display for an extension on an IP phone console. The phone must be rebooted to receive the changes.

 Copyright © 2005, Cisco Systems, Inc.



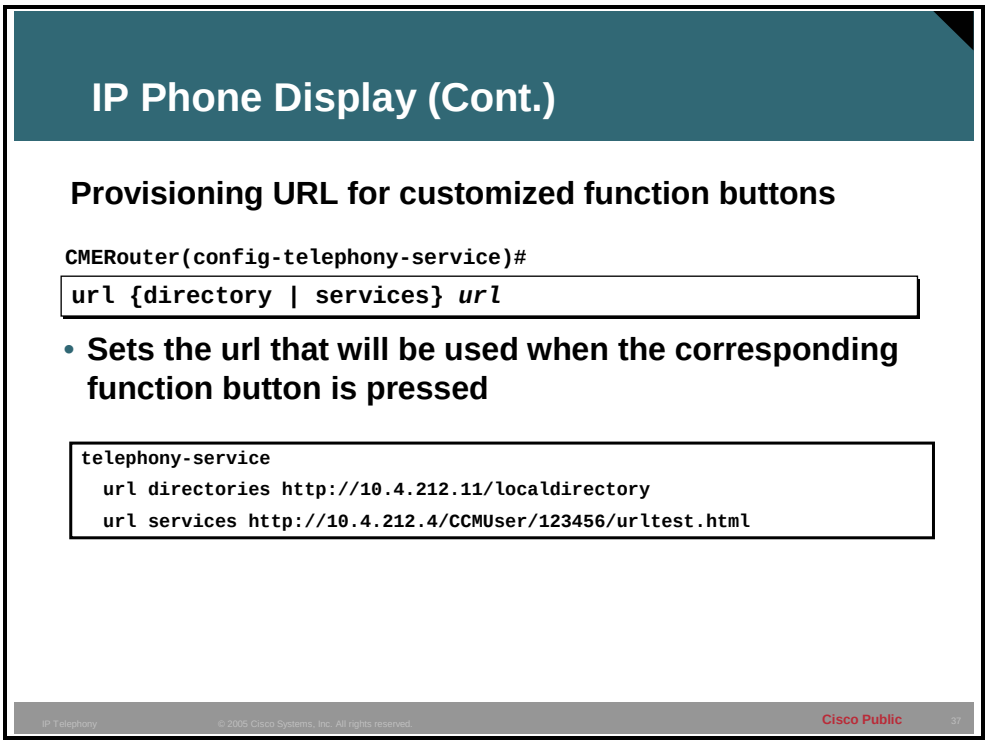
The **system message** command allows a message to be displayed on all phones in the Cisco CME system. This message is alphanumeric text only and the size of the message will vary based upon the model of phone. A common use of this command is to display the name of the company on all the phones.

The **url idle** command allows the functionality of the **system message** command to be extended to more than just a text message. The **url idle** command allows the Cisco CME router to point all the phones to a URL that resides on a back-end Web server. This Web server can then provide content in the form of text, graphics or interactive applications that will appear on the IP phones after a definable period of inactivity. These applications are written using XML. For more information, go to http://www.cisco.com/go/developersupport.

Note	The Cisco CME router should not be the Web server that serves the idle url as it will ask for credentials.

Command	Purpose
System message *text-message* Example: Router(config-telephony-service)#system message IPTXClass	Sets the message to display when a phone is idle. Uses proportional-width font, so the number of characters that are displayed varies based on the width of the characters that are used. The maximum number of displayed characters is approximately 30.
url idle *url* idle-timeout *seconds* Example: Router(config-telephony-service)#url idle http://10.0.0.1/phoneapps/logo timeout 35	Defines a URL that contains a file to display on the phone when the phone is not in use, and specifies the interval between refreshes of the display, in seconds. • url—Any URL that conforms to RFC 2396. • seconds—Range is from 0 to 300.

 Copyright © 2005, Cisco Systems, Inc.



The Cisco IP Phone 7940 and the Cisco IP Phone 7960 have customized function buttons that show the phone call status and activities on the display panels. These customized function buttons also invoke programmable non-call related services. There are two buttons that would be commonly modified to linked to a programmable URLs. This allows the administrator to override any default settings that may be assigned to the function buttons. The Messages and information button should not be customized and the Settings button cannot be customized.

Specific URLs are provisioned on the Cisco IP phone to populate these buttons. The URLs point to XML-based Web pages formatted with XML tags that the Cisco IP phone understands and uses. When you press a function button, the Cisco IP phone uses the configured URL to access the appropriate XML Web page for instructions. The Web page sends instructions to the Cisco IP phone to display information on the screen for you to navigate. You can select options and enter information by using soft keys and the scroll button.

The Cisco IP Phone 7940 and Cisco IP Phone 7960 can support four URLs in association with the four programmable feature buttons on IP phones. The four feature buttons on an IP phone are configured using the **url** command keywords. The Settings button is managed entirely by the phone and this fifth button may not be modified. Operation of these services is determined by the IP phone capabilities and the content of the referenced URL.

Note	The Cisco CME router should not be the Web server that serves the idle url as it will ask for credentials.

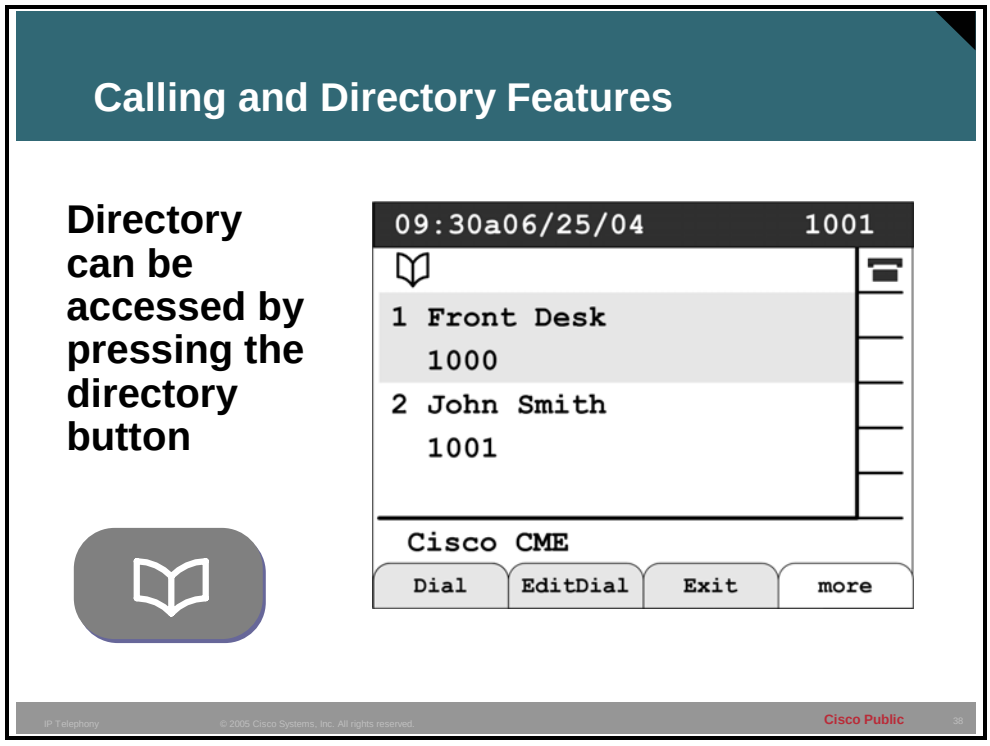
URL Commands

Command	Description
url {**directory** | **information** | **messages** | **services**} *url* **Example:** Router(config-telephony-service)# url information http://10.4.212.4/CCMUser/GetTelecasterHelpText.asp	Provisions URLs for use by the Cisco IP phones. The four keywords (**directory**, **information**, **messages**, and **services)** correspond with the four feature buttons on an IP phone: Directories, Information, Messages, and Services. The purpose of the **url** command is simply to provision the URLs through the SEPDEFAULT.cnf configuration file supplied by the Cisco CME router to the Cisco IP phones during phone registration. The maximum character length for the URL is 128. You can disable the local directory by entering the **url directories none** command. You must reset the Cisco IP phones before the **url** command can take effect. **Note** By default, the router automatically uses the local directory service. Provisioning the directory URL to select an external directory resource disables the Cisco CME local directory service.

 Copyright © 2005, Cisco Systems, Inc.

Calling and Directory Features

This topic describes calling and directory features.



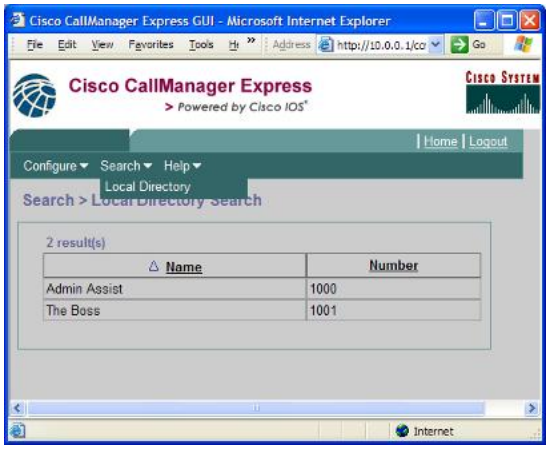
When a user does not know the number of another subscriber of commonly used external number the corporate directory that resides in the Cisco CME can be accessed and the number looked up and connected.

The directory of the Cisco CME is built and stored on the router from the configuration. It can be accessed by the phone users by pressing the directory button (assuming the url command has not been used to change this behavior) on the phone and then selecting the local directory or by using the phone user Web page. The user can be connected by pressing the dial softkey with an entry highlighted.

Calling and Directory Features (Cont.)

HTTP://*ip_address*/ccme.html

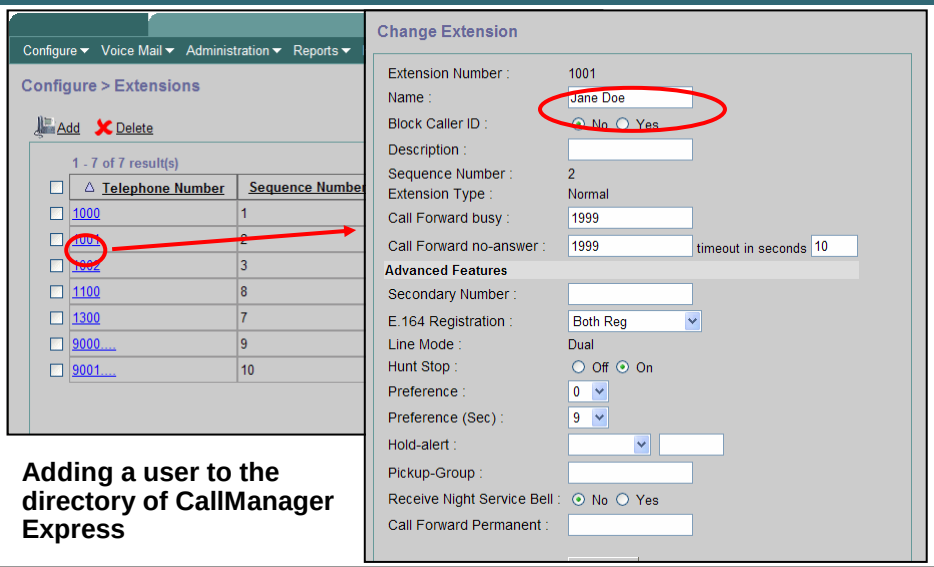
The directory can be accessed through the phone user Web page



© 2005 Cisco Systems, Inc. All rights reserved.

The directory can also be accessed through the GUI Web based interface by the phone user.

Calling and Directory Features (Cont.)



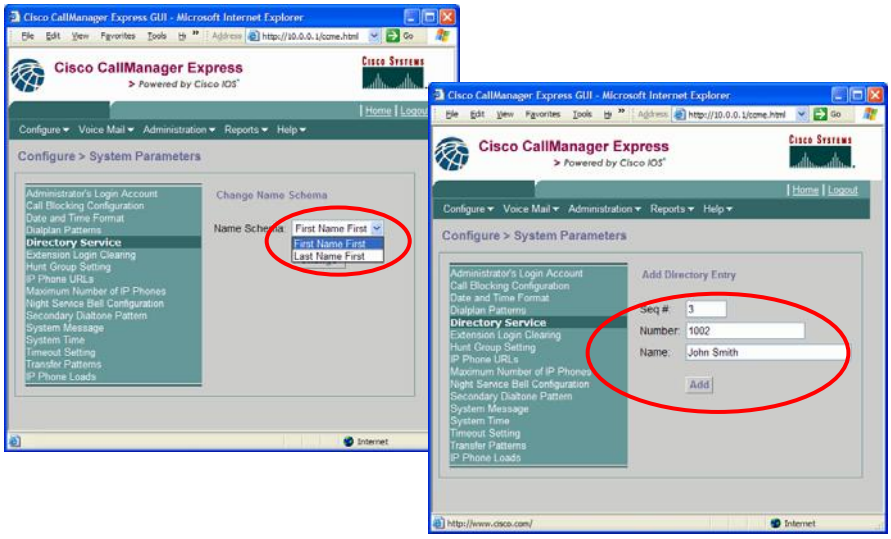
Adding a user to the directory of CallManager Express

© 2005 Cisco Systems, Inc. All rights reserved.

To add a user to the directory of Cisco CME the name field under the properties of the ephone-dn will need to be defined. The name entered should be in the same order that the Cisco CME is set to use. This topic is discussed in the next slide.

 Copyright © 2005, Cisco Systems, Inc.

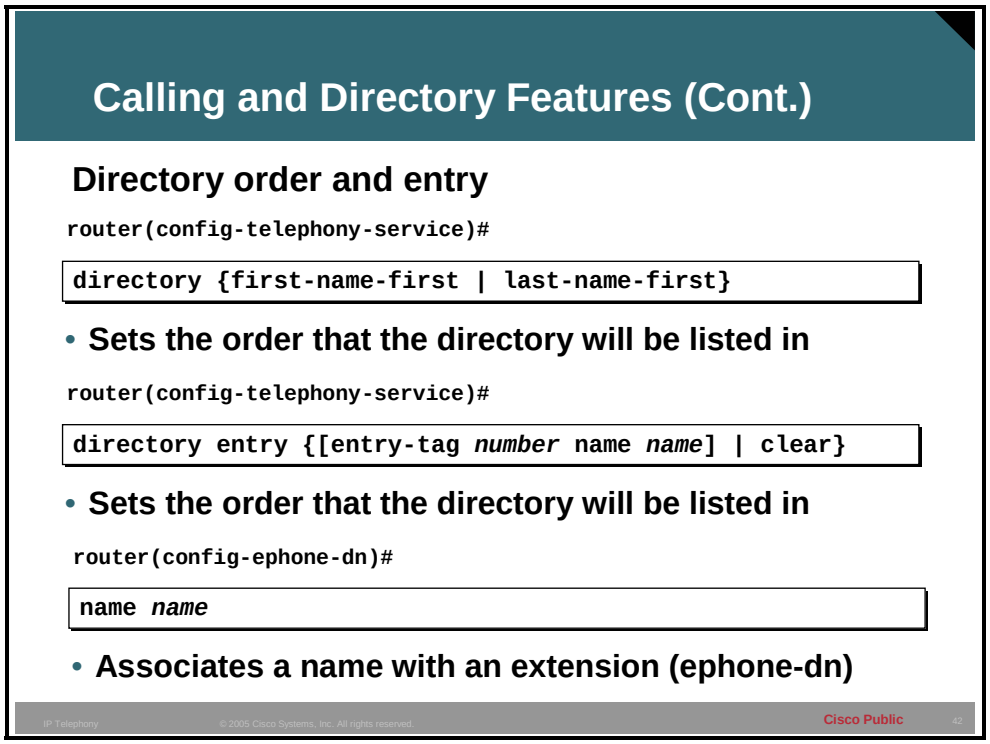
Calling and Directory Features (Cont.)



© 2005 Cisco Systems, Inc. All rights reserved.

The system administrator and, if allowed, the customer administrator can configure not only the order by which the names are listed in the directory but can also, through the Web page, add entries to the directory that are not Cisco CME controlled IP Phones.

Note This could be used to enter numbers for another site in the company that is not part of this Cisco CME installation.



The **directory** command is used to set the system-wide setting for how names will be displayed in the CME directory. The default is first name first. Entries that represent non-IP phones controlled by Cisco CME are entered into the directory from the CLI using the **directory entry** command. This can also be done by using the GUI, as seen in the previous page.

The **name** command is how an identity is associated to the ephone-dn in Cisco CME. Enter the name in the same order that was defined using the **directory** command. These names will appear in the Cisco CME directory.

Command	Purpose
directory {first-name-first | first-name-last} Example: Router(config-telephony-service)#directory first-name-first	Defines the local directory naming order. Note: the actual directory of names and phone numbers is built using the name command and the number command in ephone-dn configuration mode. When the command is set with the first-name-first keyword, you see the directory information displayed on the phone, for example, Jane J. Jones; and when the command is set with the last-name-first keyword, you see the directory information displayed on the phone as, for example, Jones, Jane J.
directory entry {[entry-tag *number* name *name*] | clear} Example: Router(config-telephony-service)#directory entry entry-tag 1 2065551212 name Seattle	To add an entry to a local phone directory that can be displayed on IP phones.
name *name* Example: Router(config-ephone-dn)# name John Smith Example: Router(config-ephone-dn)# name Smith John	Associates a name to an ephone-dn. The name should follow the entry that order defined in the **directory {first-name-first | first-name-last}** command.

 Copyright © 2005, Cisco Systems, Inc.

Productivity Tools

This topic describes the Cisco CME productivity tools.

Productivity Tools

Productivity tools for Cisco CME include:

- **Flash softkey for hookflash functionality**
- **Intercom**
- **Paging**

IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 43

Productivity Tools (Cont.)

Flash Softkey for Hookflash Functionality

```
router(config-telephony-service)#
fxo hook-flash
```

- **Enables the flash softkey button on the IP phones**

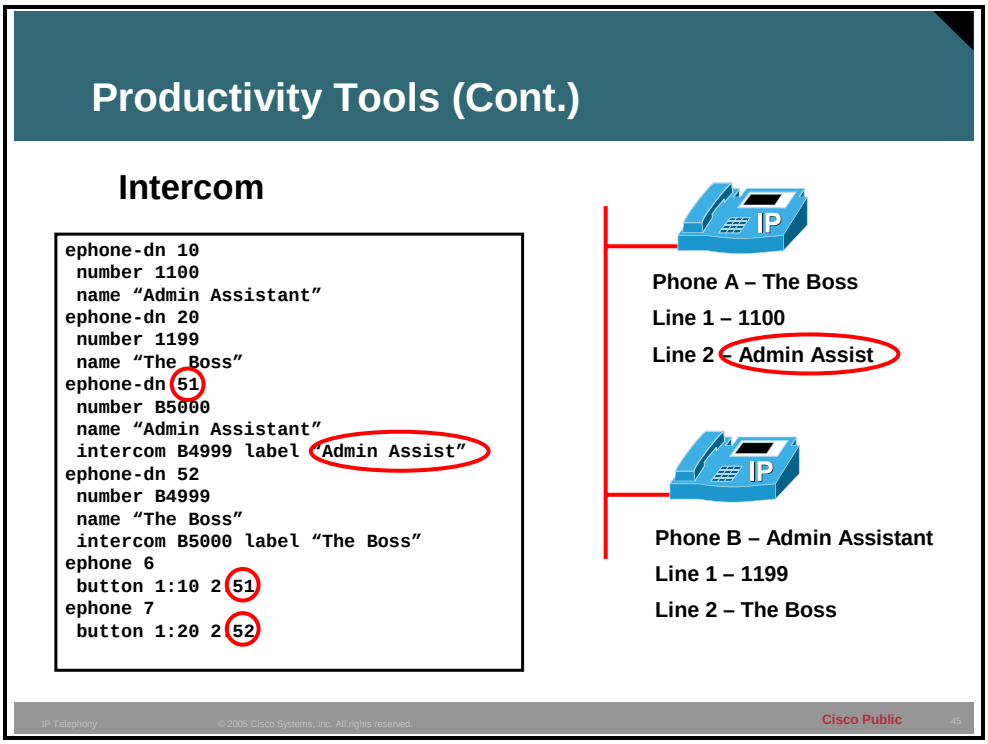
IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 44

Certain PSTN services, such as three-way calling and call waiting, require hookflash intervention from a phone user. A new soft key labeled “Flash” has been introduced to provide this functionality on FXO lines attached to the Cisco CME system. The “Flash” soft key is enabled using the **fxo hook-flash** command. Once Flash has been enabled and a reboot of the IP phone performed, the softkey is available to provide hookflash functionality during all calls except for local IP-phone-to-IP-phone calls.

Note The hookflash-controlled services can be activated only if they are supported by the PSTN connection that is involved in the call. The availability of the Flash soft key does not guarantee that hookflash-based services are actually accessible to the phone user.

Command	Purpose
fxo hook-flash Example: Router(config-telephony-service)#fxo hook-flash	Enables the flash button on the 7940 and 7960 phones for hookflash functionality

 Copyright © 2005, Cisco Systems, Inc.



Intercoms are a common feature that many deployments will desire. The intercom is commonly used between executives and assigned administrative assistants. While this is not the only situation where an intercom is used it is the most common.

Cisco CME supports intercom functionality for one-way and press-to-answer voice connections using a dedicated pair of intercom ephone-dns on two phones that speed-dial each other. When an intercom speed-dial button is pressed, a call is speed-dialed to the ephone-dn that is the other half of the dedicated pair. The called ephone-dn automatically answers the call in speakerphone mode with mute activated, which provides a one-way voice path from the initiator to the recipient.

A beep is sounded when the call is auto-answered to alert the recipient to the incoming call. To respond to the intercom call and open a two-way voice path, the recipient deactivates the mute function by taking one of the following actions:

- On a multibutton phone, pressing the **Mute** button.
- On a Cisco IP Phone 7910, lifting the handset.

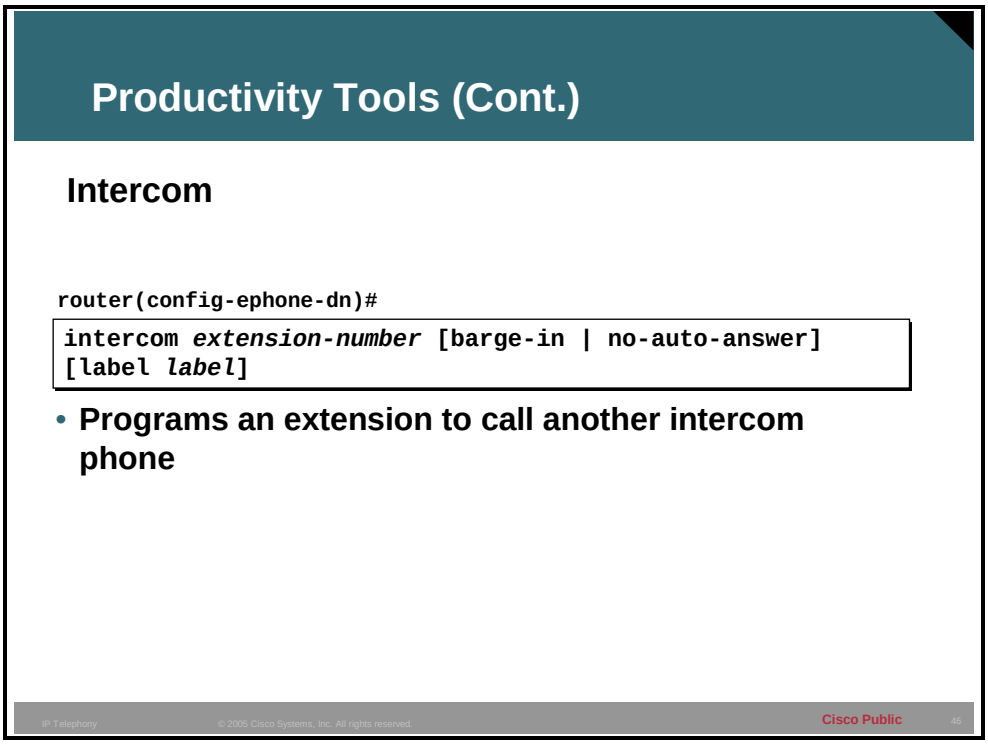
Intercom lines cannot be used in shared-line configurations. If an ephone-dn is configured for intercom operation, it must be associated with one IP phone only. The intercom attribute causes an IP phone line (ephone-dn) to operate as an autodial line for outbound calls and as an auto answer-with-mute line for inbound calls. The slide shows an intercom between a receptionist and a manager.

Any user can dial the intercom if the number of the intercom is made with the keys present on the phones. In order to configure a non-dialable intercom line you can assign the intercom ephone-dn a dialing string with an alphabetic character of A, B, C or D. No one can dial the alphabetic character from a normal phone, but the phone at the other end of the intercom can be configured to dial the number that contains the alphabetic character through the Cisco CME router. For example, the intercom ephone-dns have been assigned numbers with alphabetic

characters so that no one but the receptionist can call the manager on their intercom line, and no one but the manager can call the receptionist on their intercom line.

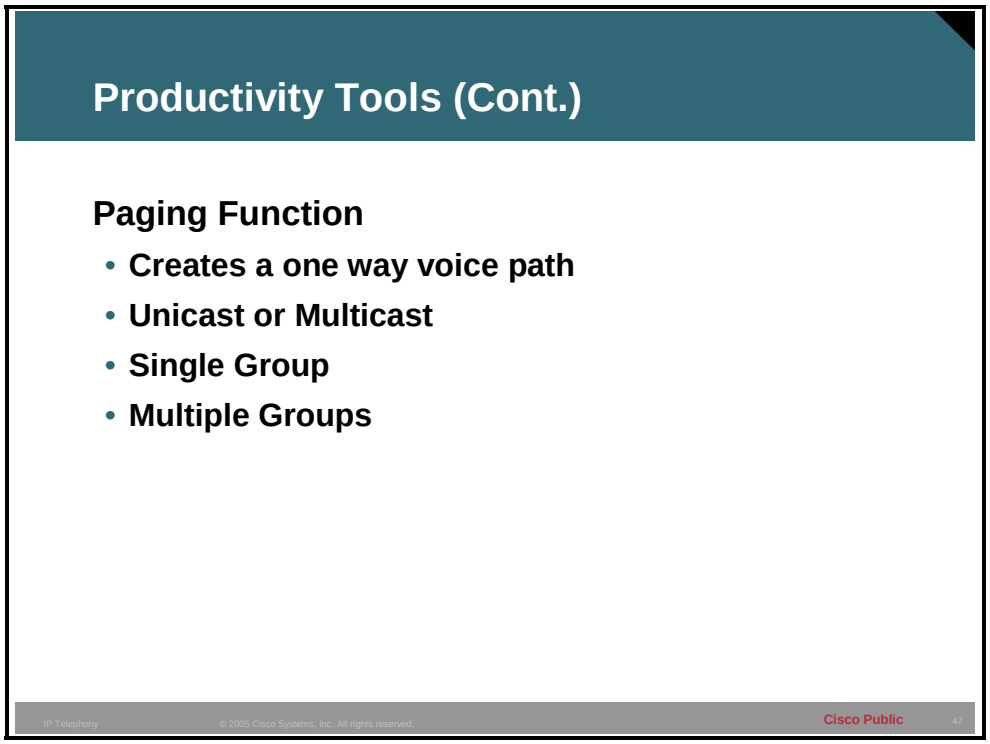
Note	An intercom requires configuration of two ephone-dns, one for each phone that makes up the intercom pair.

 Copyright © 2005, Cisco Systems, Inc.



The **intercom** command is used under the ephone-dn configuration mode; it is used to configure one half of the intercom pair. There will need to be another ephone-dn with the **intercom** command on it. This ephone-dn will then need to be assigned to a line button using the **button** command covered in Module 3. The IP phone will then need to be restarted to receive the changes.

Command	Purpose
Intercom *extension-number* [barge-in | no-auto-answer] [label *label*] Example: Router(config-ephone-dn)#intercom J3333 label “intercom to Joe”	Creates an intercom by programming a pair of extensions (ephone-dns) to automatically call and answer each other. **barge-in** (Optional) Allows inbound intercom calls to force an existing call into the call-hold state and allows the intercom call to be answered immediately. **no-auto-answer** (Optional) Disables the intercom auto-answer feature. **label *label*** (Optional) Defines an alphanumeric label for the intercom, of up to 30characters.



Audio paging provides a one-way voice path to the phones that have been designated to receive paging. It does not have a press-to-answer option like the intercom feature. Intercoms are commonly used to locate a person away from their desk, for emergency situations like a fire drill, for overhead pages using and other situations.

The paging mechanism supports audio distribution using IP multicast, replicated unicast, and a mixture of both (so that multicast is used where possible, and unicast is used for specific phones that cannot be reached using multicast).

Paging groups can be configured for a single group or for a combined group. Several paging groups can be specified in a Cisco CME system and two or more paging groups can be joined into a combined group.

A paging group is created using a dummy ephone-dn, known as the paging ephone-dn, that can be associated with any number of local IP phones. The paging ephone-dn can be dialed from anywhere, including on-net.

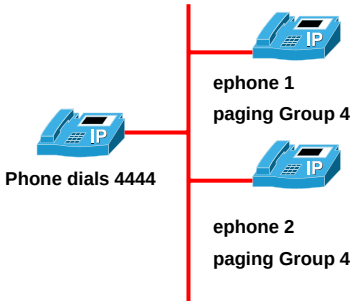
When a caller dials the paging number (ephone-dn), each idle IP phone that has been configured with the paging number automatically answers using its speakerphone mode. Displays on the phones that answer the page show the caller ID that has been set using the **name** command under the paging ephone-dn. When the caller finishes speaking the message and hangs up, the phones are returned to their idle states.

 Copyright © 2005, Cisco Systems, Inc.

Productivity Tools (Cont.)

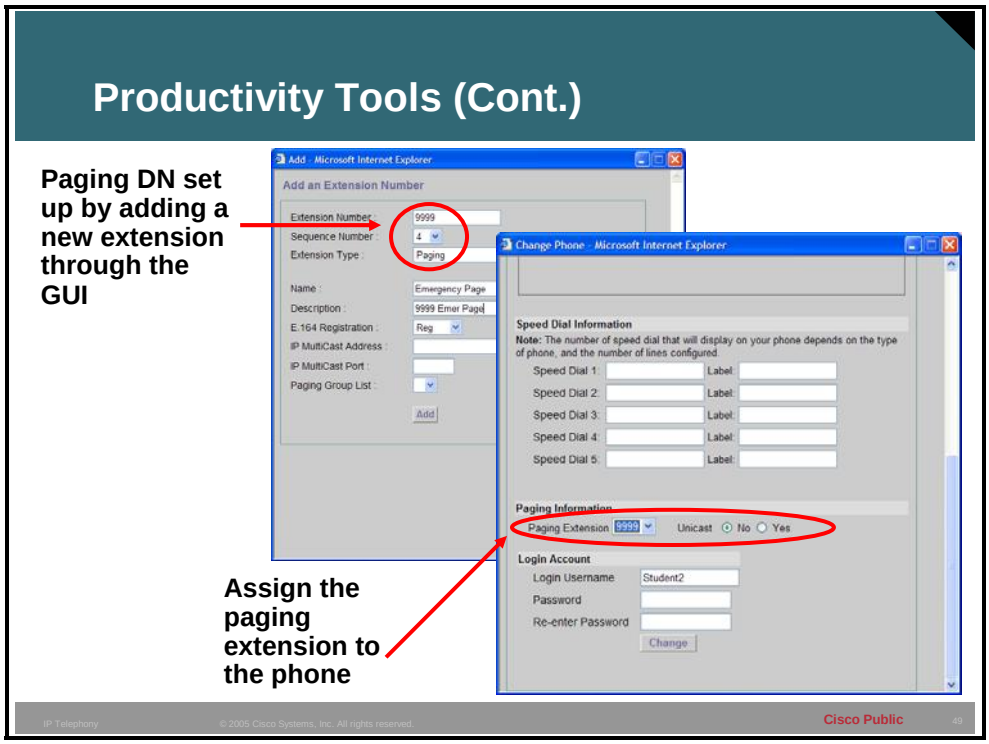
Single Paging Group

```
ephone-dn 4
 number 4444
 name Paging Shipping
 paging ip 239.0.1.20 port 2000
ephone-dn 21
 number 2121
ephone-dn 22
 number 2222
ephone 1
 mac-address 3662.0234.6ae2
 button 1:21
 paging-dn 4
ephone 2
 mac-address 9387.6738.2873
 button 1:22
 paging-dn 4
```



IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 48

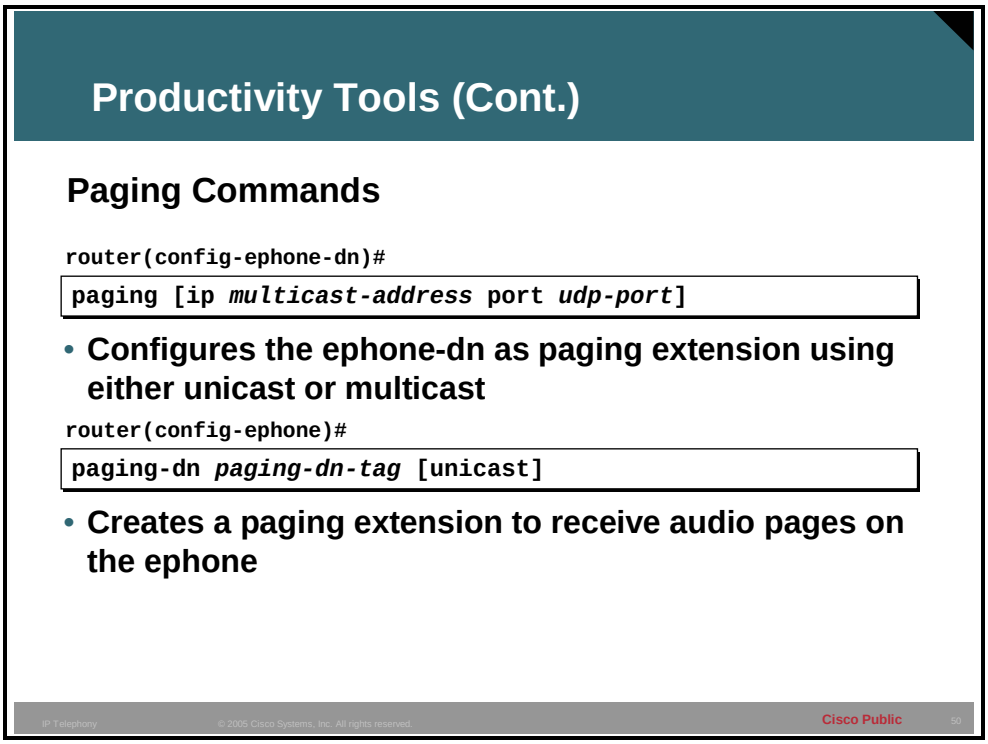
The paging feature defines an ephone-dn that sends one-way voice through a unicast or multicast mechanism to a single group of idle Cisco IP phones that have been associated with the paging ephone-dn tag. In this example, when a caller dials 4444, both ephone 1 and ephone 2 receive a page on the speaker of the IP phone.



Paging groups can be setup through the GUI by adding a new paging extension and then assigning it to one or more phones in the Cisco CME system.

Note	An IP phone can only be assigned to one paging group at a time.

 Copyright © 2005, Cisco Systems, Inc.



To configure a paging DN first create the ephone-dn with the command **ephone-dn *tag.*** Then use the **paging** command to configure the ephone-dn as a paging extension, the paging ephone-dn can then be assigned to the target ephones. The **paging** command will by default use unicast for the pages and this limits the number of target phones to 10. If the **paging ip *ip_multicast address* port *udp-port*** is used then the page can go out to more than 10 phones. The configurable range of multicast addresses is 225.0.0.0 – 239.255.255.255.

The use of multicast for paging will provide for many ephones receiving the same page without generating a separate stream of traffic for each ephone. In fact all of the IP phones in the paging group can use the same stream thereby conserving bandwidth, increasing the scalability of the page, and reducing overhead on the Cisco CME router.

Note	The network must be multicast enabled to support multicast of paging.

This assignment to one or more target ephones is done through the use of the **paging-dn** command in the ephone configuration mode for one or more ephones. The configuration of the paging ephone-dn determines whether a page will use a multicast or a unicast mechanism.

Command	Purpose
paging [ip *multicast-address* port *udp-port*] Example Unicast:Router(config-ephone-dn)#paging Example Multicast: Router(config-ephone-dn)#paging ip 239.0.1.1 port 2000	Defines an extension (ephone-dn) as a paging extension that can be called to broadcast an audio page to a set of Cisco IP phones. **ip *multicast-address*** (Optional) Uses an IP multicast address to multicast voice packets for audio paging; for example, 239.0.1.1. Note that IP phones do not support multicast at 224.x.x.x addresses. Default is that multicast is not used and IP phones are paged individually using IP unicast transmission (up to ten phones). **port *udp-port-number*** (Optional) Uses this UDP port for the multicast. Range is from 2000 to 65535. Default is 2000.
paging-dn *paging-dn-tag* [unicast] Example: Router(config-ephone)#paging-dn 77 unicast	Create a paging extension (paging-dn) to receive audio pages on a Cisco IP phone in a Cisco CME system, the unicast keyword will override the multicast configuration in the paging command

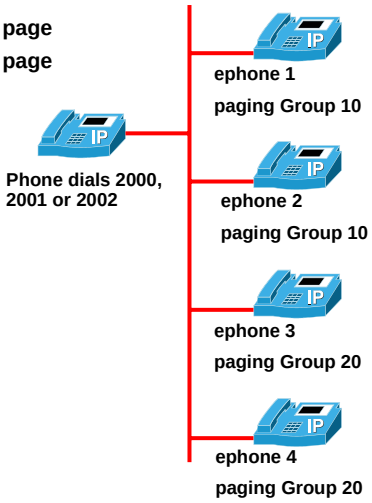
 Copyright © 2005, Cisco Systems, Inc.

Productivity Tools (Cont.)

Combined Paging Group

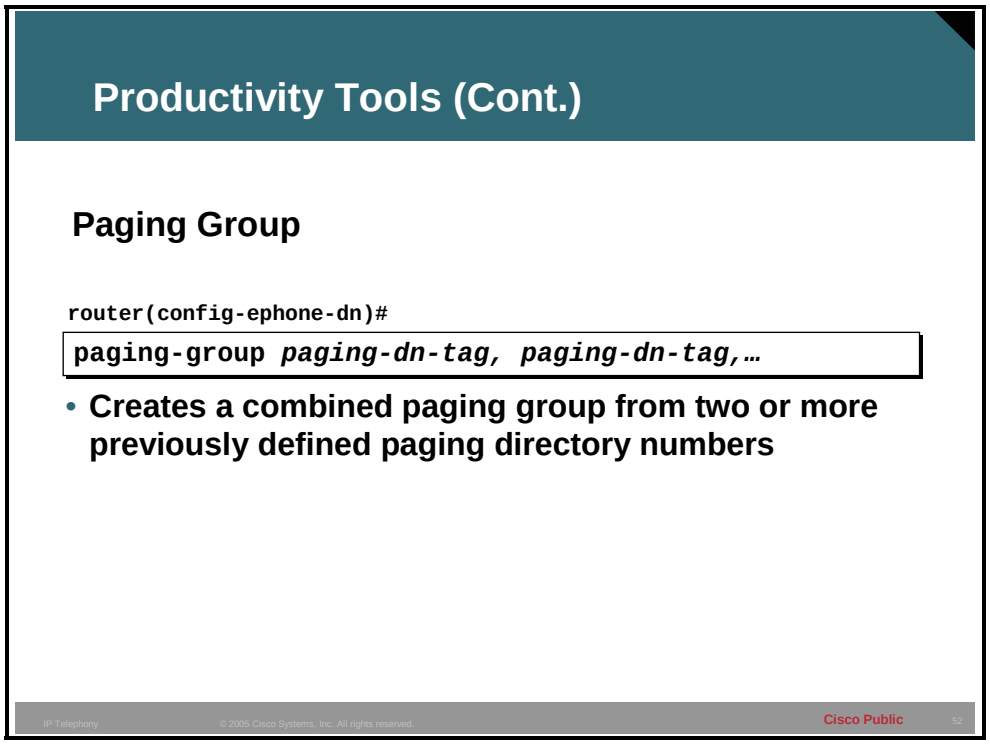
- **Phone dials 2000 and phone 1 and phone 2 get page**
- **Phone dials 2001 and phone 3 and phone 4 get page**
- **Phone dials 2002 and all 4 phones get page**

```
ephone-dn 10
 number 2000
 name Tech Support
 paging ip 239.0.1.20 port 2000
ephone-dn 20
 number 2001
 name Sales Dept
 paging ip 239.0.1.21 port 2000
ephone-dn 22
 number 2002
 paging ip 239.0.2.22 port 2000
 paging group 10,20
ephone 1
 paging-group 10
ephone 2
 paging-group 10
ephone 3
 paging-group 20
ephone 4
 paging-group 20
```



IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 51

By configuring the ability to page combined groups in addition to single groups, you provide phone users with the flexibility to page a small local paging group, like paging two phones in a company's technical support department or to page a combined set of several paging groups by paging a group that consists of technical support and sales phones.



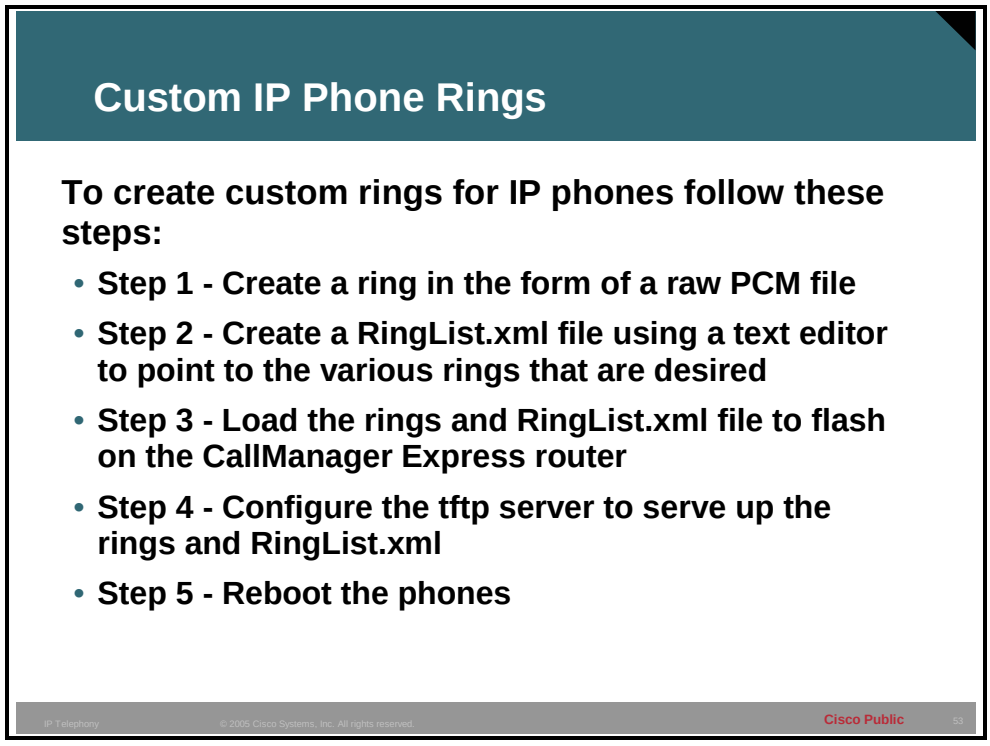
The **paging-group** command is configured under a paging ephone-dn. This allows multiple paging groups to be combined into larger groups. A common use of this is a system-wide emergency page.

Command	Purpose
Paging-group *paging-dn tag, paging-dn tag,…* Example: Router(config-ephone-dn)#paging-group 10, 20, 30, 40	Creates a combined paging group from two or more previously established paging sets.

 Copyright © 2005, Cisco Systems, Inc.

Custom IP Phone Rings

This topic describes custom IP phone rings.



One of the unique features that is enabled by using IP phones is the ability for the administrator to make custom rings that will be available for the users to select from. While this is not commonly a mission critical feature it is a commonly requested feature.

The IP Phone rings can be customized by creating your own PCM audio files and constructing a custom RingList.xml file.

Cisco IP Phones ship with two default ring types that are implemented in hardware: Chirp1 and Chirp2. Cisco IOS Telephony Service is also implemented to support custom ring sounds that are implemented in software as pulse code modulation (PCM) files. An XML file named RingList.xml that describes the ring list options available at your site is needed on the flash of Cisco CME router.

The procedure described below only applies to creating custom phone rings for the Cisco IP Phone 7940 and 7960 models.

Step 1

Create a PCM file for each custom ring (one ring per file). The PCM files for the rings must meet the following requirements for proper playback on Cisco IP Phones:

- Raw PCM (no header)
- 8000 samples per second
- 8 bits per sample
- uLaw compression

- Maximum ring size — 16080 samples
- Minimum ring size — 240 samples
- Number of samples in the ring must be evenly divisible by 240
- Ring should start and end at the zero crossing

Step 2

Use an ASCII editor to edit the RingList.xml file.

Step 3

TFTP the new PCM files and XML file to the flash of the Cisco CME router

Step 4

Set **tftp-server** command to allow access to the files

e.g. **tftp-server flash:RingList.xml**

tftp-server flash:Piano1.raw

Step 5

Reboot the IP Phones. When IP Phones are rebooted, the IP Phones will get the files and show the ring types in Ring Type Option list under Settings button.

The RingList.xml file defines an XML object that contains a list of phone ring types. Each ring type contains a pointer to the PCM file used for that ring type and the text that will be displayed on the Ring Type menu on a Cisco IP Phone for that ring. The CiscoIPPhoneRingList XML object uses the following simple tag set to describe the information:

```
<CiscoIPPhoneRingList>
<Ring>
<DisplayName/>
<FileName/>
</Ring>
</CiscoIPPhoneRingList>
```

In the above definition:

Ring contains two fields, DisplayName and FileName, that are required for each phone ring type. Up to 50 rings can be listed.

- DisplayName defines the name of the custom ring for the associated PCM file that will be displayed on the Ring Type menu of the Cisco IP Phone.
- FileName specifies the name of the PCM file for the custom ring to associate with DisplayName.

 Copyright © 2005, Cisco Systems, Inc.

- The DisplayName and FileName fields must not exceed 25 characters.

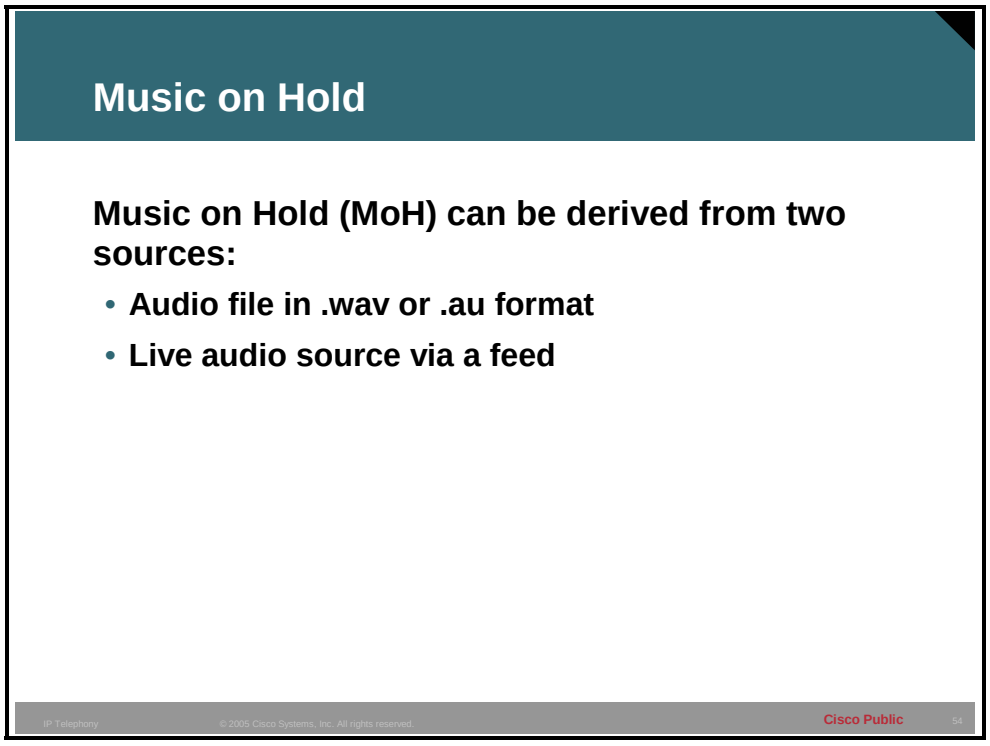
Example: Sample RingList.xml

A sample RingList.xml file that defines two phone ring types is shown below:

```
<CiscoIPPhoneRingList>
<Ring>
<DisplayName>Piano1</DisplayName>
<FileName>Piano1.raw</FileName>
</Ring>
<Ring>
<DisplayName>Chime</DisplayName>
<FileName>Chime.raw</FileName>
</Ring>
</CiscoIPPhoneRingList>
```

Music on Hold

This topic describes music on hold (MoH).



MoH is an audio stream that is played to PSTN and VoIP G.711 callers who are placed on hold by phones in a Cisco CME system. This audio stream is intended to reassure callers that they are still connected to their calls. MoH is not played to local Cisco CME phones that are on hold with other Cisco CME phones. These parties hear a periodic repeating tone instead.

The audio stream that is used for MoH can derive from one of two sources: an audio file or a live feed. If both are configured concurrently on the Cisco CME router, the router seeks the live feed first. If the live feed is found, it displaces the audio file source. If the live feed is not found or fails at any time, the router falls back to the audio file source that was specified for MoH during configuration.

If the MoH audio stream is also identified as a multicast source, the Cisco CME router additionally transmits the stream on the physical IP interfaces of the Cisco CME router that you specify during configuration, which permits external devices to have access to it.

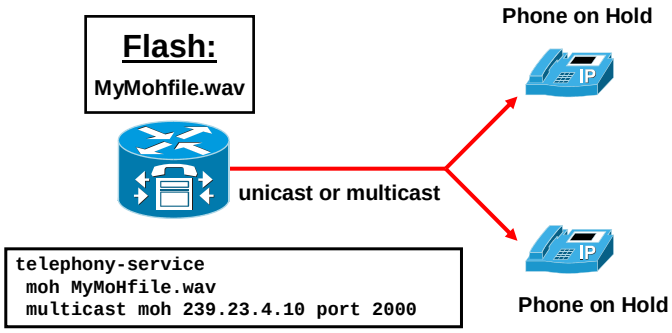
A MoH audio stream from an audio file is supplied from an .au or .wav file held in router Flash memory. A MoH audio stream from a live feed is supplied from a standard line-level audio connection that is directly connected to the router through an FXO or E&M analog voice port. The live-feed feature is typically used to connect to a CD jukebox player. Only one live MoH feed is supported per system.

Caution Use royalty-free music to avoid potential legal issues.

 Copyright © 2005, Cisco Systems, Inc.

Music on Hold (Cont.)

Configuring MoH from file



© 2005 Cisco Systems, Inc. All rights reserved.

This graphic shows a file name “MyMohfile.wav” in flash of the Cisco CME router. The file is configured to be used for music on hold by entering the **moh MyMoHfile.wav** command in telephony service mode. It is currently configured to use the multicast address of 239.23.4.10 for transmission of the music on hold.

Music on Hold (Cont.)

Configuring MoH from file

```
router(config-telephony-service)#
moh filename
```

- **Configures MoH using the file specified in flash**

```
router(config-telephony-service)#
multicast moh ip-address port port-number [route ip-address-list]
```

- **(Optional) Specifies that the MoH file should be multicast using the parameters specified**

© 2005 Cisco Systems, Inc. All rights reserved.

The **moh *filename*** command enables MoH from .au and .wav format music files. MoH is played for G.711 callers and on-net VoIP and PSTN callers who are on hold in a Cisco CME system. Local callers within a Cisco CME system hear a repeating tone while they are on hold. Audio files that are used for MoH must be copied to the Cisco CME router Flash memory. A MoH file can be in .au or .wav file format; however, the file format must contain 8-bit 8-kHz data in a-law or mu-law data format.

To replace or modify the audio file that is currently specified, you must first disable the MoH capability using the **no moh** command. The following example replaces file1 with file2:

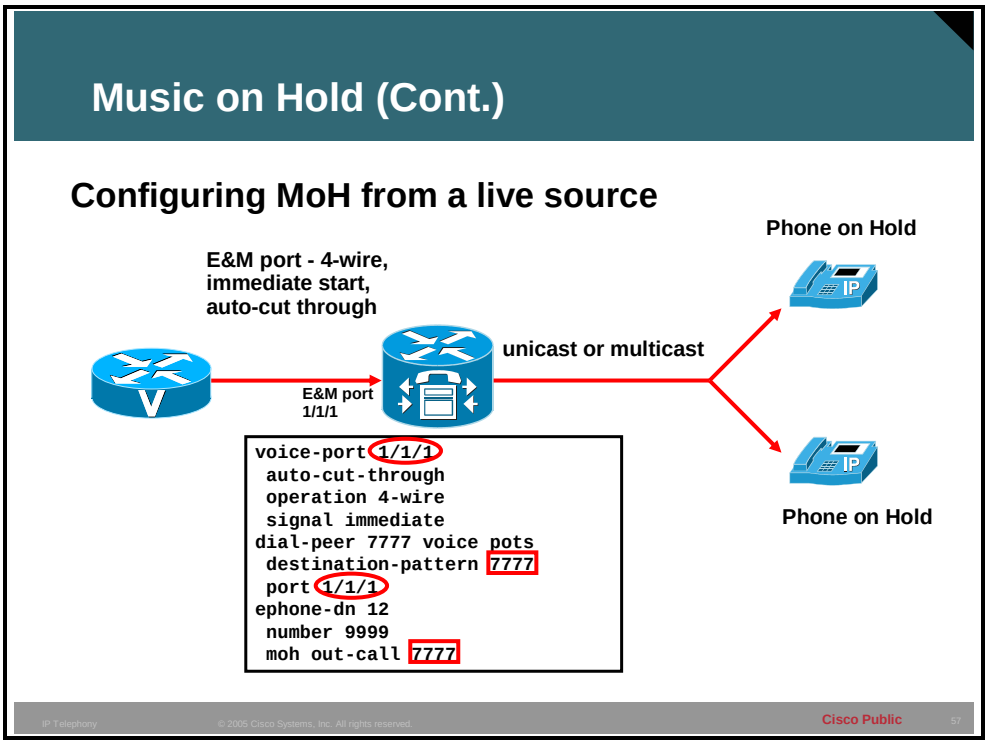
- Router(config-telephony-service)# moh file1
- Router(config-telephony-service)# no moh
- Router(config-telephony-service)# moh file2

If a second file is specified without first removing the original file, the MoH mechanism stops working and may require a router reboot to clear the problem.

Note IP phones do not support multicast at 224.x.x.x addresses.

Command	Purpose
moh *filename* Example: Router(config-telephony-service)#moh MyMoHfile.wav	Generates an audio stream from a file for music on hold (MoH) in a Cisco CME system.
multicast moh *ip address* port *port-number* [route *ip-address-list*] Example: Router(config-telephony-service)#moh 239.2.2.2 port 2000 route 10.0.0.1 11.0.0.1	Configures MoH audio stream as a multicast source in a Cisco CME system. **ip-address** Specifies the destination IP address for multicast. **port** port-number Specifies the media port for multicast. Range is from 2000 to 65535. Port 2000 is recommended because this port is already used for normal Real-Time Transport Protocol (RTP) media transmissions between IP phones and the Cisco CME router. **route ip-address-list** (Optional) Indicates specific router interfaces over which to transmit the IP multicast packets. Up to four IP addresses can be listed, each separated from the other by a space. The default is that the MoH multicast stream is automatically output on the interfaces that correspond to the address that was configured with the ip source-address command.

 Copyright © 2005, Cisco Systems, Inc.

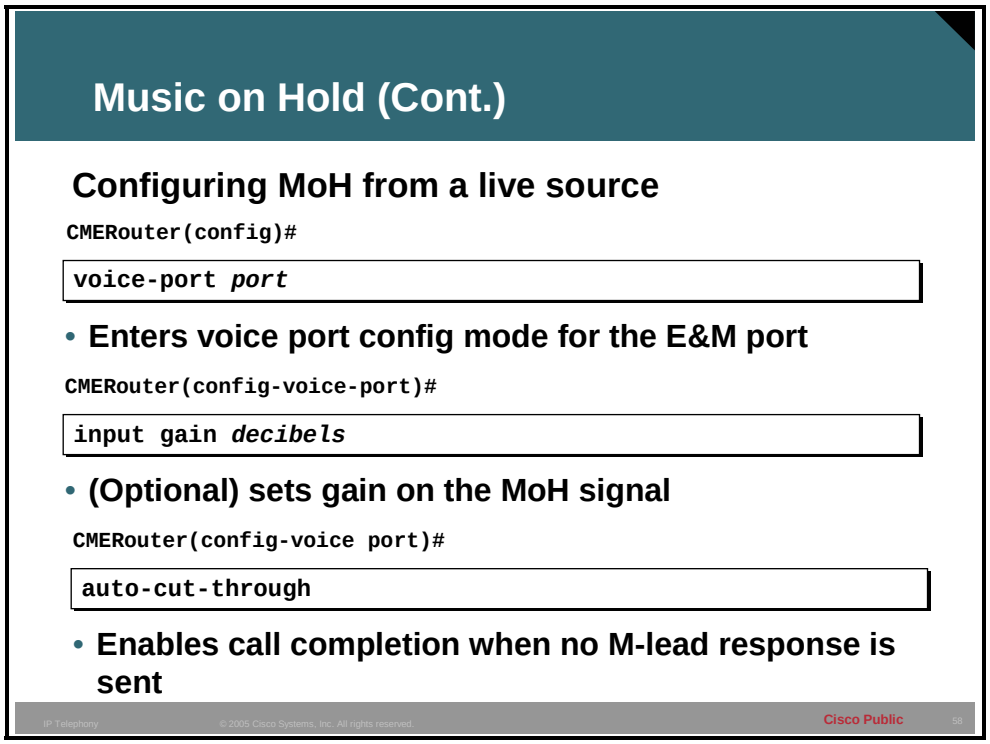


To configure MoH from a live feed, you establish a voice port and dial peer for the call and also create a “dummy” ephone-dn. The ephone-dn must have a phone or extension number assigned to it so that it can make and receive calls, but the number is never assigned to a physical phone. The recommended interface for live-feed MoH is an analog E&M port because it requires the minimum number of external components. You connect a line-level audio feed (standard audio jack) directly to pins 3 and 6 of an E&M RJ-45 connector.

The E&M Voice interface card (VIC) has a built-in audio transformer that provides appropriate electrical isolation for the external audio source. (An audio connection on an E&M port does not require loop-current.) The **signal immediate** and **auto-cut-through** commands disable E&M signaling on this voice port. A digital signal processor (DSP) on the E&M port generates a G.711 audio packet stream.

If you are using an FXO voice port for live-feed MoH instead of an E&M port, connect the MoH source to the FXO voice port. This connection requires an external adapter to supply normal telephone company (telco) battery voltage with the correct polarity to the tip and ring leads of the FXO port. The adapter must also provide transformer-based isolation between the external audio source and the tip and ring leads of the FXO port.

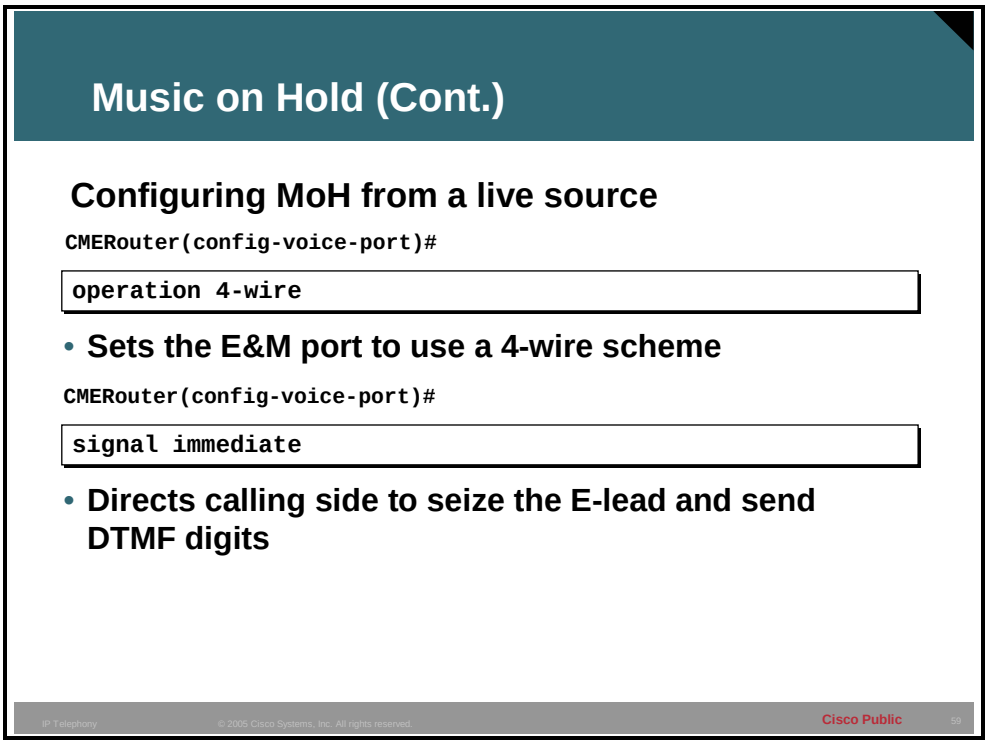
Music from a live feed is continuously fed into the MoH playout buffer instead of being read from a Flash file, so there is typically a 2-second delay. An outbound call to a MoH live-feed source is attempted (or reattempted) every 30 seconds until the connection is made by the directory number that has been configured for MoH. If the live-feed source is shut down for any reason, the Flash memory source will automatically activate. A live-feed MoH connection is established as an automatically connected voice call that is made by the Cisco CME MoH system itself or by an external source directly calling in to the live-feed MoH port.



If the MoH arrives on an analog port that FXO or E&M port will need to be configured. The command **input gain** allows the volume of the feed to be tuned up or down on either an FXO or E&M port. E&M ports require additional configuration, one of these E&M command is the **auto-cut-through** command which allows the connection to the feed to be set up even though the source of the feed will not provide a M-lead response.

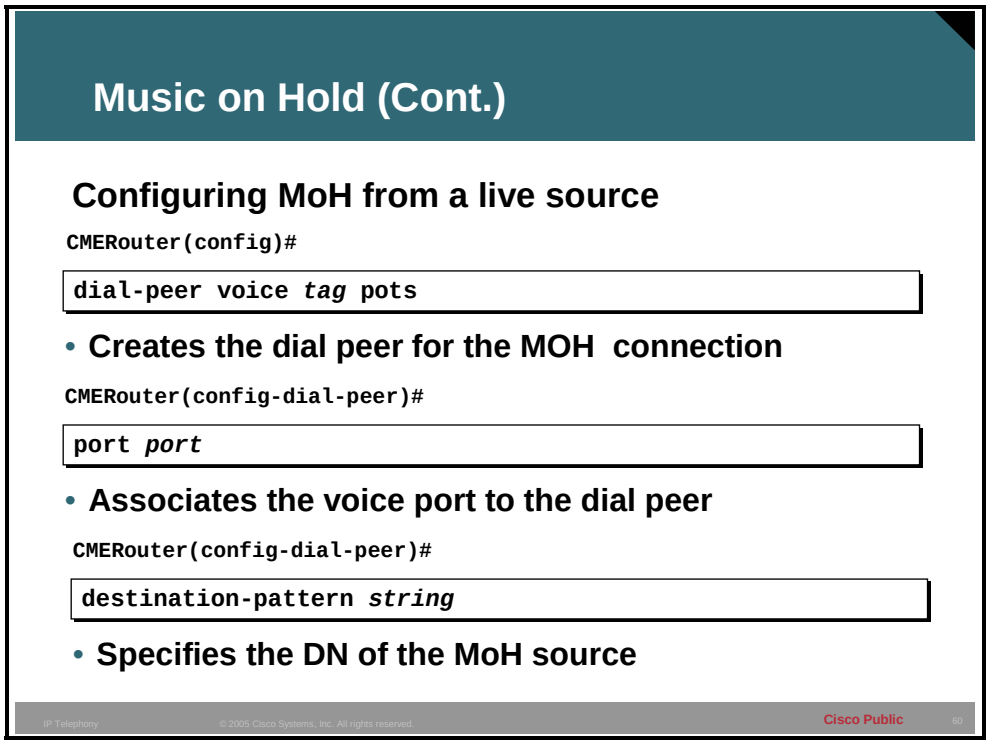
Command	Purpose
voice-port *port* Example: Router(config)#voice-port 1/0/1	Enters voice port configuration mode
Input gain *decimals* Example: Router(config-voice-port)#input gain *decimals*	Specifies, in decibels, the amount of gain to be inserted at the receiver side of the interface. Acceptable values are integers from –6 to 14.
auto-cut-through Example: Router(config-voice-port)#auto-cut-through	(E&M ports only) Enables call completion when a device does not provide an M-lead response. MoH requires that you use this command with E&M ports.

 Copyright © 2005, Cisco Systems, Inc.



The E&M port that music on hold arrives on will also need to be configured in 4-wire mode. This is done by entering the **operation 4-wire** command. E&M ports also needs to be configured to proceed with connecting the call by seizing the line and sending DTMF digits without waiting for any signal from the other side of the connection. This is done by the use of the command **signal immediate**.

Command	Purpose
operation 4-wire Example: Router(config-voice-port)#operations 4-wire	(E&M ports only) Selects the 4-wire cabling scheme. MoH requires that you specify 4-wire operation with this command for E&M ports.
signal immediate Example: Router(config-voice-port)#signal immediate	(E&M ports only) For E&M tie trunk interfaces, directs the calling side to seize a line by going off-hook on its E-lead and to send address information as DTMF digits.

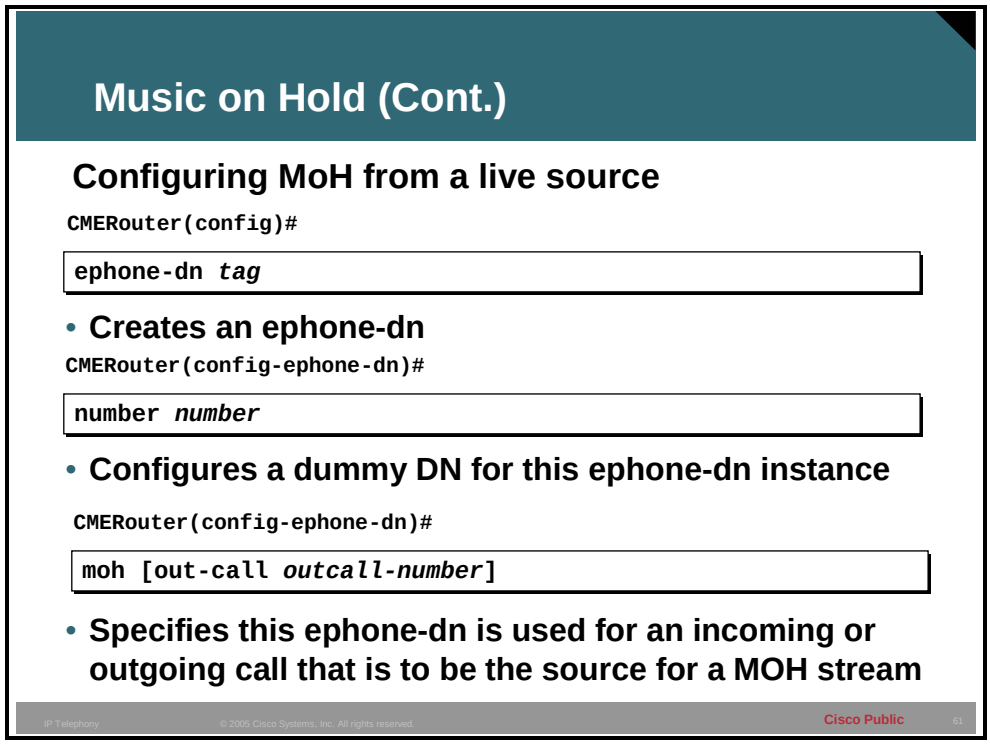


The dial peer that is used to connect the physical E&M or FXO port to the destination pattern that will be used to connect to the MoH feed is created with the **dial-peer voice *tag* pots** command. The physical voice port that will be used is associated with the **port** command and the telephone number used is defined by the **destination-pattern** command.

MoH Commands

Command	Description
dial-peer voice *tag* pots **Example:** Router(config)# dial peer voice 7777 pots	Enters dial peer configuration mode
port *port* **Example:** Router(config-dial-peer)# port 1/1/0	Associates the dial peer with a voice port
destination-pattern *string* **Example:** Router(config-dial-peer)# destination-pattern 7777	Specifies either the prefix or the full E.164 telephone number to be used for a dial peer.

 Copyright © 2005, Cisco Systems, Inc.



An ephone-dn will need to be configured with the **ephone-dn** command. Then the number of the source of the MoH feed will need to be configured with the **number** command. The ephone-dn will need the **moh** command to take the specified live-feed audio stream and uses it as MoH for a Cisco CME system. The connection for the live-feed audio stream is established as an automatically connected voice call. If the **out-call** keyword is used, the type of connection can include VoIP calls if voice activity detection (VAD) is disabled. The typical operation is for the MoH ephone-dn to establish a call to a local router E&M port.

If the out-call keyword is used, an outbound call to the MoH live-feed source is attempted (or reattempted) every 30 seconds until the call is connected to the ephone-dn (extension) that has been configured for MoH. Note that this ephone-dn is not associated with any physical phone.

If the MoH (ephone-dn) command is used without any keywords or arguments, the ephone-dn will accept an incoming call and use the audio stream from the call as the source for the MoH stream, displacing any audio stream that is available from a Flash file. To accept an incoming call, the ephone-dn must have an extension or phone number configured for it. A typical usage would be for an external H.323-based server device to call the ephone-dn to deliver an audio stream to the Cisco CME system. Normally, only a single ephone-dn would be configured like this. If there is more than one ephone configured to accept incoming calls for MoH, the first ephone-dn that is successfully connected to a call (incoming or outgoing) is the MoH source for the system.

MoH Commands

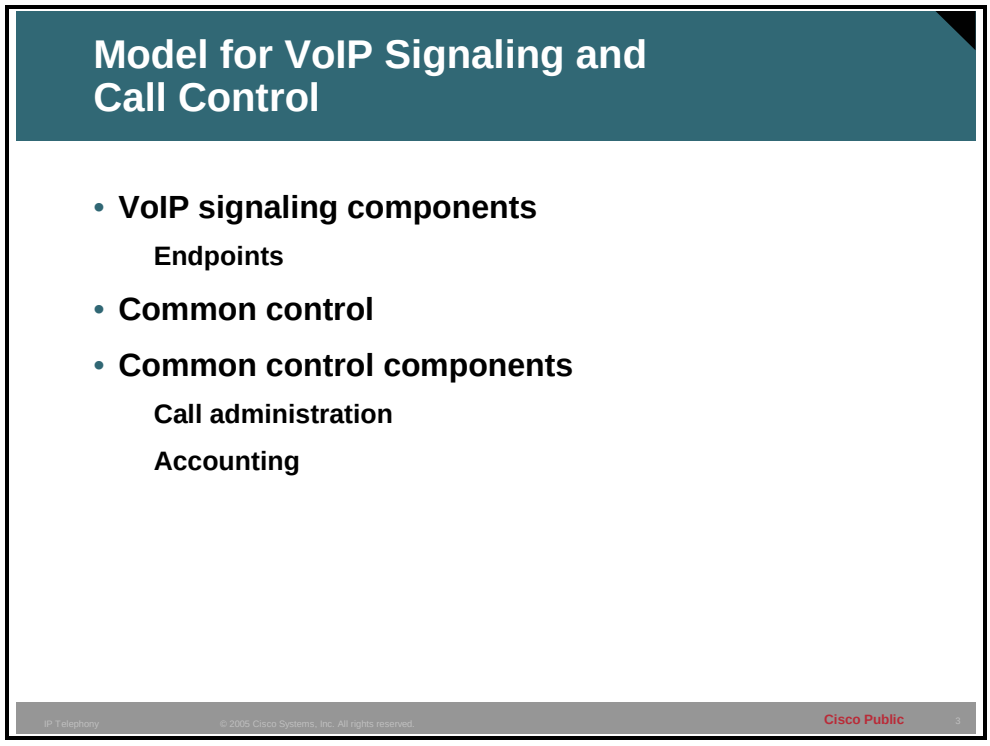
Command	Description
ephone-dn *dn-tag* **Example:** Router(config)# ephone-dn 55	Enters ephone-dn configuration mode. • *dn-tag*—Unique sequence number that identifies this ephone-dn during configuration tasks. Range is from 1 to 288.
number *number* **Example:** Router(config-ephone-dn)# number 5555	Configures a valid extension number for this ephone-dn instance. This number is not assigned to any phone; it is only used to make and receive calls that contain an audio stream to be used for MoH. • *number*—String of up to 16 digits that represents a telephone or extension number to be associated with this ephone-dn.
moh [out-call *outcall-number*] **Example:** Router(config-ephone-dn)# moh out-call 7777	Specifies that this ephone-dn is to be used for an incoming or outgoing call that is to be the source for an MoH stream. If this command is used without the **out-call** keyword, the MoH stream is received from an incoming call. • **out-call** *outcall-number*—(Optional) Indicates that the router is calling out for a live feed that is to be used for MoH and specifies the number to be called. Forces a connection to the local router voice port that was specified

 Copyright © 2005, Cisco Systems, Inc.

Need for Signaling and Call Control

VoIP Signaling

In a traditional voice network, call establishment, progress, and termination are managed by interpreting and propagating signals. Transporting voice over an IP internetwork creates the need for mechanisms to support signaling over the IP component of the end-to-end voice path. This topic introduces the components and services provided by VoIP signaling.



In the traditional telephone network, a voice call consists of two paths: an audio path carrying the voice and a signaling path carrying administrative information such as call setup, teardown messages, call status, and call-progress signals. ISDN D channel signaling and Common Channel Signaling System 7 (CCSS7) or Signaling System 7 (SS7) are two examples of signaling systems that are used in traditional telephony.

By introducing VoIP into the call path, the end-to-end path involves at least one call leg that uses an IP internetwork. As in a traditional voice call, support for this VoIP call leg requires two paths: a protocol stack that includes RTP, which provides the audio call leg, and one or more call control models that provide the signaling path.

A VoIP signaling and call control environment model includes endpoints and optional common control components, as follows:

- **Endpoints:** Endpoints are typically simple, single-user devices, such as terminals, that support either a voice process (for example, the Cisco IP Phone application) or a gateway. In either case, the endpoint must be able to participate in signaling with other VoIP endpoints—directly or indirectly—through common control components. The endpoints must also be able to manipulate the audio that is in the audio path. This may involve performing analog-to-digital conversion or converting the format to digital voice so that it takes advantage of compression technology.

  Gateways provide physical or logical interfaces to the traditional telephone network. A gateway that is connected digitally to a service provider central office (CO) switch is an example of a gateway providing a physical interface. A gateway that provides access to an interactive response dialog application is an example of a gateway providing a logical interface.

- **Common control:** In some call control models, the common control component is not defined; in others, it is employed optionally. Common control components provide call administration and accounting. These components provide a variety of services to support call establishment, including the following:

  — Call status

  — Address registration and resolution

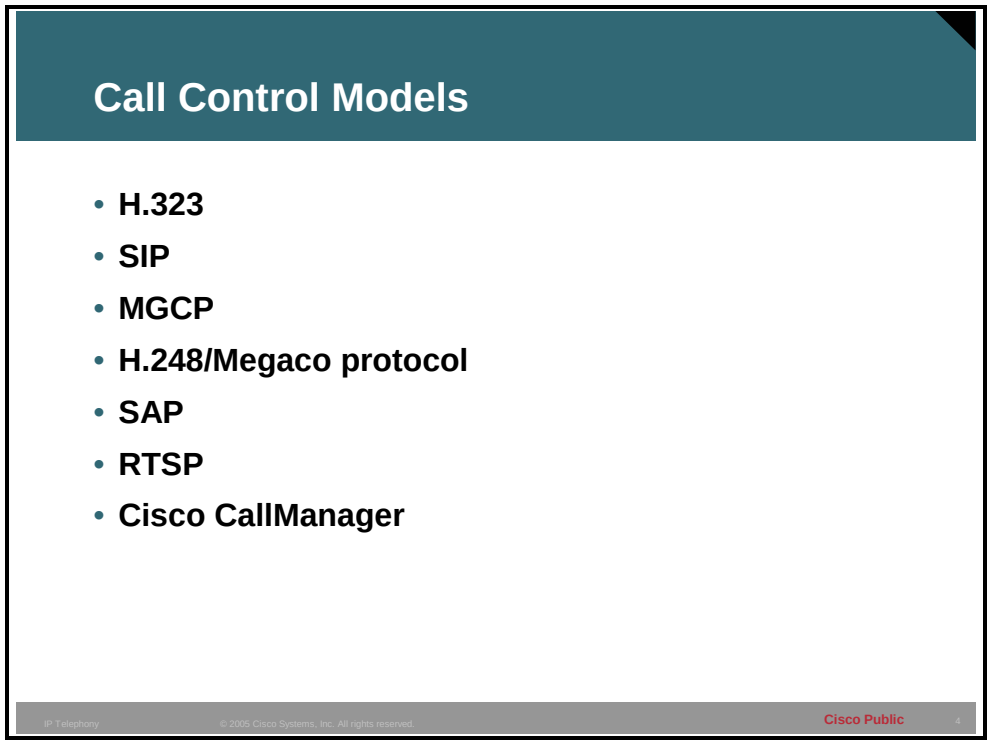
  — Admission control

Typically, the services of the common control components are implemented as applications. These services are colocated in a single physical device, or distributed over several physical devices with standalone endpoints and gateways.

 Copyright © 2005, Cisco Systems, Inc.

Call Control Models

This topic describes several call control models and their corresponding protocols.

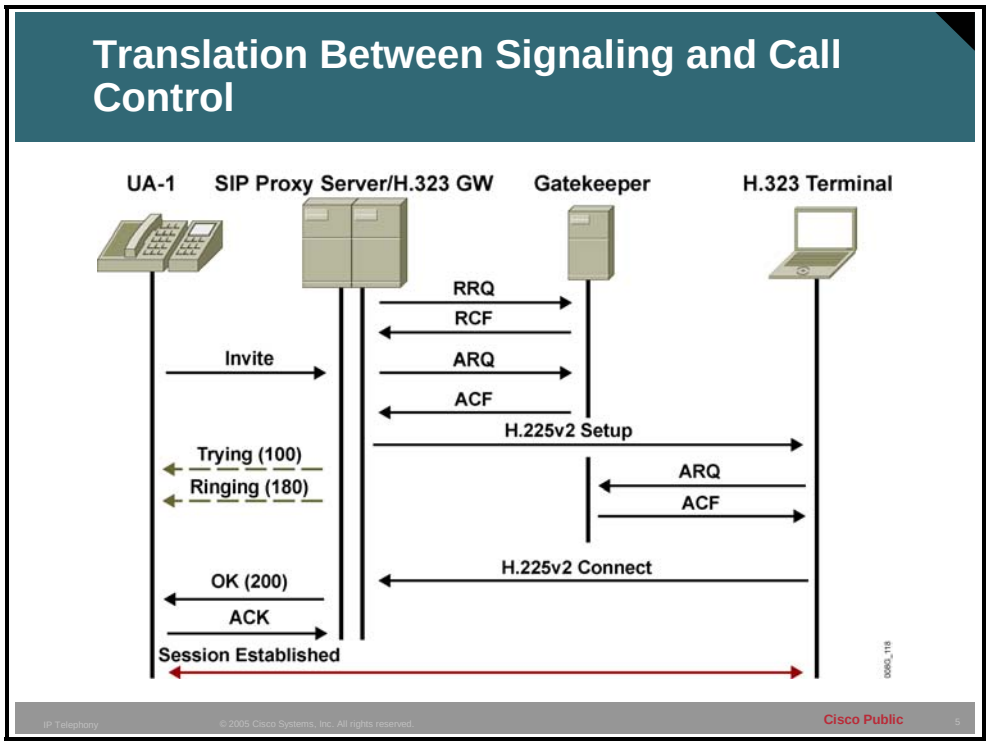


The following call control models and their corresponding protocols exist or are in development:

- **H.323:** International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Recommendation H.323 describes the architecture to support multimedia communications over networks without quality of service (QoS) guarantees. Originally intended for LANs, H.323 has been adapted for IP.
- **SIP:** SIP is an Internet Engineering Task Force (IETF) RFC 3261 call control model for creating, modifying, and terminating multimedia sessions or calls.
- **MGCP:** MGCP (IETF RFC 2705) defines a call control model that controls VoIP gateways from an external call control element or call agent.
- **H.248/Megaco protocol:** The Megaco protocol is used in environments in which a media gateway consists of distributed subcomponents, and communication is required between the gateway subcomponents. The Megaco protocol is a joint effort of IETF (RFC 3015) and ITU-T (Recommendation H.248).
- **Session Announcement Protocol (SAP):** SAP (IETF RFC 2974) describes a multicast mechanism for advertising the session characteristics of a multimedia session, including audio and video.
- **Real Time Streaming Protocol (RTSP):** RTSP (IETF RFC 2326) describes a model for controlled, on-demand delivery of real-time audio and video.
- **Cisco CallManager (“Skinny”):** Cisco CallManager is a proprietary Cisco Systems implementation of a call control environment that provides basic call processing, signaling, and connection services to configured devices, such as IP telephones, VoIP gateways, and software applications.

Translation Between Signaling and Call Control Models

When VoIP endpoints support different call control procedures, the calls between the endpoints require cooperation between the originating and terminating procedures. This topic identifies the need for interworking or translation between call control models.



In the traditional telephone network, the individual call legs contributing to an end-to-end call often involve different signaling systems and procedures. In the graphic, an IP Phone is communicating with its SIP proxy server using the SIP protocol. However, it is also attempting to reach an H.323 endpoint. Because the two VoIP protocols are different, a translation is necessary at the SIP proxy server (namely, an H.323 gateway) to allow the two telephony endpoints to establish a connection.

Example: Call Control Translation

A call between a residential user and an office worker likely involves a signaling system that is unique to the various call legs that exist between the originator and the destination. In this scenario, the sequence of signaling systems includes the following:

- Analog signaling (Foreign Exchange Station [FXS] or Foreign Exchange Office [FXO] loop start) to the CO
- CCSS7 between the COs
- ISDN PRI signaling to the PBX
- Proprietary signaling to the desktop telephone

 Copyright © 2005, Cisco Systems, Inc.

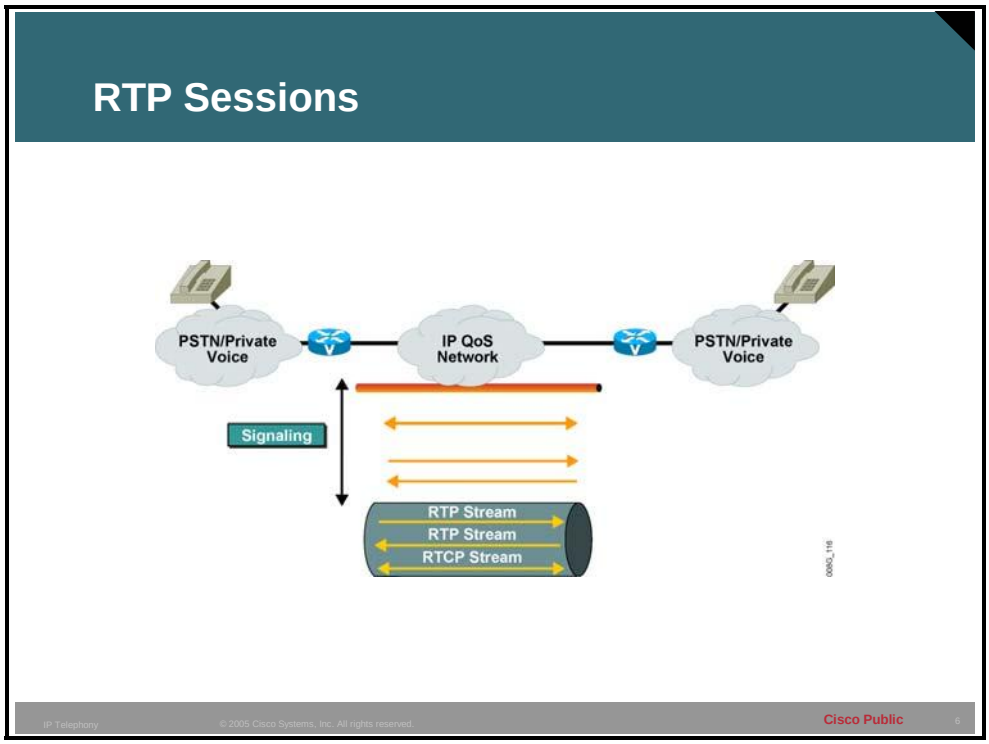
When part of the path is replaced with an IP internetwork, the audio path between the IP endpoints is provided by RTP, and the call control mechanism is based on a call control protocol, such as SIP, H.323, or MGCP.

But what if different call control models represent the endpoints? What if, for example, the originating endpoint uses H.323 and the destination is managed as an SIP endpoint?

To complete calls across the IP internetwork, a call control gateway that recognizes the procedures of *both* call control models is required. In particular, the translating gateway interprets the call setup procedure on the originating side and translates the request to the setup procedure on the destination side. Ideally, this translation is transparent to the endpoints that are involved and results in a single endpoint-to-endpoint audio relationship.

Call Setup

A fundamental objective of VoIP call control is to initiate communication between VoIP endpoints. This topic discusses the role of call control in establishing RTP sessions and negotiating features during the call setup procedure.

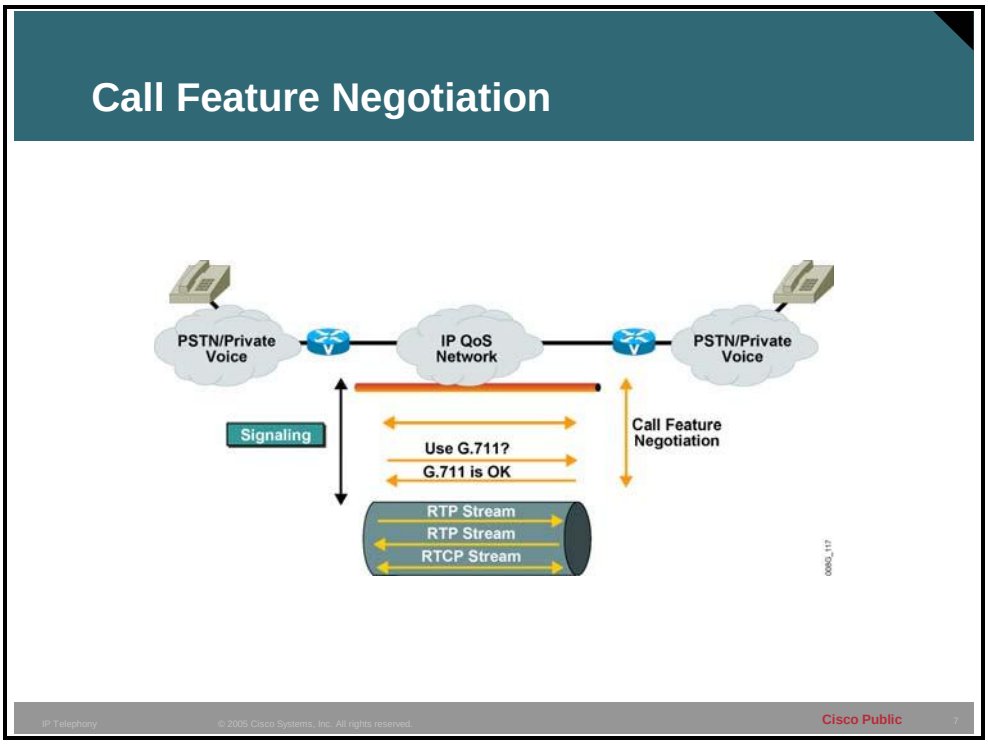


An audio path of a VoIP call leg is dependent on the creation of RTP sessions. These RTP sessions transport voice unidirectionally, so that bidirectional voice uses two RTP sessions. (In principle, if voice is needed in one direction only, as in the case of a recorded announcement or voice mail, only one RTP session is required.) The figure shows RTP sessions being created during call setup.

To create RTP sessions, each endpoint must recognize the IP address and User Datagram Protocol (UDP) port number of its peer. In a limited implementation of VoIP, these values are preprogrammed. However, to be truly scalable, the addresses and port numbers must be recognized dynamically and on demand.

During call setup, call control procedures exchange the IP address and UDP port numbers for the RTP sessions.

 Copyright © 2005, Cisco Systems, Inc.



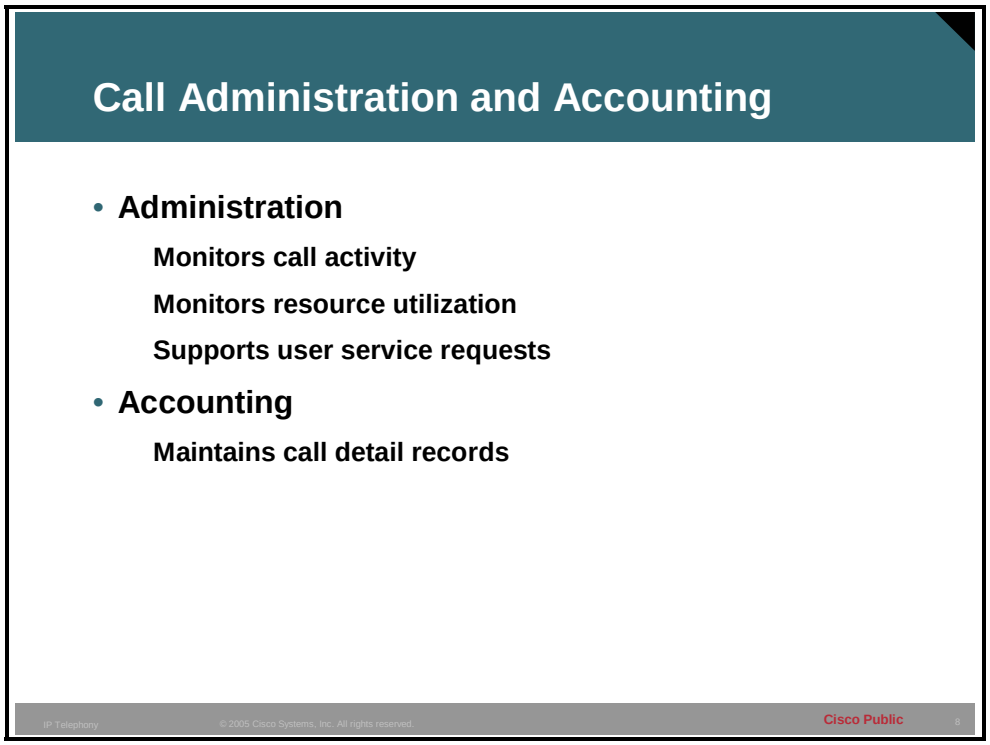
Creating the RTP sessions is not the only task of call control during call setup. The endpoints need to establish a bilateral agreement in which the communicating parties discover acceptable call parameters and then agree on the operating parameters of the call. When agreement is not possible, the call is not completed and is dropped.

Following are some examples of call parameters:

- **Coder-decoder (codec):** Each endpoint must share a common format for the voice, or at least must recognize the opposite endpoint choice for voice encoding. This is an example of a mandatory agreement. Not finding a common format is analogous to calling a foreign land and discovering that you are unable to carry on a conversation because the other party speaks a different language.
- **Receive/transmit:** Based on the application, the voice is one-way or two-way. Some endpoints do not meet the requirement for the session because they are designed to handle receive-only or transmit-only traffic when the call requests two-way communication.
- **Multipoint conferences:** The types of conferences and parameters to join.
- **Media type:** Audio, video, or data.
- **Bit rate:** Throughput requirements.

Call Administration and Accounting

Call control procedures typically provide support for call administration and accounting. This topic discusses administration and accounting capabilities of call control.



Call administration and accounting functions provide optional services for the improved operation, administration, and maintenance of a VoIP environment.

Accounting makes use of the historical information that is usually formatted as call detail records. Call detail records are useful for cost allocation, and for determining call distribution and service grade for capacity-planning purposes.

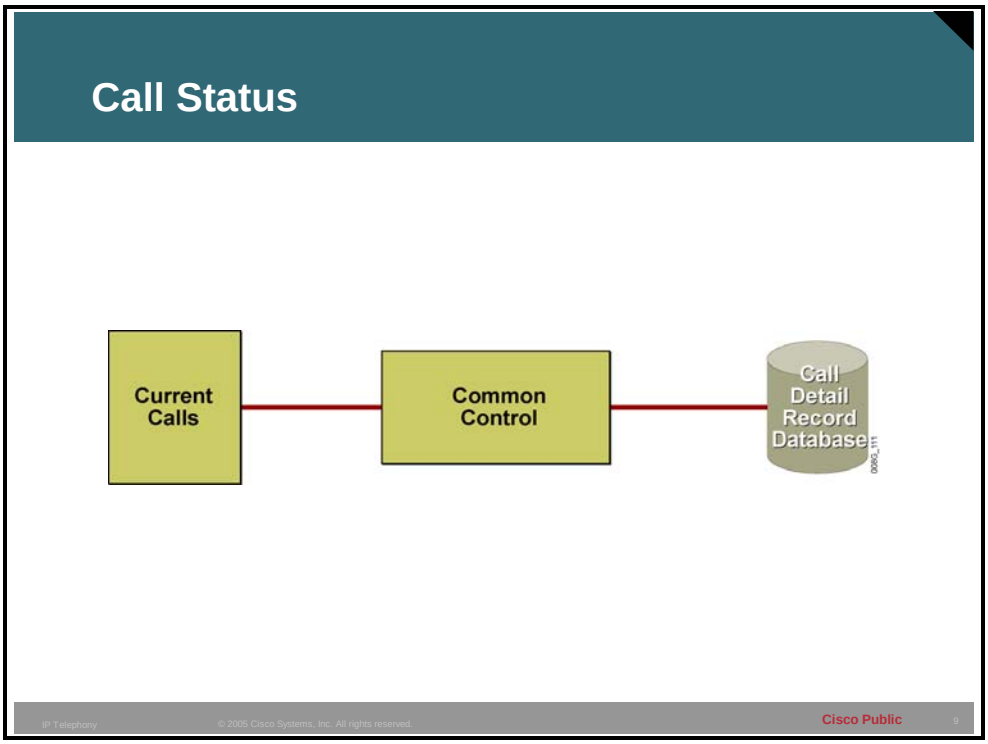
Call administration includes the following capabilities:

- **Call status:** Monitoring calls in real time
- **Address management:** Supporting users with services such as address resolution
- **Admission control:** Ensuring that resources are being used effectively

 Copyright © 2005, Cisco Systems, Inc.

Call Status and Call Detail Records

Several call control protocols offer dynamic access to the status of calls within the VoIP network. This topic discusses the benefits of maintaining call status information and describes where and how call status is used.



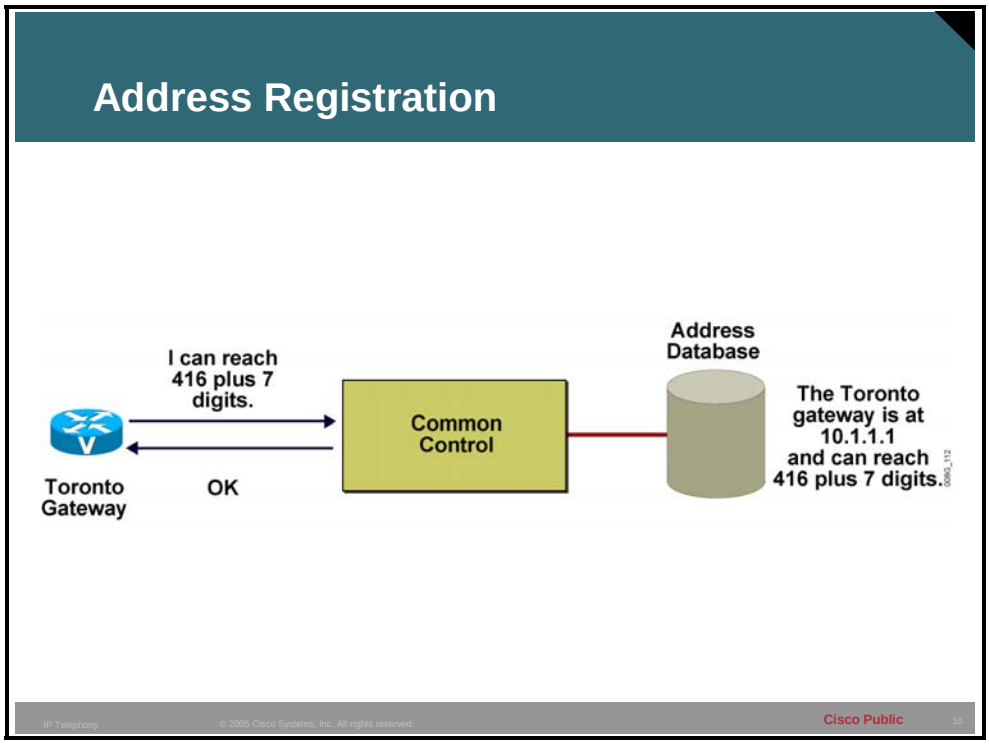
Several of the responsibilities that are assigned to call administration and accounting are dependent on access to current call status information or records of changes in the call status. Call status has both historical and instantaneous (real-time) benefits. Call detail records have consequential benefits in terms of distributing costs and planning capacity.

Call status provides an instantaneous view of the calls that are in progress. This view assists other processes (for example, bandwidth management) or assists an administrator with troubleshooting or user support.

Call detail records include information about a call start time, duration, origin, destination, and other statistics that may be useful for a variety of purposes. This data is collected as a function of call status.

Address Management

As an aspect of call administration, call control maintains a database of endpoints and their identifiers. This topic discusses how endpoints register their addresses and how these addresses are resolved to IP addresses.



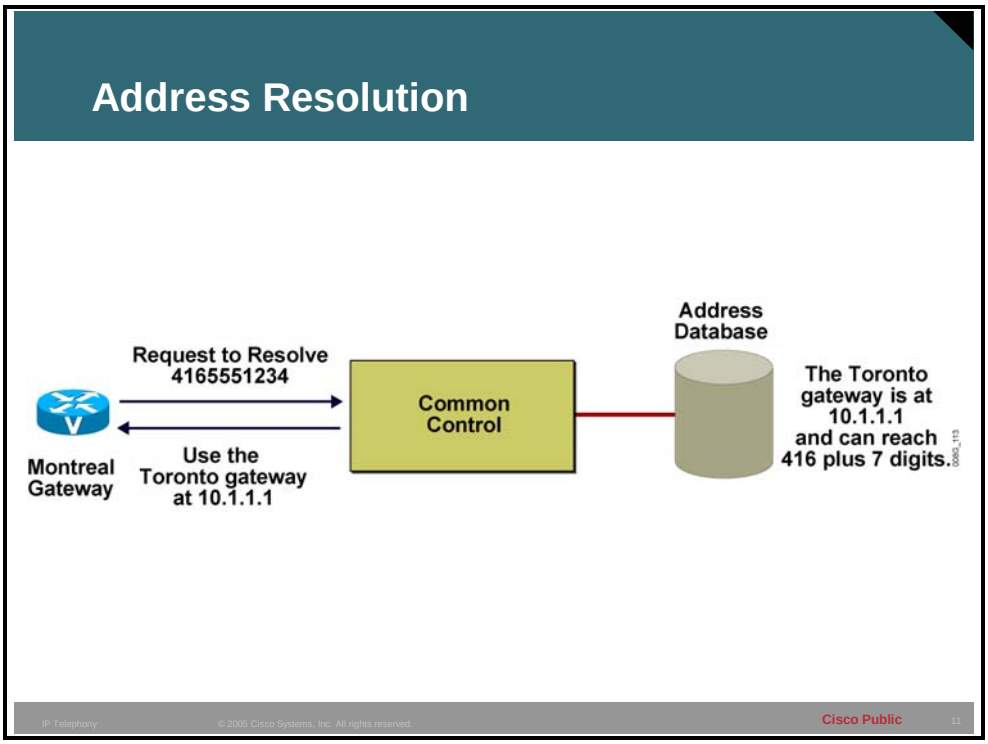
When an endpoint registers with a call control component, it supplies its telephone address or addresses and, if it is a gateway, the addresses of the destinations it can reach. The endpoint provides other information relating to its capabilities. Multiple destinations that are reachable through a gateway are usually represented by a prefix. The use of a prefix allows call control to create a database that associates a telephony-type address, for example, with its corresponding IP address.

In the traditional telephone network, the address of a station is limited to the keys available on a dual-tone multifrequency (DTMF) keypad. In VoIP, an address takes on one of several other formats as well; for example, the address can be a host name or a URL.

Example: Address Registration

The figure illustrates the Toronto gateway registering its accessibility information. In this example, the gateway informs the common control component that it can reach all telephone numbers in the 416 area. This information is deposited into a database for future reference.

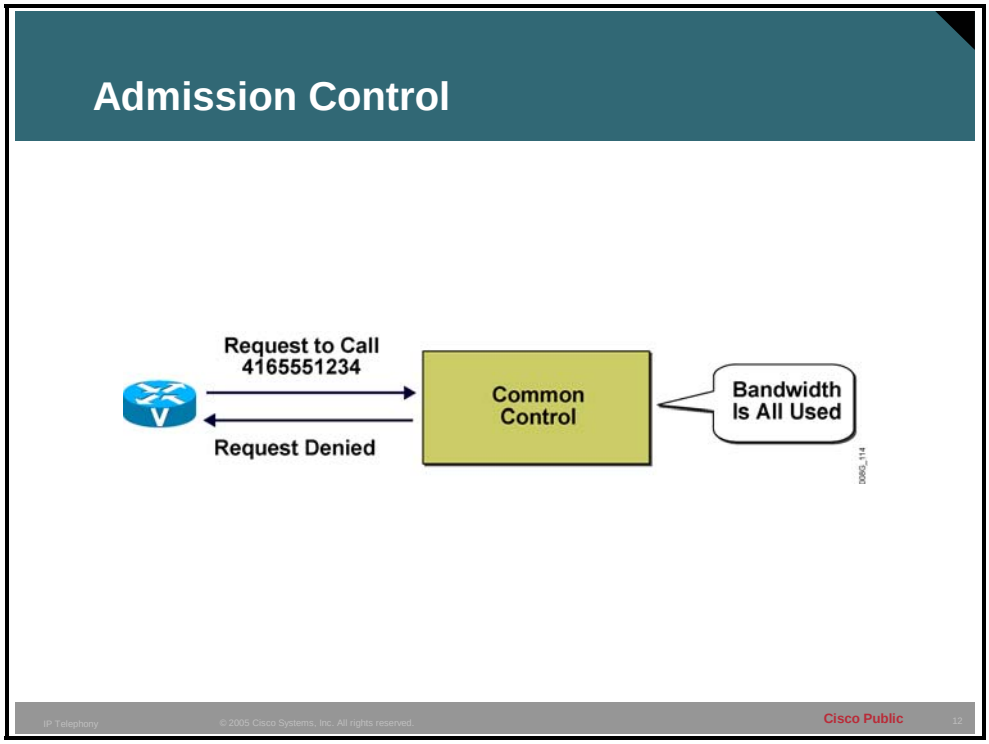
 Copyright © 2005, Cisco Systems, Inc.



After an address is registered, it can be discovered through address resolution. Address resolution translates a multimedia user address to an IP address so that the endpoints can communicate with each other to establish a control relationship and create an audio path.

Admission Control

This topic discusses how common control and bandwidth management restrict access to the network.



Admission control has at least two aspects: authorization and bandwidth management.

Access to a network should not imply permission to use the resources of the network. Common control limits access to the resources by checking the intentions and credentials of users before authorizing them to proceed.

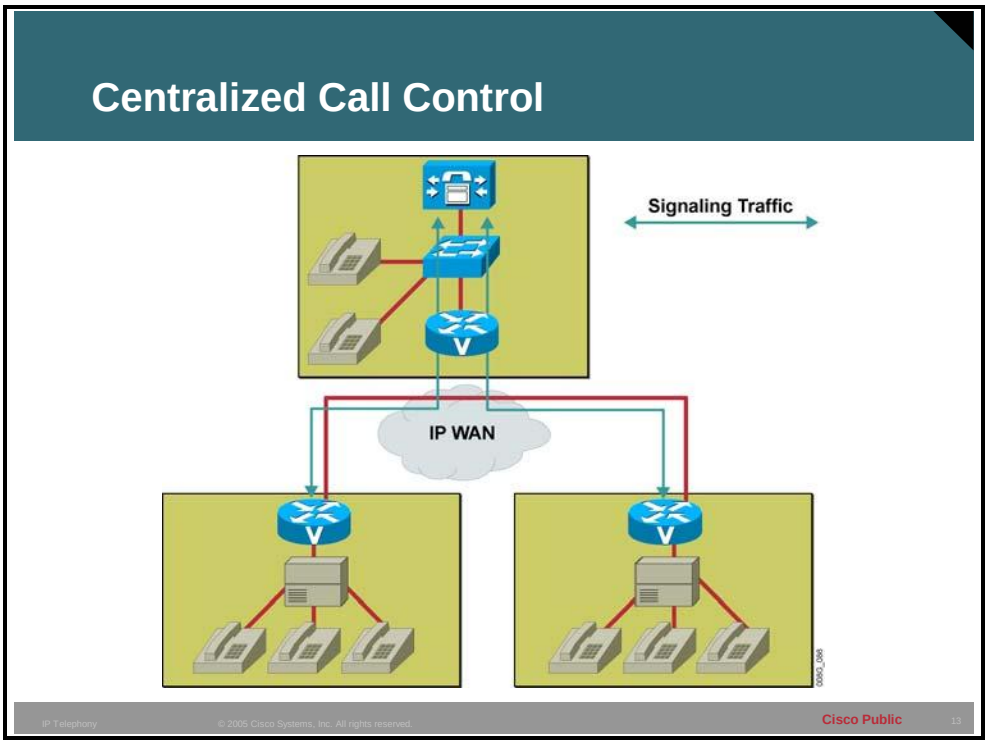
Bandwidth is a finite resource. Appropriate bandwidth management is essential to maintaining voice quality. Allowing too many voice calls over an IP internetwork results in loss of quality for both new and existing voice calls.

To avoid degrading voice quality, a call control model establishes a bandwidth budget. By using data available from call status, the bandwidth management and call admission control functions monitor current bandwidth consumption. Calls may proceed up to the budgeted level, but are refused when the budget has reached its limit. This process is illustrated in the figure.

 Copyright © 2005, Cisco Systems, Inc.

Centralized Call Control

This topic describes the function of endpoints in a centralized call control model.



The level of “intelligence” associated with an endpoint classifies call control models. In centralized call control, the intelligence in the network is associated with one or several controllers. Endpoints provide physical interconnection to the telephone network. However, endpoints still require the central controller to dictate when and how to use their interconnect capability. For example, the central controller may require the endpoint to provide dial tone to a telephone and alert the controller when a telephone goes off hook. The endpoint does not make decisions autonomously.

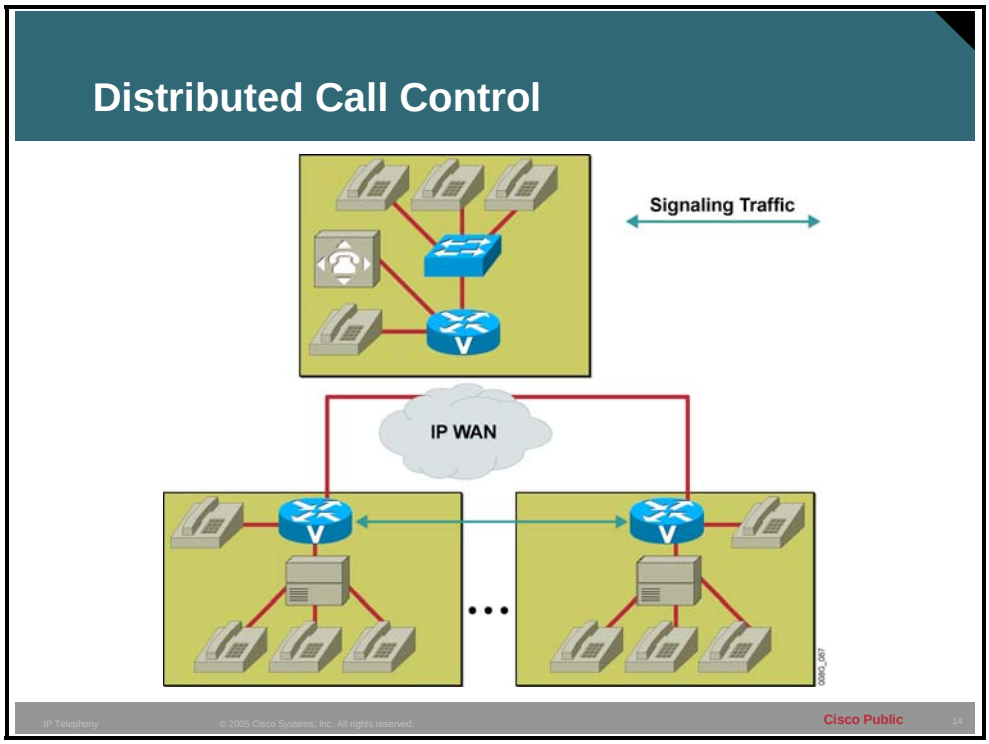
Example: Centralized Call Control

The figure illustrates two gateways interacting with a centralized call control component for call setup and management. Notice that the media path is between the two gateways.

A centralized call control model is similar to the mainframe model of computing and uses centralized common control concepts that are found in circuit-switching solutions.

Distributed Call Control

This topic describes the functions of the endpoints in a distributed call control model.



Endpoints in a distributed call control model have sufficient intelligence to autonomously manage the telephone interface and initiate VoIP call setup. Although the endpoint in a distributed model often depends on shared common control components for scalability, it possesses enough intelligence to operate independently from the common control components. If a common control component fails, an endpoint can use its own capabilities and resources to make routing or rerouting decisions.

Example: Distributed Call Control

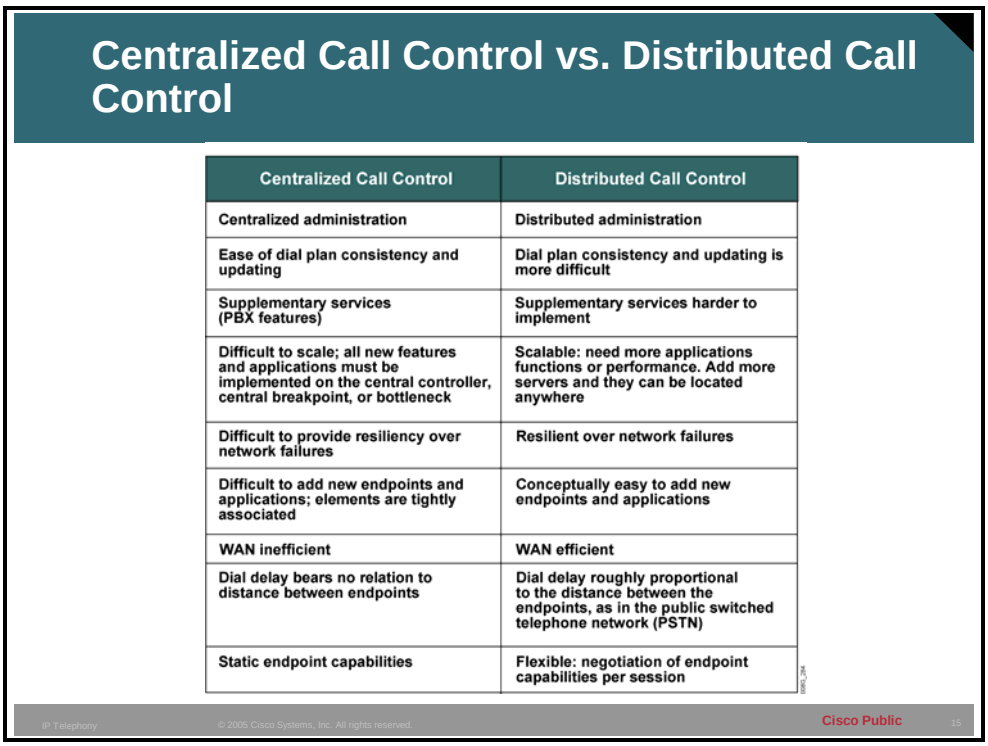
In the figure, the two gateways have established a call control path and a media path between themselves, without the assistance of a centralized call control component.

A distributed call model is analogous to a desktop computing model.

 Copyright © 2005, Cisco Systems, Inc.

Centralized Call Control vs. Distributed Call Control

This topic compares the advantages and disadvantages of the centralized and distributed call control models.



The figure shows a comparison of the centralized and distributed call control models. Both models have advantages and disadvantages. Features that are considered advantages of one type of call control model are disadvantages of the other type. The main differences between the two models are in the following areas:

- **Configuration:** The centralized call control model provides superior control of the configuration and maintenance of the dial plan and endpoint database. It simplifies the introduction of new features and supplementary services and provides a convenient location for the collection and dissemination of call detail records. The distributed model requires distributed administration of the configuration and management of endpoints, thus complicating the administration of a dial plan. Although distributed call control simplifies the deployment of additional endpoints, new features and supplementary services are difficult to implement.
- **Security:** Centralized call control requires that endpoints be known to a central authority, which avoids (or at least reduces) security concerns. The autonomy of endpoints in the distributed model elevates security concerns.
- **Reliability:** The centralized model is vulnerable because of its single point-of-failure and contention. It places high demands on the availability of the underlying data network, necessitating a fault-tolerant WAN design. The distributed call control model minimizes the dependence on shared common control components and network resources, thus reducing vulnerability.

- **Efficiency:** Centralized call control fails to take full advantage of computer-based technology that resides in the endpoints. It also consumes bandwidth through the interaction of the call agent and its endpoints. Distributed call control takes advantage of the inherent computer-based technology in endpoints.

Example: Comparing Centralized and Distributed

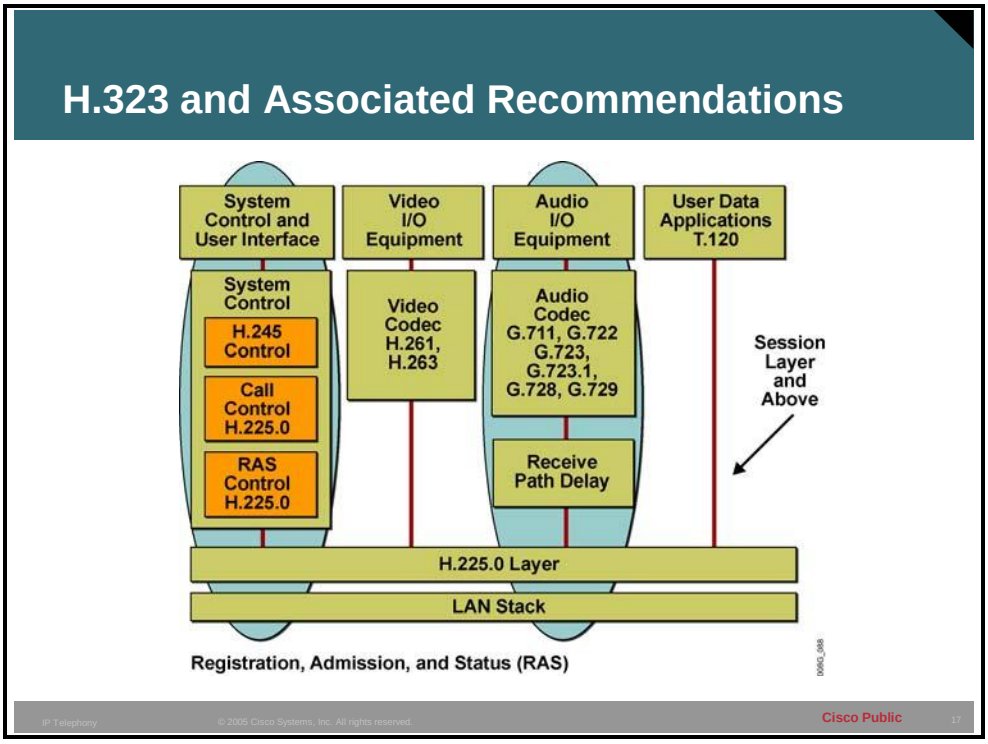
Because the centralized model increases vulnerability, it mandates the implementation of survivability and load management strategies that involve the replication of the central components. Few implementations of call control are totally distributed. For example, although H.323 and SIP operate in a purely distributed mode, for scalability reasons, both are most often deployed with common control components that give endpoints many of the advantages of a centralized call control environment. Unfortunately, these implementations also inherit many of the disadvantages of centralized call control.

 Copyright © 2005, Cisco Systems, Inc.

Configuring H.323

H.323 and Associated Recommendations

This topic describes H.323 and its protocols and explains how H.323 is used in the IP internetwork environment.



Recommendation H.323 describes an infrastructure of terminals, common control components, services, and protocols that are used for multimedia (voice, video, and data) communications. The figure illustrates the elements of an H.323 terminal and highlights the protocol infrastructure of an H.323 endpoint.

H.323 was originally created to provide a mechanism for transporting multimedia applications over LANs. Although numerous vendors still use H.323 for videoconferencing applications, it has rapidly evolved to address the growing needs of VoIP networks. H.323 is currently the most widely used VoIP signaling and call control protocol, with international and domestic carriers relying on it to handle billions of minutes of use each year.

H.323 is considered an “umbrella protocol” because it defines all aspects of call transmission, from call establishment to capabilities exchange to network resource availability. H.323 defines the following protocols:

- H.245 for capabilities exchange
- H.225.0 for call setup
- H.225.0 for registration, admission, and status (RAS) control for call routing

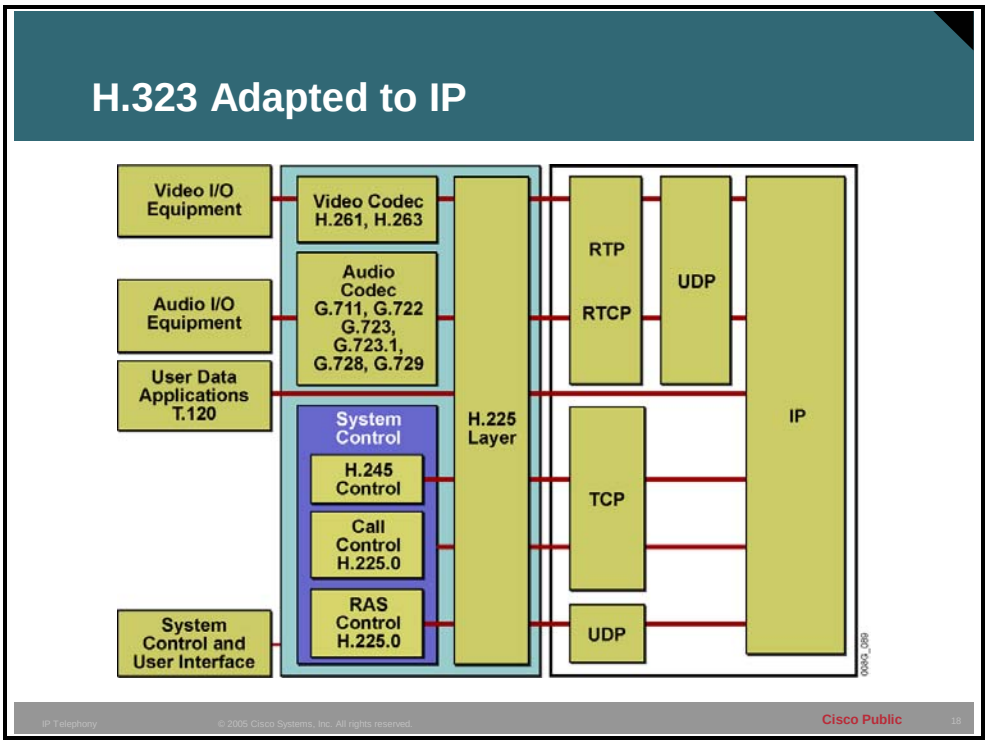
H.323 is based on the ISDN Q.931 protocol, which allows H.323 to easily interoperate with legacy voice networks, such as the public switched telephone network (PSTN) or SS7. In addition to providing support for call setup, H.225.0 provides a message transport mechanism for the H.245 control function and the RAS signaling function. Following is a description of these functions:

- **Call-signaling function:** The call-signaling function uses a call-signaling channel that allows an endpoint to create connections with other endpoints. The call-signaling function defines call setup procedures, based on the call setup procedures for ISDN (Recommendation Q.931). The call-signaling function uses messages formatted according to H.225.0.
- **H.245 control function:** The H.245 control function uses a control channel to transport control messages between endpoints or between an endpoint and a common control component, such as a gatekeeper or multipoint controller (MC). The control channel used by the H.245 control function is separate from the call-signaling channel.

  The H.245 control function is responsible for the following:

  - **Logical channel signaling:** Opens and closes the channel that carries the media stream
  - **Capabilities exchange:** Negotiates audio, video, and codec capability between the endpoints
  - **Master or responder determination:** Determines which endpoint is master and which is responder; used to resolve conflicts during the call
  - **Mode request:** Requests a change in mode, or capability, of the media stream
  - **Timer and counter values:** Establishes values for timers and counters and agreement of those values by the endpoints
- **RAS signaling function:** The RAS signaling function uses a separate signaling channel (RAS channel) to perform registration, admissions, bandwidth changes, status, and disengage procedures between endpoints and a gatekeeper. The RAS signaling function uses messages formatted according to H.225.0.

 Copyright © 2005, Cisco Systems, Inc.

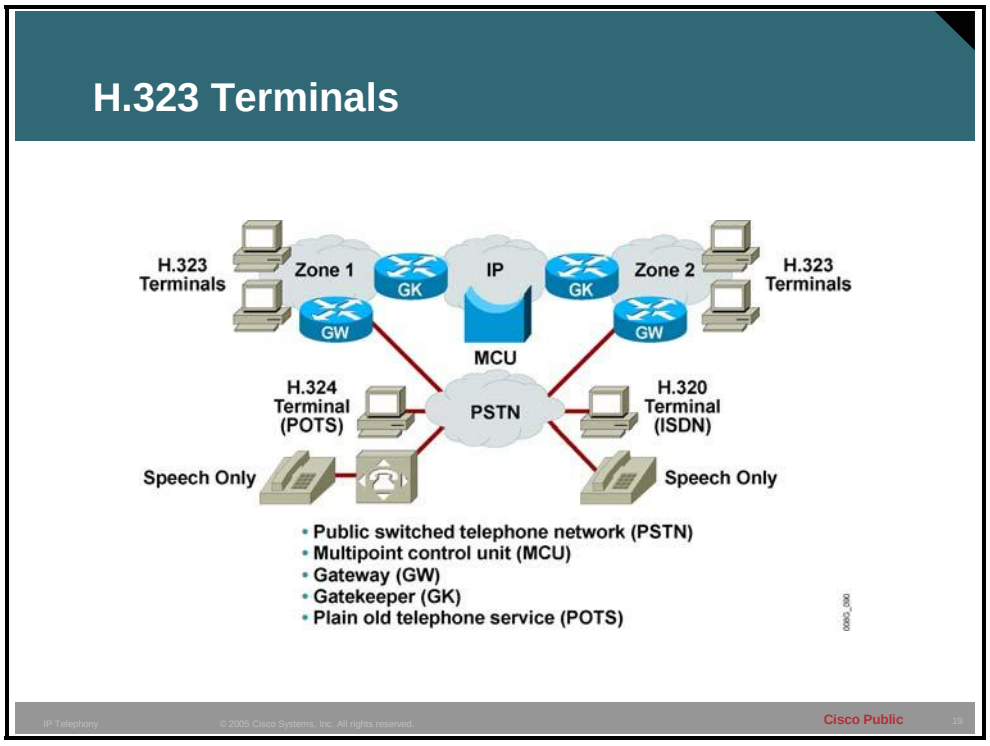


Example: H.323 Adapted to IP

A typical implementation of H.323 goes beyond the original LAN context of H.323. The figure illustrates a specific application of H.323 on an IP internetwork. Notice that real-time aspects of H.323 rely on UDP. Both the session-oriented control procedures and the data media type of H.323 use TCP.

Functional Components of H.323

This topic describes the functional components that make up an H.323 environment.

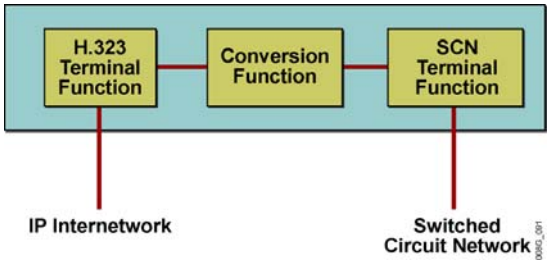


An H.323 terminal is an endpoint that provides real-time voice (and optionally, video and data) communications with another endpoint, such as an H.323 terminal, gateway, or multipoint control unit (MCU).

An H.323 terminal must be capable of transmitting and receiving G.711 (a-law and µ-law) 64-kbps pulse code modulation (PCM)-encoded voice, and may support other encoded voice formats, such as G.729 and G.723.1.

 Copyright © 2005, Cisco Systems, Inc.

H.323 Gateways

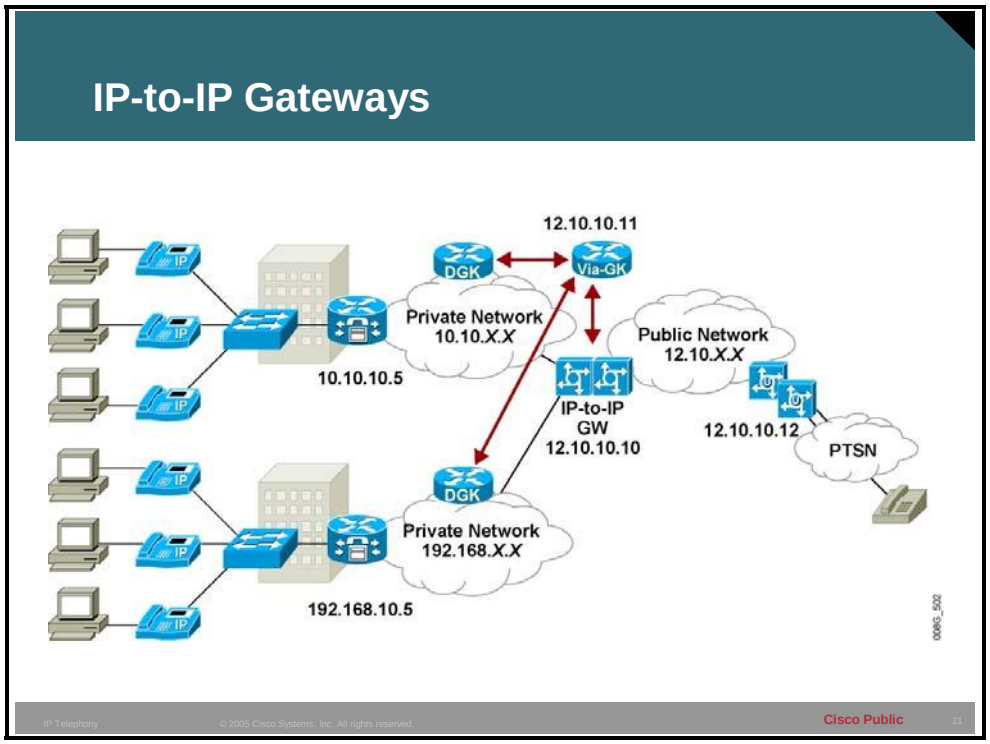


IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 20

An H.323 gateway is an optional type of endpoint that provides interoperability between H.323 endpoints and endpoints located on a switched-circuit network (SCN), such as the PSTN or an enterprise voice network. Ideally, the gateway is transparent to both the H.323 endpoint and the SCN-based endpoint.

An H.323 gateway performs the following services:

- Translation between audio, video, and data formats
- Conversion between call setup signals and procedures
- Conversion between communication control signals and procedures

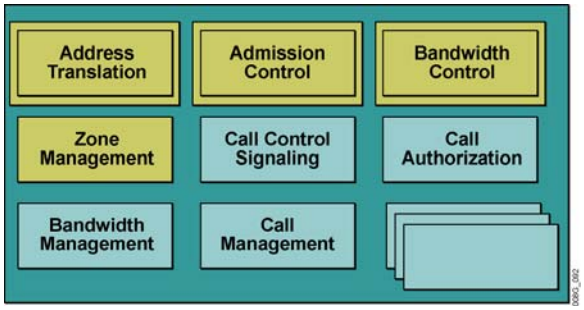


The IP-to-IP gateway facilitates easy and cost-effective connectivity between independent VoIP service provider networks. Some in the industry call IP-to-IP gateways “border elements” or “session border controllers.” The IP-to-IP gateway provides a network-to-network interface point for billing, security, Cisco CallManager interconnectivity, call admission control, and signaling interworking. It will perform most of the same functions of a PSTN-to-IP gateway, but will join two VoIP call legs. Media packets can either flow through the gateway and hide the networks from each other, or flow around the IP-to-IP gateway if network security is not of primary importance.

The figure illustrates a basic IP-to-IP gateway network. From the perspective of the private, or customer, networks, the IP-to-IP gateway will appear as a single public address that must be routable on their private networks (in this case a 12.*x.x.x* address routable on the 10.10.*x.x* and 192.168.*x.x* networks). Care must be taken at the IP-to-IP gateway to ensure that proper routing restrictions are in place to prevent communication directly between the private networks attached to it. Also note that this model works only if no overlapping address schemes are used on the customers’ networks. Finally, to the hop-off gateways on the public network, all calls will appear to originate from the 12.*x.x.x* address of the IP-to-IP gateway and not the private addresses on the customer networks. Also note that the gatekeepers shown in the diagram control each zone independently, with the 12.10.10.11 gatekeeper acting as the control point for the public network, and therefore the IP-to-IP gateway.

 Copyright © 2005, Cisco Systems, Inc.

H.323 Gatekeepers



© 2005 Cisco Systems, Inc. All rights reserved.

An H.323 gatekeeper is an optional component that provides call control support and services to H.323 endpoints. Although a gatekeeper is considered a distinct and optional component, it can be colocated with any other H.323 component.

The scope of endpoints over which a gatekeeper exercises its authority is called a “zone.” H.323 defines a one-to-one relationship between a zone and a gatekeeper.

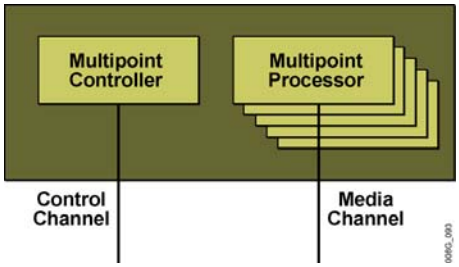
When a gatekeeper is included, it must perform the following functions:

- **Address translation:** Converts an alias address to an IP address
- **Admission control:** Limits access to network resources based on call bandwidth restrictions
- **Bandwidth control:** Responds to bandwidth requests and modifications
- **Zone management:** Provides services to registered endpoints

The gatekeeper may also perform:

- **Call control signaling:** Performs call signaling on behalf of the endpoint (gatekeeper-routed call signaling)
- **Call authorization:** Rejects calls based on authorization failure
- **Bandwidth management:** Limits the number of concurrent accesses to IP internetwork resources (Call Admission Control [CAC])
- **Call management:** Maintains a record of ongoing calls

Multipoint Conference Components



IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 23

Support for multipoint conferences is provided by the following three functional components:

- **Multipoint controller:** An MC provides the functions that are necessary to support conferences involving three or more endpoints. The MC establishes an H.245 control channel with each of the conference participants. Through the control channel, the MC completes a capability exchange during which the MC indicates the mode of the conference (decentralized or centralized).

  An MC is not modeled as a standalone component; it may be located with an endpoint (terminal or gateway), a gatekeeper, or a multipoint control unit.

- **Multipoint processor:** A multipoint processor (MP) adds functionality to multipoint conferences. An MP can receive multiple streams of multimedia input, process the streams by switching and mixing the streams, and then retransmit the result to all or some of the conference members.

  Similar to an MC, an MP is not modeled as a standalone component; it resides in an MCU.

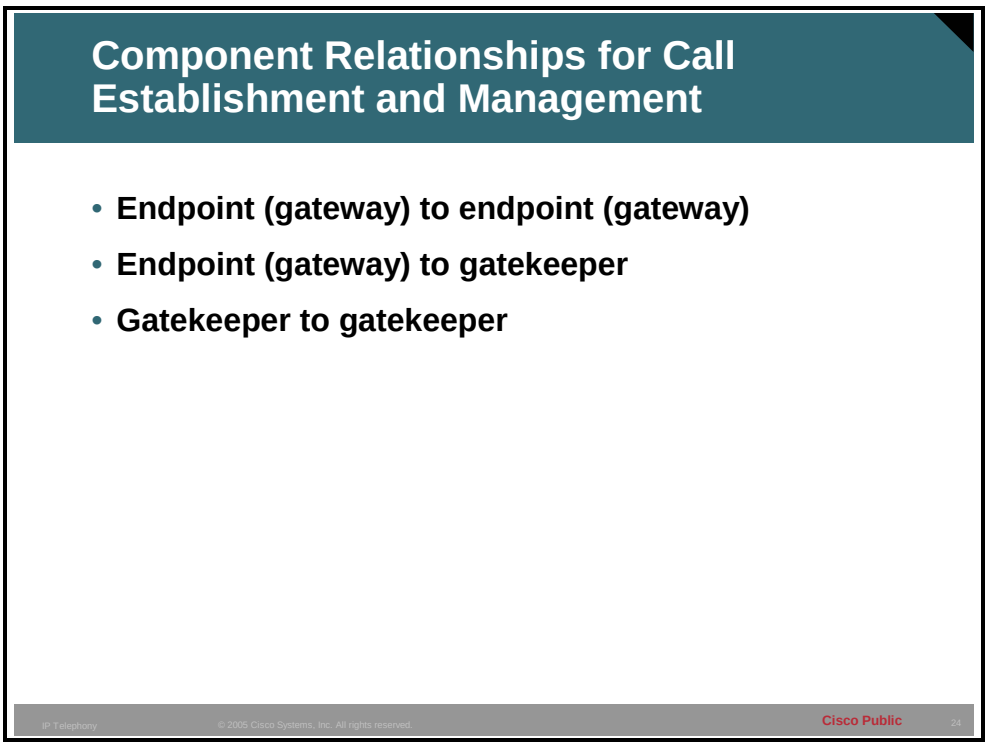
- **Multipoint control unit:** An MCU is modeled as an endpoint that provides support for multipoint conferences by incorporating one MC and zero or more MPs.

  An MCU is modeled as a standalone component.

 Copyright © 2005, Cisco Systems, Inc.

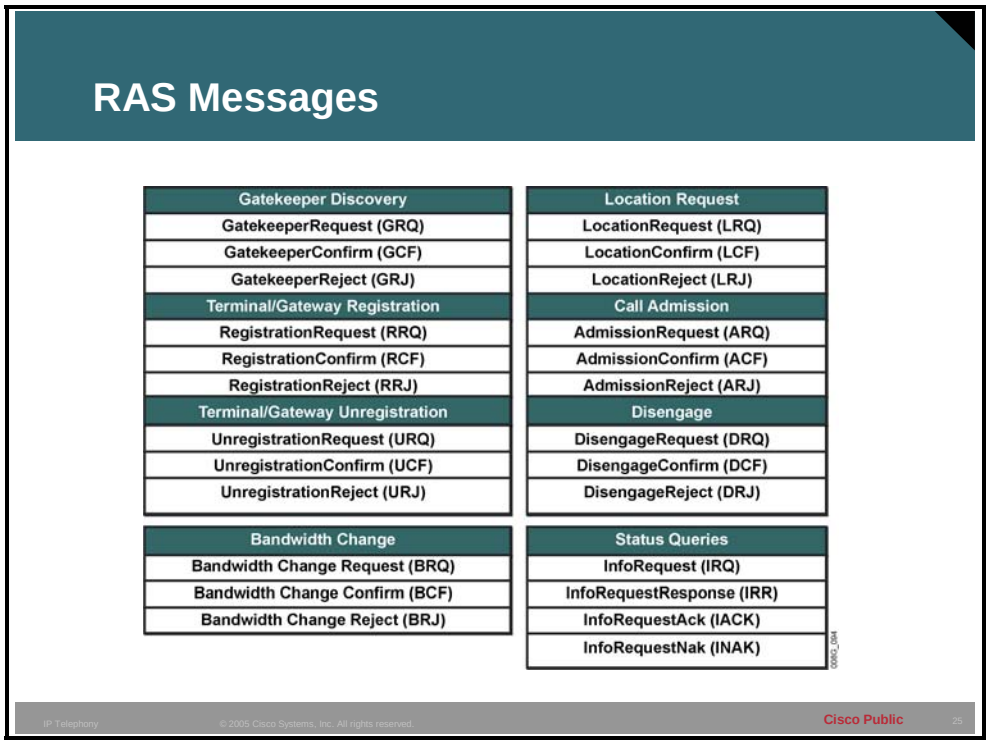
H.323 Call Establishment and Maintenance

This topic describes possible component scenarios required to establish end-to-end connections and the commands used by the components to establish VoIP calls.



Although H.323 is based on the concepts of a distributed call control model, it often embodies centralized call control model concepts. Calls can be established between any of the following components:

- **Endpoint to endpoint:** The intelligence of H.323 endpoints allows them to operate autonomously. In this mode of operation, endpoints locate other endpoints through nonstandard mechanisms and initiate direct communication between the endpoints.
- **Endpoint to gatekeeper:** When a gatekeeper is added to the network, endpoints interoperate with the gatekeeper using the RAS channel.
- **Gatekeeper to gatekeeper:** In the presence of multiple gatekeepers, gatekeepers communicate with each other on the RAS channel.



Gatekeepers communicate through the RAS channel using different types of RAS messages. These message types include the following:

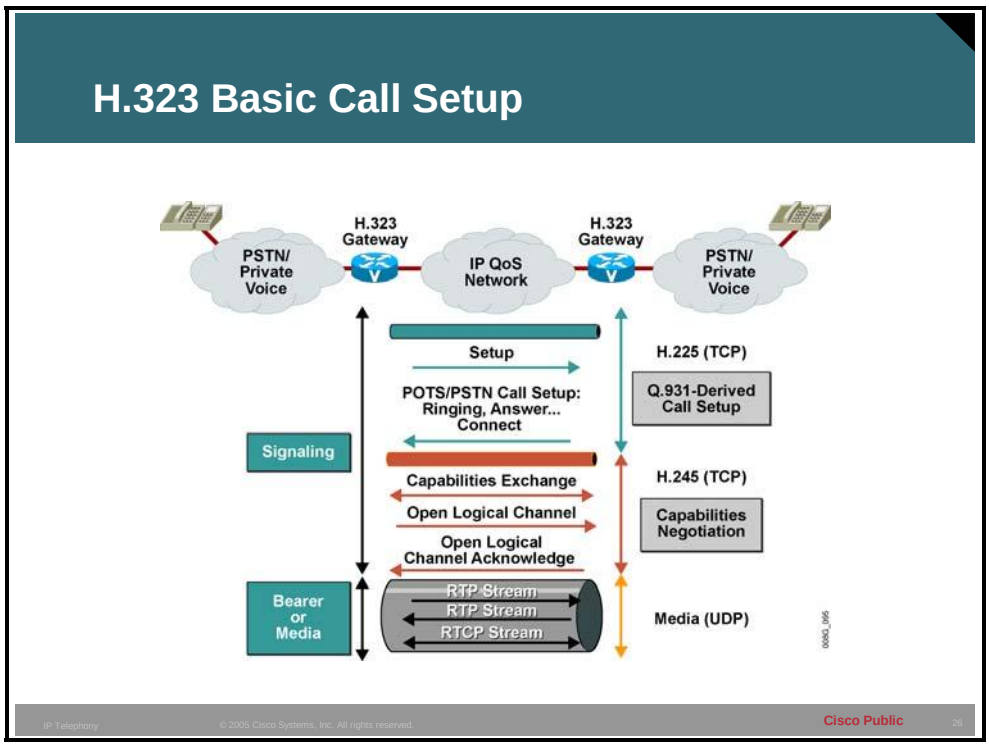
- **Gatekeeper discovery:** An endpoint multicasts a gatekeeper discovery request (GRQ). A gatekeeper may confirm (gatekeeper confirmation [GCF]) or reject (gatekeeper rejection [GRJ]) an endpoint.
- **Terminal/gateway registration:** An endpoint sends a registration request (RRQ) to its gatekeeper to register and provide reachable prefixes. A gatekeeper confirms (registration confirmation [RCF]) or rejects (registration rejection [RRJ]) the registration.
- **Terminal/gateway unregistration:** An endpoint or gatekeeper sends an unregistration request (URQ) to cancel a registration. The responding device confirms (unregistration request [UCF]) or rejects (unregistration rejection [URJ]) the request.
- **Location request:** An endpoint or gatekeeper sends a location request (LRQ) to a gatekeeper. An LRQ is sent directly to a gatekeeper if one is known, or it is multicast to the gatekeeper discovery multicast address. An LRQ requests address translation of an E.164 address and solicits information about the responsible endpoint. The responding gatekeeper confirms (location confirmation [LCF]) with the IP address of the endpoint or rejects the request (location rejection [LRJ]) if the address is unknown.
- **Call admission:** An endpoint sends an admission request (ARQ) to its gatekeeper. The request identifies the terminating endpoint and the bandwidth required. The gatekeeper confirms (admission confirmation [ACF]) with the IP address of the terminating endpoint or rejects (admission rejection [ARJ]) if the endpoint is unknown or inadequate bandwidth is available.
- **Bandwidth change:** An endpoint sends a bandwidth change request (BRQ) to its gatekeeper to request an adjustment in call bandwidth. A gatekeeper confirms (bandwidth confirmation [BCF]) or rejects (bandwidth rejection [BRJ]) the request.

 Copyright © 2005, Cisco Systems, Inc.

- **Disengage:** When a call is disconnected, the endpoint sends a disengage request (DRQ) to the gatekeeper. The gatekeeper confirms (disengage confirmation [DCF]) or rejects (disengage rejection [DRJ]) the request.
- **Status queries:** A gatekeeper uses status request (IRQ) to determine the status of an endpoint. In its response (IRR), the endpoint indicates whether it is online or offline. The endpoint may also reply that it understands the information request (information request acknowledged [IACK]) or that it does not understand the request (information request not acknowledged [INAK]).

Call Flows Without a Gatekeeper

This topic describes call setup scenarios without a gatekeeper and provides examples of actual call-flow procedures.



The figure shows an H.323 basic call setup exchange between two gateways. The optional gatekeeper is not present in this example. Although gateways are shown, the same procedure is used when one or both endpoints are H.323 terminals.

The flow procedure without a gatekeeper includes these steps:

1. The originating gateway initiates an H.225.0 session with the destination gateway on registered TCP port 1720. The gateway determines the IP address of the destination gateway internally. The gateway has the IP address of the destination endpoint in its configuration or it knows a Domain Name System (DNS) resolvable domain name for the destination.

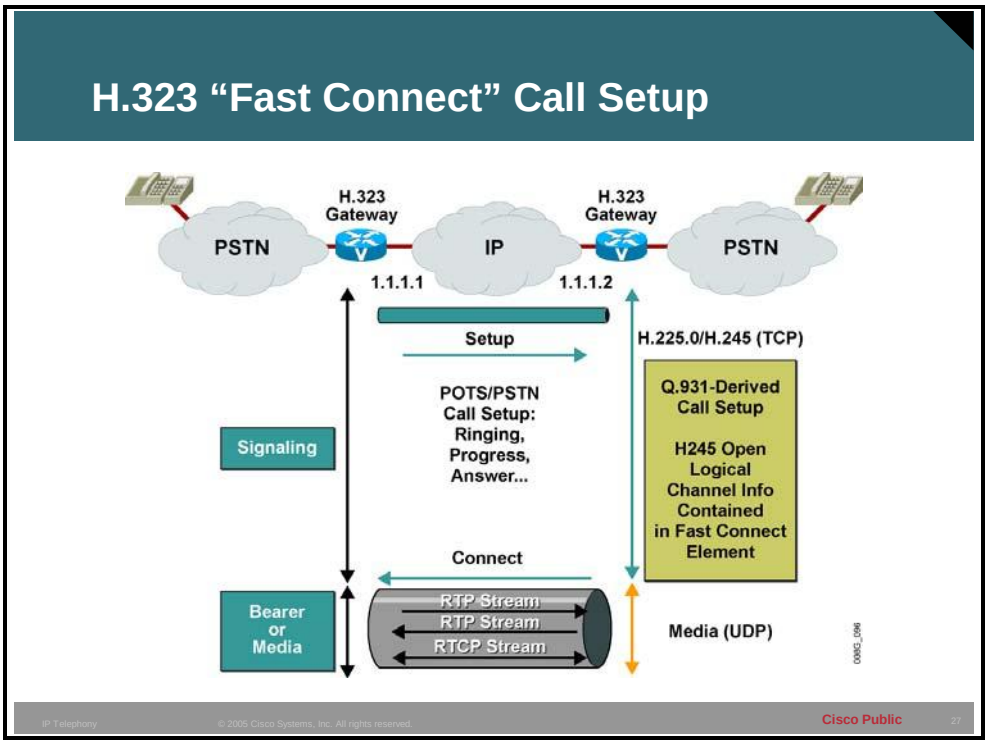
2. Call setup procedures based on Q.931 create a call-signaling channel between the endpoints.

3. The endpoints open another channel for the H.245 control function. The H.245 control function negotiates capabilities and exchanges logical channel descriptions.

4. The logical channel descriptions open RTP sessions.

5. The endpoints exchange multimedia over the RTP sessions.

 Copyright © 2005, Cisco Systems, Inc.

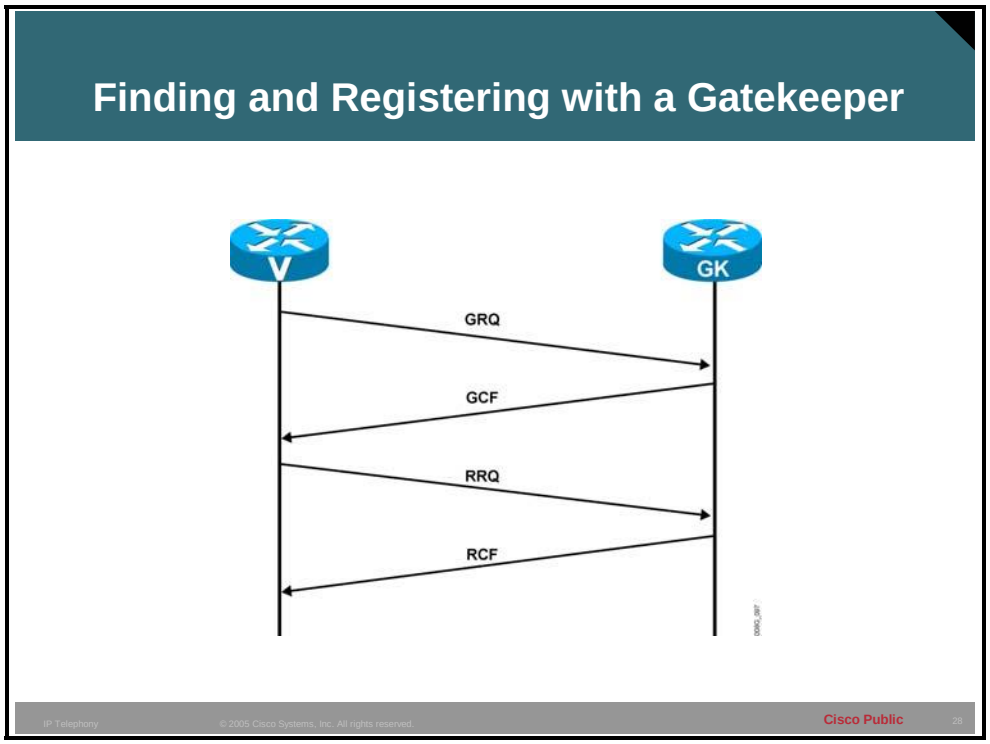


The figure shows an H.323 setup exchange that uses the Fast Connect abbreviated procedure available in version 2 of Recommendation H.323. The Fast Connect procedure reduces the number of round-trip exchanges and achieves the capability exchange and logical channel assignments in one round trip.

The Fast Connect procedure includes these steps:

1. The originating gateway initiates an H.225.0 session with the destination gateway on registered TCP port 1720.
2. Call setup procedures based on Q.931 create a combined call-signaling channel and control channel for H.245. Capabilities and logical channel descriptions are exchanged within the Q.931 call setup procedure.
3. Logical channel descriptions open RTP sessions.
4. The endpoints exchange multimedia over the RTP sessions.

Note	Cisco H.323 voice equipment supports up to version 4 of H.323 and is backward compatible to earlier versions.



The figure illustrates how an endpoint locates and registers with a gatekeeper. A gatekeeper adds scalability to H.323. Without a gatekeeper, an endpoint must recognize or have the ability to resolve the IP address of the destination endpoint.

Before an endpoint can use a gatekeeper, it must register with the gatekeeper. To register, an endpoint must recognize the IP address of the gatekeeper.

One of these two methods are used to determine the address of the gatekeeper:

- An endpoint can be preconfigured to recognize the domain name or IP address of its gatekeeper. If configured to recognize the name, an endpoint must have a means to resolve the name to an IP address. A common address resolution technique is the DNS.
- An endpoint can issue a multicast GRQ to the gatekeeper discovery address (224.0.1.41) to discover the IP address of its gatekeeper. If the endpoint receives a GCF to the request, it uses the IP address to proceed with registration.

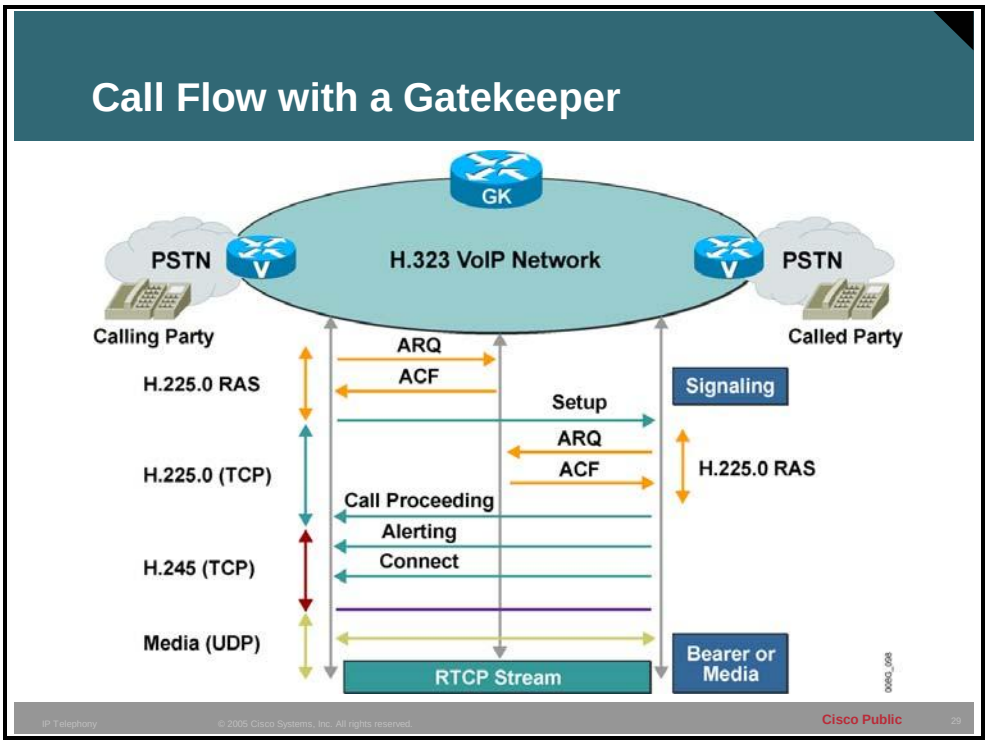
To initiate registration, an endpoint sends an RRQ to the gatekeeper. In the register request, the endpoint identifies itself with its ID and provides its IP address. Optionally, the endpoint lists the prefixes (for example, telephone numbers) that it supports. These prefixes are gleaned from the plain old telephone service (POTS) dial-peer destination patterns associated with any FXS port.

With this procedure, a gatekeeper determines the location and identity of endpoints and the identities of SCN endpoints from gateway registrations.

 Copyright © 2005, Cisco Systems, Inc.

Call Flows with a Gatekeeper

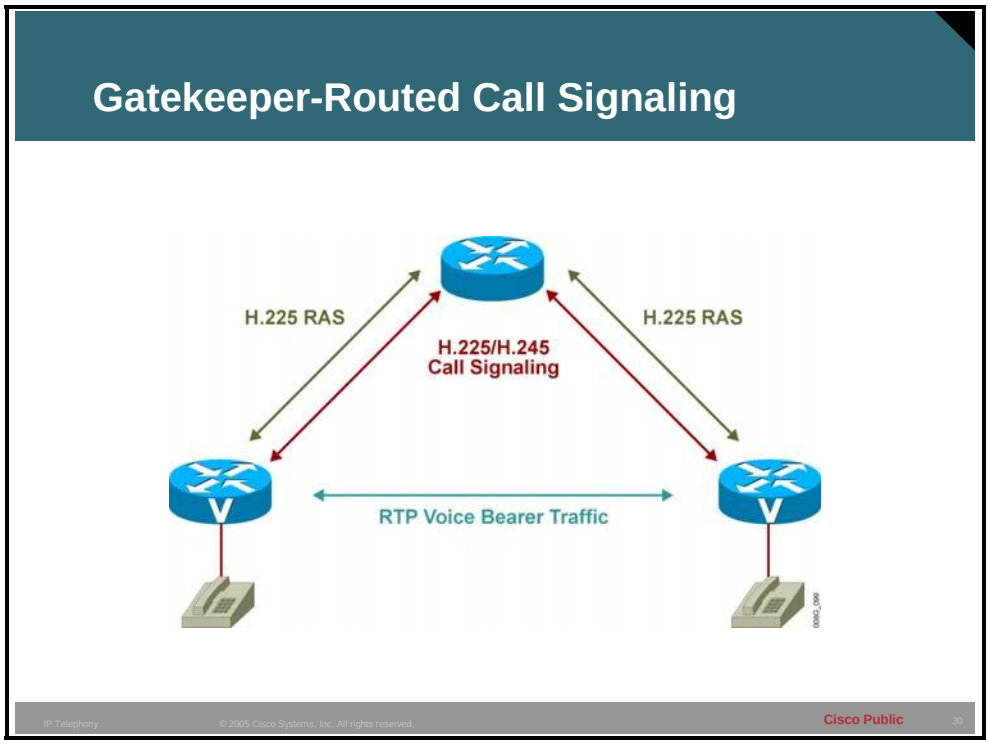
This topic discusses call setup scenarios with a gatekeeper.



The exchanges in the figure illustrate the use of a gatekeeper by both endpoints. In this example, both endpoints have registered with the same gatekeeper. Call flow with a gatekeeper proceeds as follows:

1. The gateway sends an ARQ to the gatekeeper to initiate the procedure. The gateway is configured with the domain or address of the gatekeeper.
2. The gatekeeper responds to the admission request with an ACF. In the confirmation, the gatekeeper provides the IP address of the remote endpoint.
3. When the originating endpoint identifies the terminating endpoint, it initiates a basic call setup.
4. Before the terminating endpoint accepts the incoming call, it sends an ARQ to the gatekeeper to gain permission.
5. The gatekeeper responds affirmatively, and the terminating endpoint proceeds with the call setup procedure.

During this procedure, if the gatekeeper responds to either endpoint with an ARJ to the admission request, the endpoint that receives the rejection terminates the procedure.



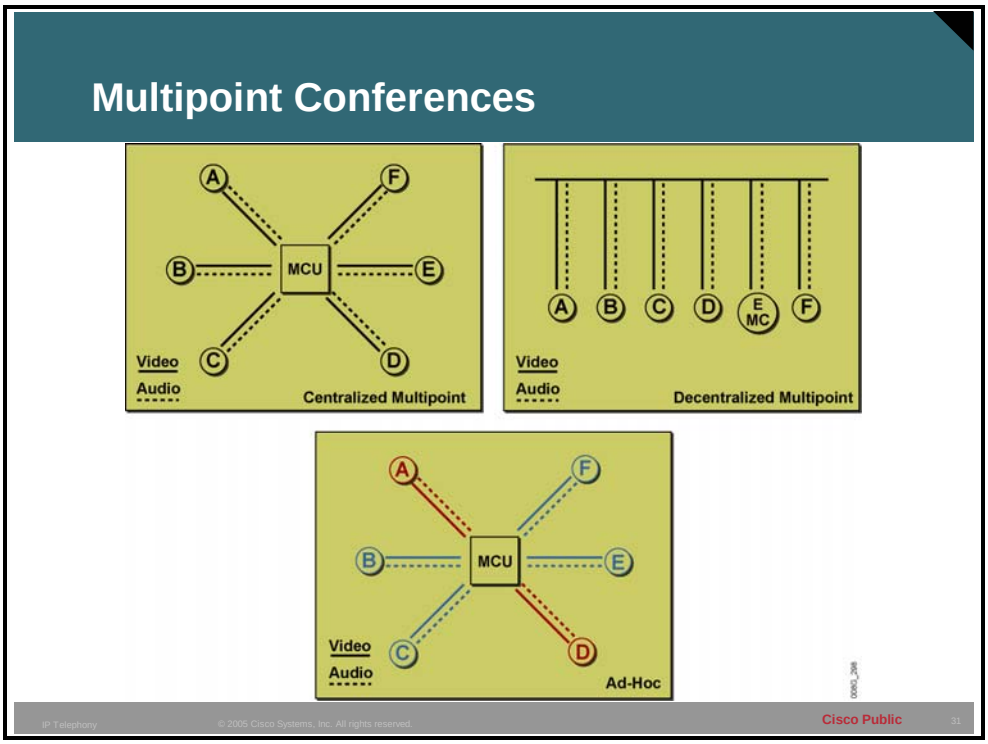
In the previous examples, the call-signaling channel is created from endpoint to endpoint. In some cases, it is desirable to have the gatekeeper represent the other endpoint for signaling purposes. This method is called gatekeeper-routed call signaling. The process for gatekeeper-routed call signaling is as follows:

1. The gatekeeper responds to an admission request and advises the endpoint to perform the call setup procedure with the gatekeeper, not with the terminating endpoint.
2. The endpoint initiates the setup request with the gatekeeper.
3. The gatekeeper sends its own request to the terminating endpoint and incorporates some of the details acquired from the originating request.
4. When a connect message is received from the terminating endpoint, the gatekeeper sends a connect to the originating endpoint.
5. The two endpoints establish an H.245 control channel between them. The call procedure continues normally from this point.

 Copyright © 2005, Cisco Systems, Inc.

Multipoint Conferences

H.323 defines three types of multipoint conferences: centralized, distributed, and ad-hoc. H.323 also defines a hybrid of the first two. This topic describes the multipoint conference control components used to support these conferences.



All types of multipoint conferences rely on a single MC to coordinate the membership of a conference. Each endpoint has an H.245 control channel connection to the MC. Either the MC or the endpoint initiates the control channel setup. H.323 defines the following three types of conferences:

- **Centralized multipoint conference:** The endpoints must have their audio, video, or data channels connected to an MP. The MP performs mixing and switching of the audio, video, and data, and if the MP supports the capability, each endpoint can operate in a different mode.
- **Distributed multipoint conference:** The endpoints do not have a connection to an MP. Instead, endpoints multicast their audio, video, and data streams to all participants in the conference. Because an MP is not available for switching and mixing, any mixing of the conference streams is a function of the endpoint, and all endpoints must use the same communication parameters.

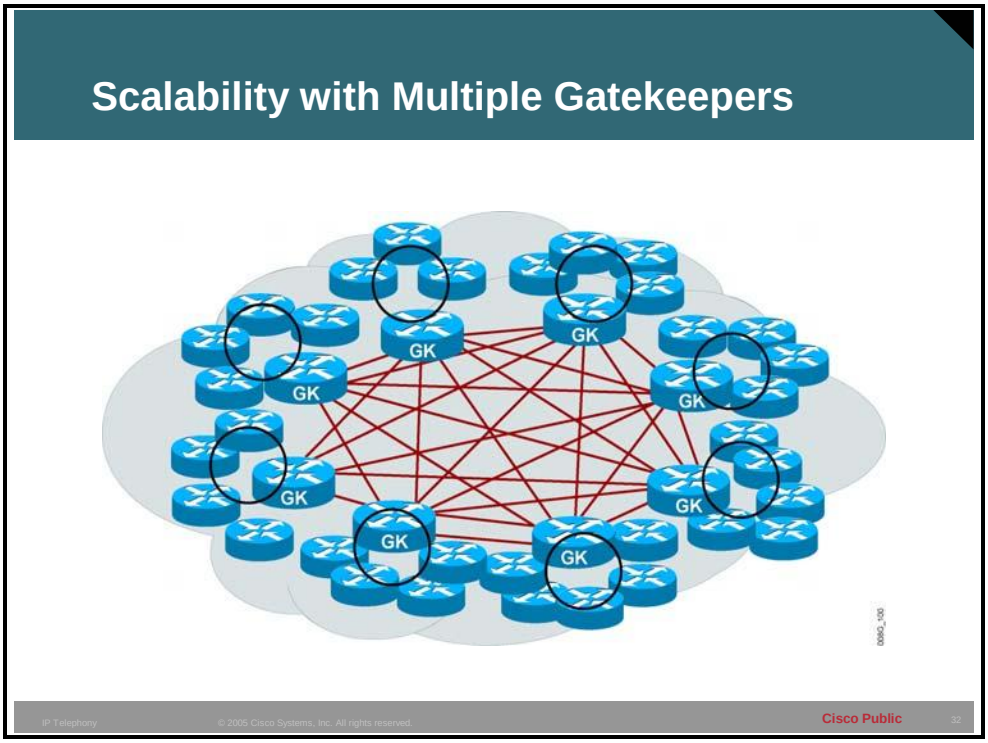
To accommodate situations in which two streams (audio and video) would be handled by the different multipoint conference models, H.323 defines a “hybrid.” A hybrid describes a situation in which the audio and video streams are managed by a single H.245 control channel with the MC, but where one stream relies on multicast (according to the distributed model) and the other uses the MP (as in the centralized model).

- **Ad-hoc multipoint conference:** Any two endpoints in a call can convert their relationship into a point-to-point conference. If neither of the endpoints has a colocated MC, then the services of a gatekeeper are used. When the point-to-point conference is created, other endpoints become part of the conference by accepting an invitation from a current participant, or the endpoint can request to join the conference.

 Copyright © 2005, Cisco Systems, Inc.

Call Flows with Multiple Gatekeepers

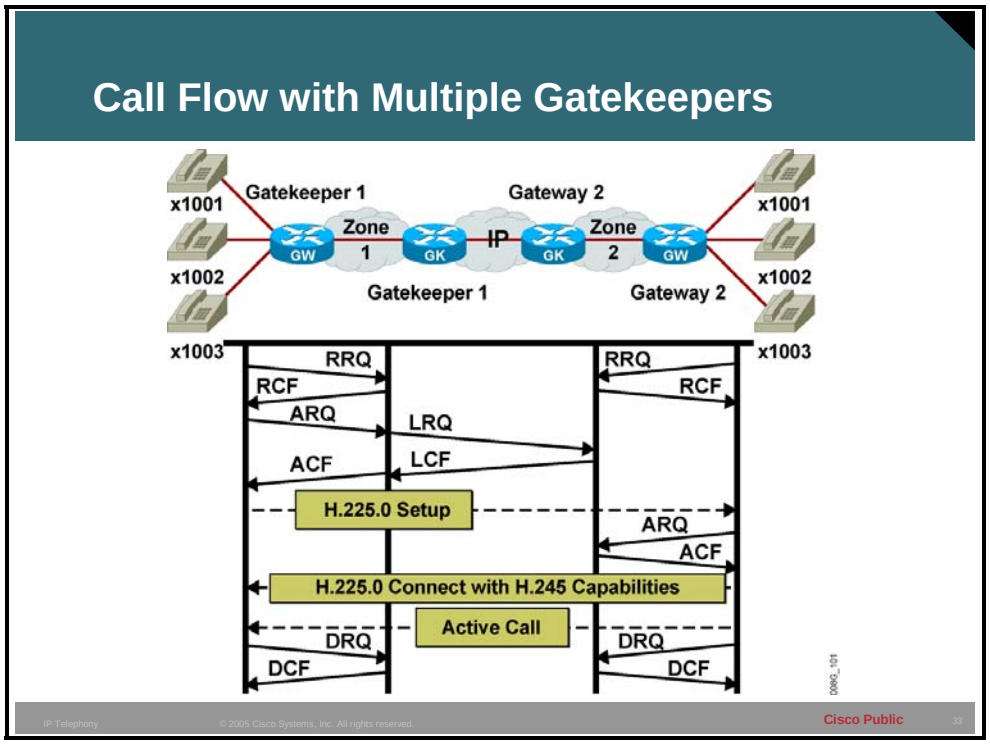
By simplifying configuration of the endpoints, gatekeepers aid in building large-scale VoIP networks. As the VoIP network grows, incorporating additional gatekeepers enhances the network scalability. This topic discusses the use of multiple gatekeepers for scalability and illustrates call flow in a multiple gatekeeper environment.



Without a gatekeeper, endpoints must find each other by any means available. This limits the growth potential of the VoIP network. Through the registration and address resolution services of a gatekeeper, growth potential improves significantly.

A single gatekeeper design may not be appropriate for several reasons. A single gatekeeper can become overloaded, or it can have an inconvenient network location, necessitating a long and expensive round trip to it.

Deploying multiple gatekeepers offers a more scalable and robust environment.



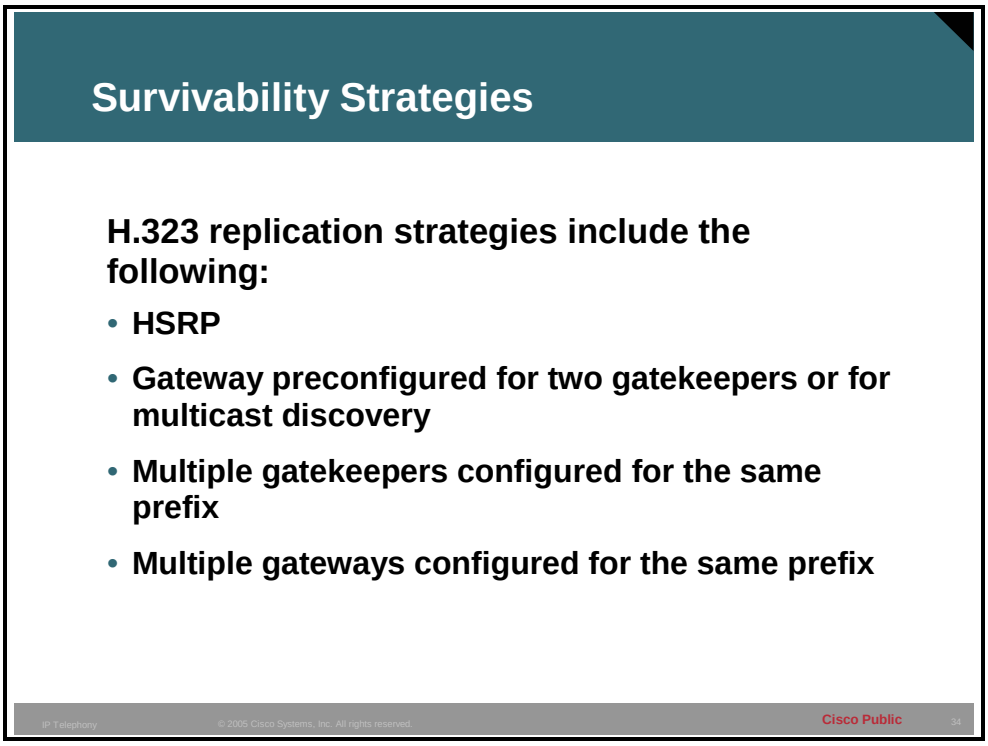
The figure illustrates a call setup involving two gatekeepers. In this example, each endpoint is registered with a different gatekeeper. Notice the changes in the following call setup procedure:

1. The originating endpoint sends an admission request to its gatekeeper requesting permission to proceed and asking for the session parameters for the terminating endpoint.
2. The gatekeeper for the originating endpoint (gatekeeper 1) determines from its configuration or from a directory resource that the terminating endpoint is potentially associated with gatekeeper 2. Gatekeeper 1 sends an LRQ to gatekeeper 2.
3. Gatekeeper 2 recognizes the address and sends back an LCF. In the confirmation, gatekeeper 2 provides the IP address of the terminating endpoint.
4. If gatekeeper 1 considers the call acceptable for security and bandwidth reasons, it maps the LCF to an ARQ and sends the confirmation back to the originating endpoint.
5. The endpoint initiates a call setup to the remote endpoint.
6. Before accepting the incoming call, the remote endpoint sends an ARQ to gatekeeper 2 requesting permission to accept the incoming call.
7. Gatekeeper 2 performs admission control on the request and responds with a confirmation.
8. The endpoint responds to the call setup request.
9. The call setup progresses through the H.225.0 call function and H.245 control function procedures until the RTP sessions are initiated.
10. At the conclusion of the call, each endpoint sends a disconnect request to its gatekeeper to advise the gatekeeper that the call is complete.
11. The gatekeeper responds with a confirmation.

 Copyright © 2005, Cisco Systems, Inc.

Survivability Strategies

Maintaining high availability in an H.323 environment requires a design that accommodates failure of a critical component. This topic describes strategies for maintaining VoIP service.



In any environment that depends on common control components, the vulnerability of the environment is directly proportional to the probability of common control component failure. In a classical telephone application, fault tolerance is accommodated by incorporating extra common control technology. One strategy replicates all critical components. This expensive approach is often replaced with the more cost-effective solution of "*n* out of *n* + 1" redundancy; a single spare component is available to step in when any one of the active *n* components fails. The essential part of either strategy is the replication of key components.

In H.323, the key components are the gateways and the gatekeeper. H.323 can employ any of the following strategies:

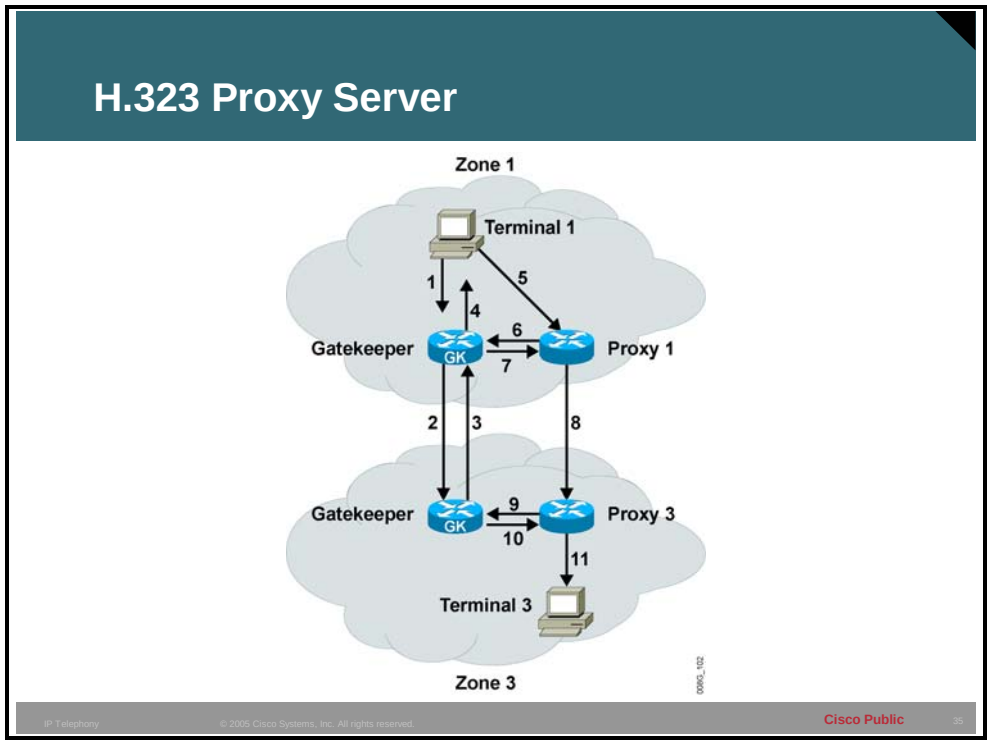
- **Hot Standby Router Protocol:** The Hot Standby Router Protocol (HSRP) allows two gatekeepers to share both an IP address and access to a common LAN; however, at any time, only one is active. Endpoints are configured with the name of the gatekeeper, which they can resolve using DNS or the IP address of the gatekeeper.
- **Multiple gatekeepers with gatekeeper discovery:** Deployment of multiple gatekeepers reduces the probability of total loss of gatekeeper access. However, adding new gatekeepers presents a new challenge. Each gatekeeper creates a unique H.323 zone. Because an H.323 endpoint is associated with only one gatekeeper at a time (in only one zone at a time), endpoints are configured to find only one of several working gatekeepers. Fortunately, a gateway can be configured with an ordered list of gatekeepers, or to use IP multicast to locate a gatekeeper.

- **Multiple gatekeepers configured for the same prefix:** Gatekeepers send location request messages to other gatekeepers when locating an endpoint. By supporting the same prefix on multiple gatekeepers, the location request can be resolved by multiple gatekeepers. This strategy makes the loss of one gatekeeper less significant.
- **Multiple gateways configured for the same prefix:** Survivability is enhanced at the gateway with multiple gateways that are configured to reach the same SCN destination. By configuring the same prefix of destinations in multiple gateways, the gatekeeper sees the same prefix more than once as each gateway registers with its gatekeeper.

 Copyright © 2005, Cisco Systems, Inc.

H.323 Proxy Server

This topic describes a call setup scenario involving a proxy server.



An H.323 proxy server can circumvent the shortcomings of a direct path in cases where the direct path between two H.323 endpoints is not the most appropriate; for example, when the direct path has poor throughput and delay characteristics, is not easily available because of a firewall, or zones are configured as inaccessible on the gatekeepers in order to isolate addressing information in different zones.

When a proxy server is involved, two sessions are typically established as follows:

- Originating endpoint to the proxy server
- Proxy server to the terminating endpoint

However, when a proxy server also represents the terminating endpoint, a third session is required, as follows:

- Originating endpoint to proxy server 1
- Proxy server 1 to proxy server 2
- Proxy server 2 to terminating endpoint

Example: H.323 Proxy

The figure illustrates an example with three sessions. The objective in this scenario is for terminal 1 and terminal 3 to establish an end-to-end relationship for multimedia communications. The following sequence of events occurs:

1. Terminal 1 asks gatekeeper 1 for permission to call terminal 3.

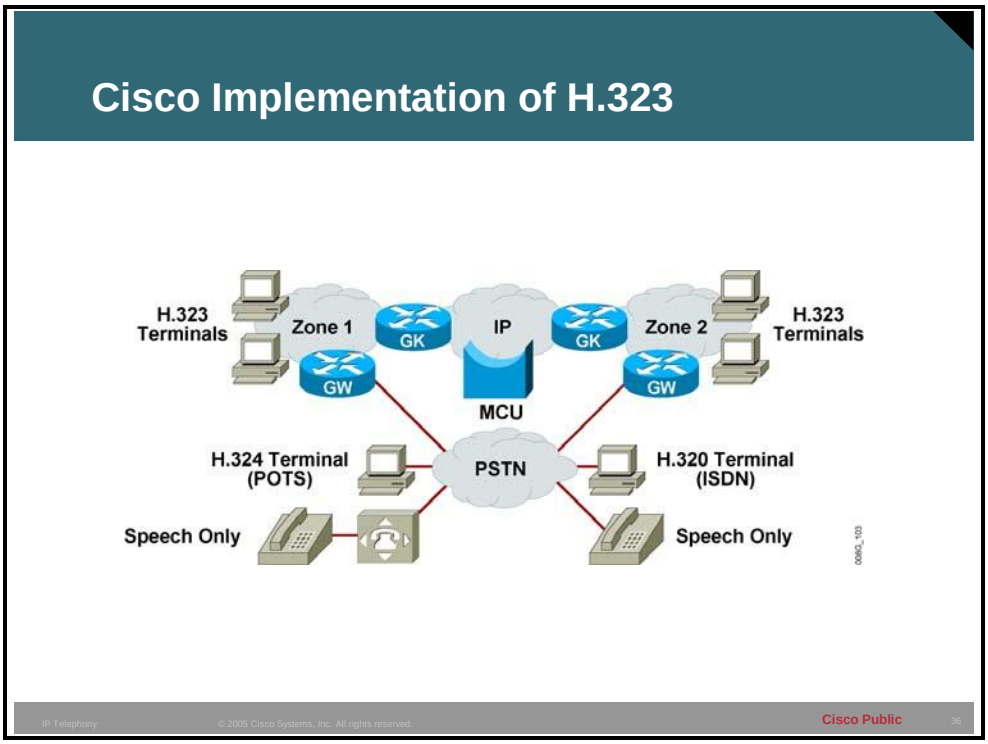
2. Gatekeeper 1 locates gatekeeper 3 as the terminal 3 gatekeeper. Gatekeeper 1 asks gatekeeper 3 for the address of terminal 3.
3. Gatekeeper 3 responds with the address of proxy 3 (instead of the address of terminal 3) to hide the identity of terminal 3.
4. Gatekeeper 1 is configured to get to proxy 3 by way of proxy 1, so gatekeeper 1 returns the address of proxy 1 to terminal 1.
5. Terminal 1 calls proxy 1.
6. Proxy 1 consults gatekeeper 1 to discover the true destination of the call, which is terminal 3 in this example.
7. Gatekeeper 1 instructs proxy 1 to call proxy 3.
8. Proxy 1 calls proxy 3.
9. Proxy 3 consults gatekeeper 3 for the true destination, which is terminal 3.
10. Gatekeeper 3 gives the address of terminal 3 to proxy 3.
11. Proxy 3 completes the call to terminal 3.

Notice that the resulting path between terminal 1 and terminal 3 involves three separate legs; one between terminal 1 and proxy 1, one between proxy 1 and proxy 3, and one between proxy 3 and terminal 3. Both the media and any signaling are carried over these three legs.

 Copyright © 2005, Cisco Systems, Inc.

Cisco Implementation of H.323

This topic discusses how Cisco implements H.323.

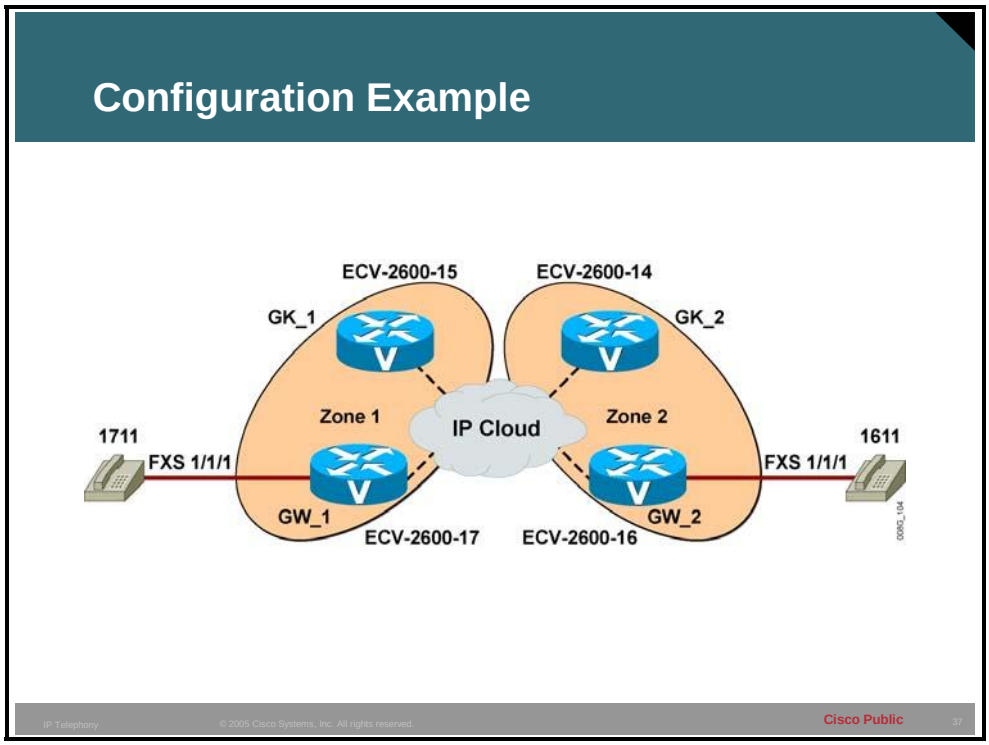


Cisco provides support for all H.323 components. These H.323 components include the following:

- **H.323 terminals:** Cisco provides support for H.323 terminals in Cisco IP Phone.
- **Gateways:** Cisco implements H.323 gateway support in:
  - Cisco voice-enabled routers (first available in Cisco IOS Release 11.3)
  - Cisco SC2200 Signaling Controllers
  - Cisco PGW 2200 PSTN gateways
  - Voice-enabled Cisco AS5*xx*0 access servers
  - Cisco BTS 10200 Softswitch
- **Gatekeepers:** Cisco implements gatekeeper support in:
  - Cisco Multimedia Conference Manager
  - Cisco CallManager
  - Routers (first available in Cisco IOS Release 11.3)
- **Multipoint control unit:** The MC and MP of the Cisco IP/VC 3500 Series MCU support all H.323 conference types. The IP/VC 3500 also incorporates a gatekeeper.
- **Other support:** Cisco PIX 500 Series firewalls and Context-Based Access Control (CBAC) support in the Cisco Secure Integrated Software monitor the logical channel handshaking of the H.245 control function and dynamically open conduits for the RTP sessions.

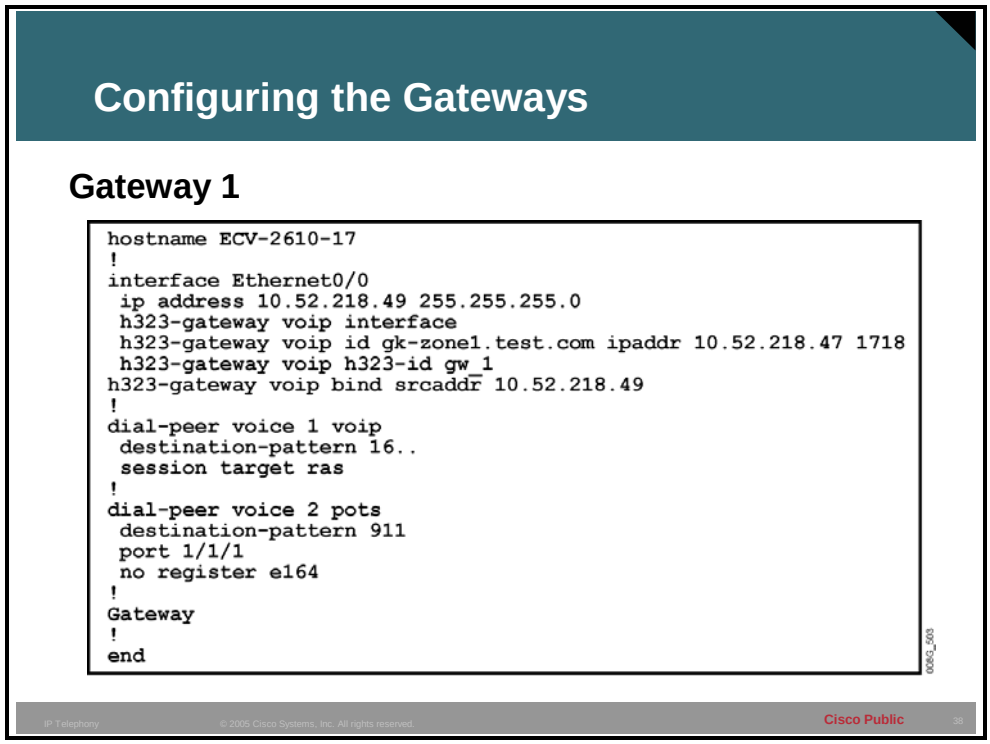
Configuring H.323 Gateways

This topic illustrates and describes the configuration commands used to create a two-zone, two-gatekeeper scenario.



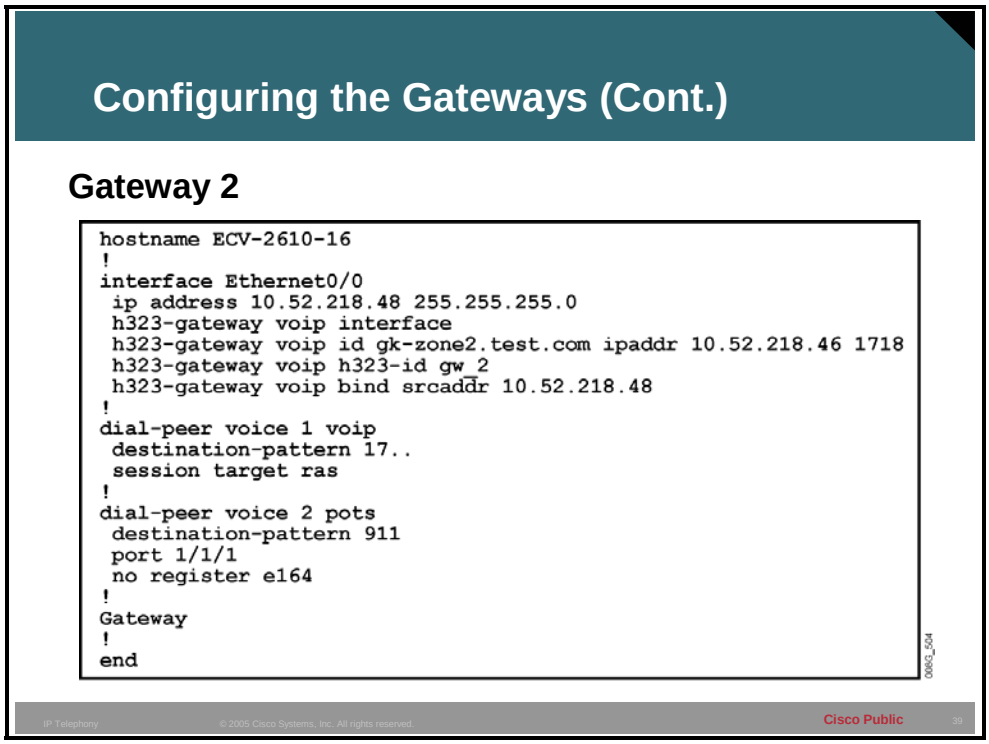
The figure illustrates the scenario on which the gateway configurations are based.

 Copyright © 2005, Cisco Systems, Inc.



To use a gatekeeper, the user must complete the following three tasks on the gateway:

1. Enable the gateway with the **gateway** command.
2. Configure the relationship with the gatekeeper. This requires three interface subcommands:
   - **h323-gateway voip interface:** Tells the router that this interface should be enabled for H.323 packet processing.
   - **h323-gateway voip id:** Identifies the ID of the gatekeeper.
   - **h323-gateway voip h323-id:** Configures the ID of this router. When the router registers with the gatekeeper, the gatekeeper recognizes the gateway by this ID.
3. Configure a dial peer to use the gatekeeper with the **ras** parameter on the dial peer subcommand **session target**.



You can use other interface subcommands, one of which is illustrated in the configuration for both gateways. This command performs the following function:

- **h323-gateway voip tech-prefix 1#:** Registers a technology prefix
- **h323-gateway voip bind srcaddr 10.52.218.48:** Sets the source address in H.323 packets

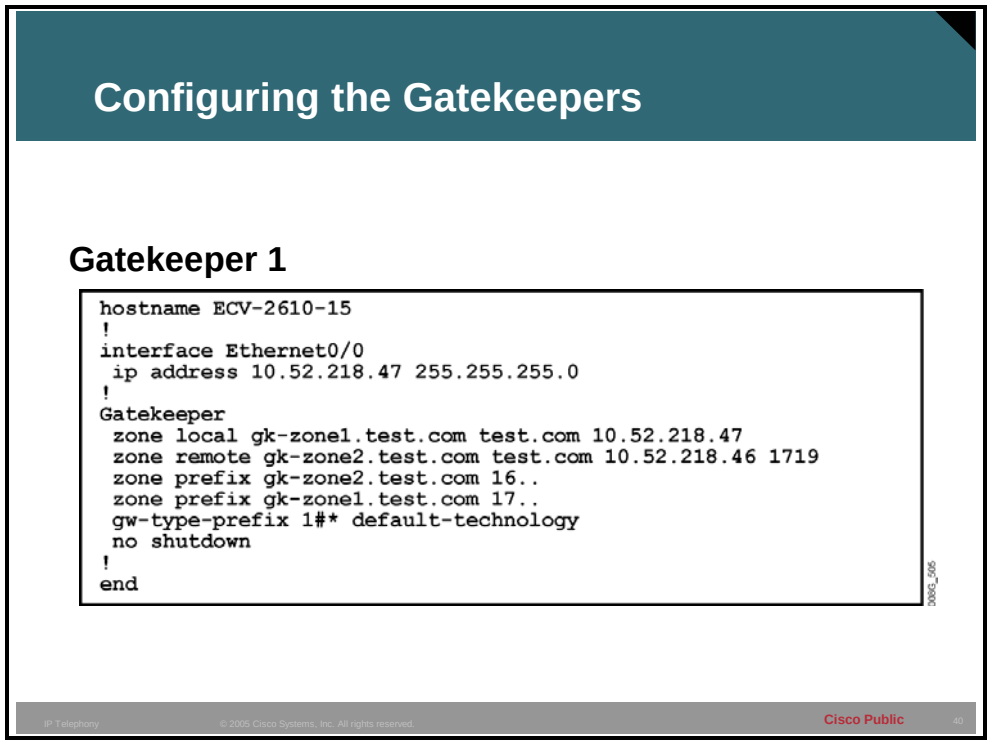
A technology prefix advises the gatekeeper that this gateway can handle type 1# destinations. For routing purposes, a technology prefix may be assigned to a multimedia type, such as video. By registering type 1# support, the gateway supports the video applications.

In the dial peer, the **no register e164** subcommand causes the gateway not to register the destination pattern when communicating with the gatekeeper. When the dial peer does not register its prefix, the dial peer requires an alternative mechanism for the gatekeeper to acquire this information.

 Copyright © 2005, Cisco Systems, Inc.

Configuring H.323 Gatekeepers

This topic illustrates the gatekeeper configuration for a two-zone, two-gatekeeper scenario.



The gatekeeper application is enabled with the **gatekeeper** command.

For this example, the gateways are configured to withhold their E.164 addresses, so the gatekeepers must define the addresses locally. This is done with the **zone prefix** command. In the example, each gatekeeper has two **zone prefix** commands, the first pointing to the other gatekeeper and the second pointing to the local zone (meaning the prefix is in the local zone). The **zone prefix** command that points to itself is configured with the name of the gateway used to direct traffic to the destination. The address of the gateway is not required, because it is determined automatically when the gateway registers. The commands in the figure perform the following functions:

- **zone local gk-zone1.test.com test.com 10.52.218.47:** Defines the ID of the local gatekeeper
- **zone remote gk-zone2.test.com test.com 10.52.218.46 1719:** Defines the identity and IP address of neighboring gatekeepers

Configuring the Gatekeepers (Cont.)

Gatekeeper 2

```
hostname ECV-2610-14
!
interface Ethernet0/0
 ip address 10.52.218.46 255.255.255.0
!
Gatekeeper
 zone local gk-zone2.test.com test.com 10.52.218.46
 zone remote gk-zone1.test.com test.com 10.52.218.47 1719
 zone prefix gk-zone2.test.com 16..
 zone prefix gk-zone1.test.com 17..
 gw-type-prefix 1#* default-technology
 no shutdown
!
end
```

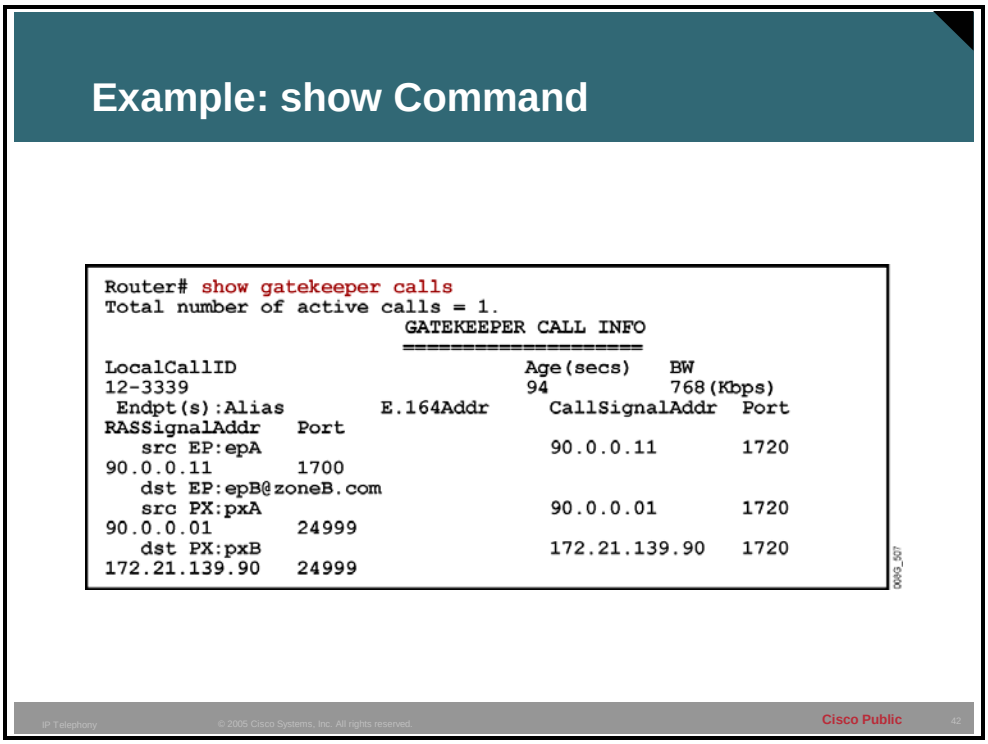
IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 41

Because the gateways register their technology prefixes, the gatekeeper does not need to be configured. If a technology prefix is required, the **gw-type-prefix** defines a technology prefix, and can manually update technology prefix knowledge in the gatekeeper. In the example configuration in this figure, the gatekeeper attempts to define a technology prefix as the default with the command **gw-type-prefix 1#* default-technology**. Any unknown destination is assumed to be of the default technology type, and calls are forwarded to any gateway that registered the default technology type.

 Copyright © 2005, Cisco Systems, Inc.

Monitoring and Troubleshooting

The **show** and **debug** commands are valuable when examining the status of the H.323 components and during troubleshooting. This topic lists many **show** and **debug** commands that are used to provide support for monitoring and troubleshooting H.323.



Following are some of the **show** commands used for H.323:

- **show call active voice** [**brief**]: Displays the status, statistics, and parameters for all active voice calls
- **show call history voice** [**last** *n*|**record**|**brief**]: Displays call records from the history buffer
- **show gateway**: Displays the current status of the H.323 gateway configured in the router
- **show gatekeeper calls**: Displays the active calls for which the gatekeeper is responsible (illustrated in the figure)
- **show gatekeeper endpoints**: Lists the registered endpoints with ID and supported prefixes
- **show gatekeeper gw-type-prefix**: Displays the current technology prefix table
- **show gatekeeper status**: Displays the current status of the gatekeeper
- **show gatekeeper zone prefix**: Displays the gateways and their associated E.164 prefixes
- **show gatekeeper zone status**: Displays the status of the connections to gateways in the local zone and the status of the connections to gatekeepers in other zones

Selected debug Commands

The **debug** commands used for H.323 include the following:

- **debug voip ccapi inout:** Shows every interaction with the call control application programming interface (API) on the telephone interface and the VoIP side. Monitoring the

debug voip ccapi inout command output allows users to follow the progress of a call from the inbound interface or VoIP peer to the outbound side of the call. Because this debug is highly active, use it sparingly in a live network.

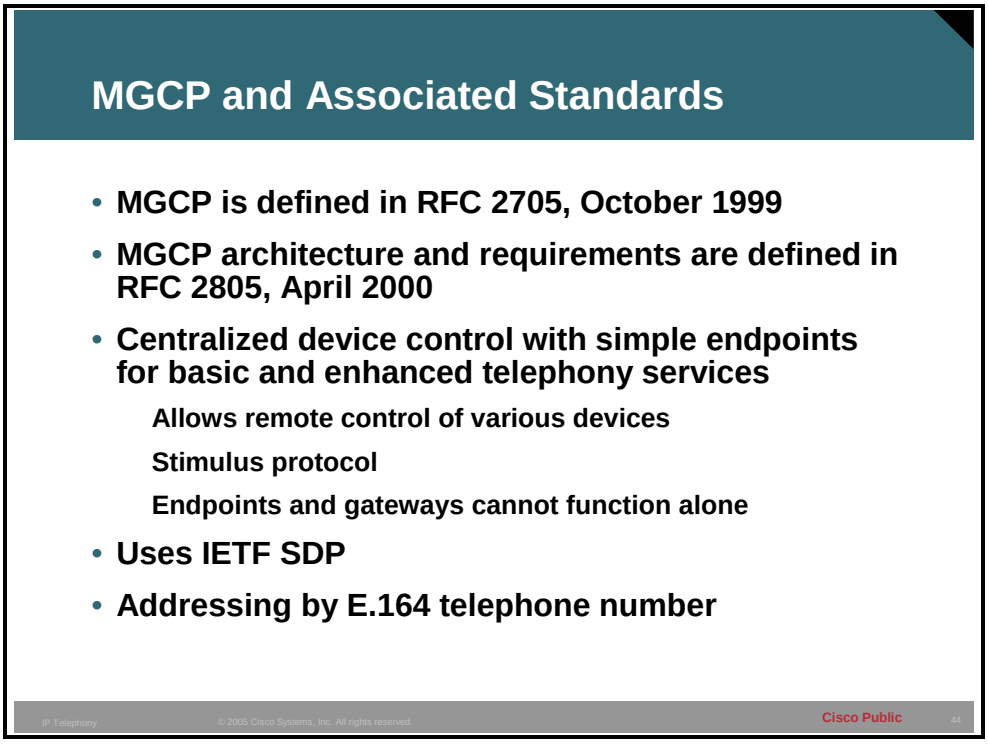
- **debug cch323 h225:** Traces the transitions in the H.225.0 state machine during the establishment of the call control channel. The first step in establishing a relationship between any two components is to bring up the call control channel. Monitoring the output of the **debug cch323 h225** command allows users to follow the progress and determine if the channel is established correctly.
- **debug cch323 h245**: Traces the state transitions in the H.245 state machine during the establishment of the H.245 control channel. Monitoring the output of the **debug cch323 h245** command allows users to follow the progress to see if the channel is established correctly.
- **debug cch323 ras**: Traces the state transition in the establishment of the RAS control channel. Monitoring the output of the **debug cch323 ras** command allows users to determine if the channel is established correctly.
- **debug h225 asn1**: Displays an expansion of the ASN.1-encoded H.225.0 messages. When investigating VoIP peer association problems, this **debug** command helps users monitor the activity of the call-signaling channel. Because H.225.0 encapsulates H.245, this is a useful approach for monitoring both H.225.0 and H.245.
- **debug h225 events**: Similar to the ASN.1 version of the command but does not expand the ASN.1. Debugging events usually imposes a lighter load on the router.
- **debug h245 asn1**: Similar to the H.225.0 variant except that it displays only the H.245 messages.
- **debug h245 events**: Similar to the H.225.0 variant except that it displays only the H.245 messages.

 Copyright © 2005, Cisco Systems, Inc.

Configuring MGCP

MGCP and Its Associated Standards

MGCP controls telephony gateways from a centralized call agent. This topic describes MGCP and identifies its associated standards.

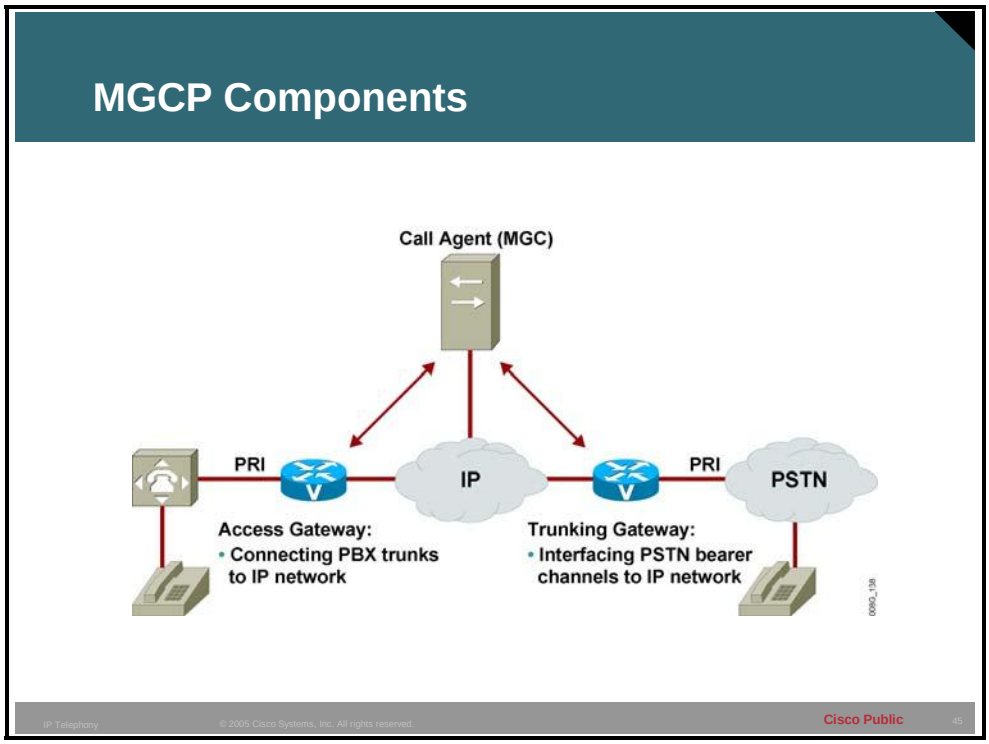


MGCP defines an environment for controlling telephony gateways from a centralized call control component known as a call agent. An MGCP gateway handles the translation of audio between the telephone SCN and the packet-switched network of the Internet. Gateways interact with a call agent that performs signaling and call processing.

IETF RFC 2705 defines MGCP. RFC 2805 defines an architecture for MGCP. These IETF standards describe MGCP as a centralized device control protocol with simple endpoints. The MGCP protocol allows a central control component, or call agent, to remotely control various devices. This protocol is referred to as a stimulus protocol because the endpoints and gateways cannot function alone. MGCP incorporates the IETF SDP to describe the type of session to initiate.

Basic MGCP Components

MGCP defines a number of components and concepts. You must understand the relationships between components and how the components use the concepts to implement a working MGCP environment. This topic describes the basic MGCP components.



The following components are used in an MGCP environment:

- **Endpoints:** Represent the point of interconnection between the packet network and the traditional telephone network
- **Gateways:** Handle the translation of audio between the SCN and the packet network
- **Call agent:** Exercises control over the operation of a gateway

The figure shows an MGCP environment with all three components.

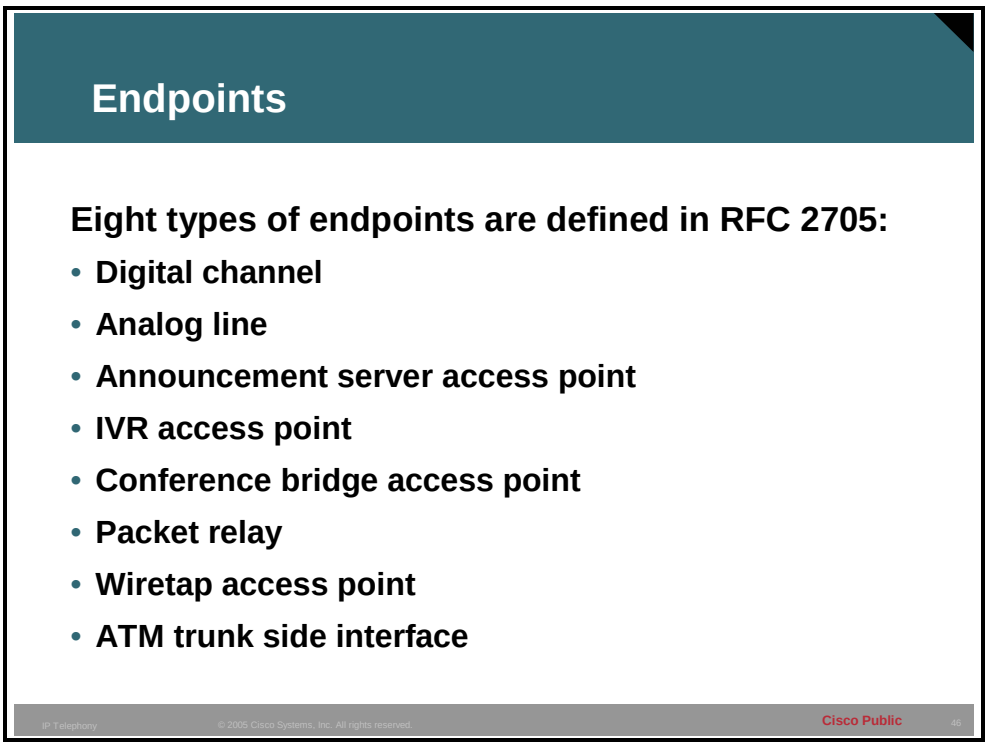
Example: Cisco MGCP Components

Cisco voice gateways can act as MGCP gateways. Cisco CallManager acts as an MGCP call agent.

 Copyright © 2005, Cisco Systems, Inc.

MGCP Endpoints

This topic lists the standard endpoints and defines the way that identifiers are associated with an endpoint.



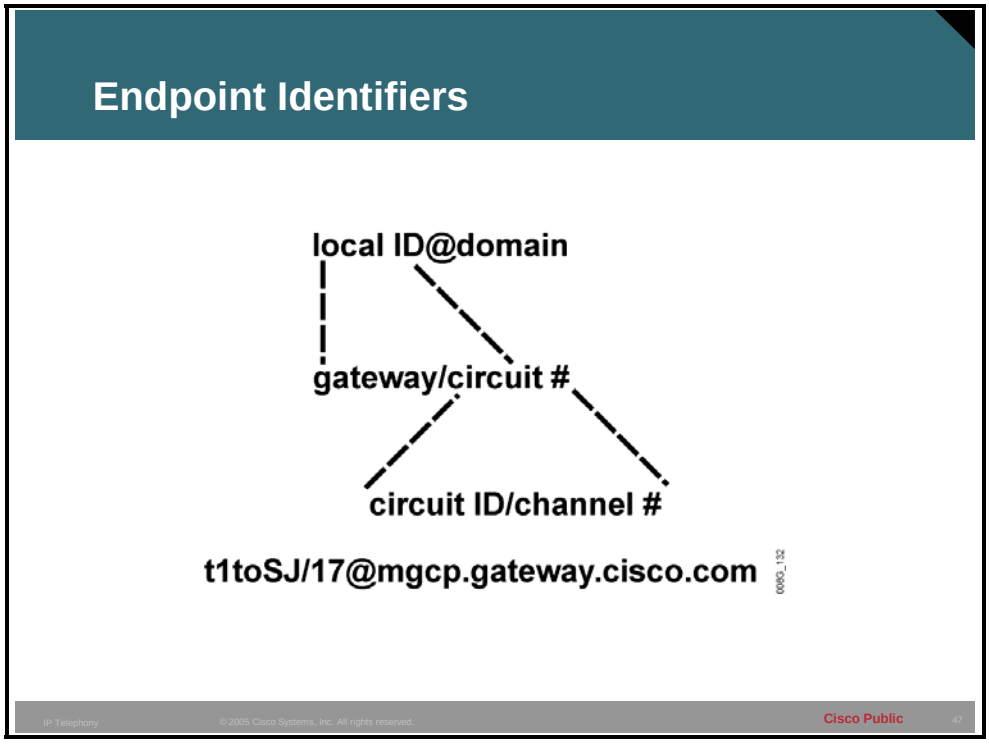
Endpoints represent the point of interconnection between the packet network and the traditional telephone network. Endpoints can be physical, representing an FXS port or a channel in a T1 or E1, or they can be logical, representing an attachment point to an announcement server.

To manage an endpoint, the call agent must recognize the characteristics of an endpoint. To aid in this process, endpoints are categorized into several types. The intent is to configure a call agent to manage a type of endpoint rather than to manage each endpoint individually.

There are several types of endpoints. RFC 2705 defines eight types, as follows:

- **Digital service level zero (DS0):** Represents a single channel (DS0) in the digital hierarchy. A digital channel endpoint supports more than one connection.
- **Analog line:** Represents the client-side interface, such as FXS, or switch-side interface, such as FXO, to the traditional telephone network. An analog line endpoint supports more than one connection.
- **Announcement server access point:** Represents access to an announcement server, for example, to play recorded messages. An announcement server endpoint may have only one connection. Multiple users of the announcement server are modeled to use different endpoints.
- **Interactive voice response (IVR) access point:** Represents access to an IVR service. An IVR endpoint has one connection. Multiple users of the IVR system are modeled to use different endpoints.

- **Conference bridge access point:** Represents access to a specific conference. Each conference is modeled as a distinct endpoint. A conference bridge endpoint supports more than one connection.
- **Packet relay:** Represents access that bridges two connections for interconnecting incompatible gateways or relaying them through a firewall environment. A packet relay endpoint has two connections.
- **Wiretap access point:** Represents access for recording or playing back a connection. A wiretap access point endpoint has one connection.
- **ATM trunk side interface:** Represents a single instance of an audio channel in the context of an ATM network. An ATM interface supports more than one connection.



When interacting with a gateway, the call agent directs its commands to the gateway for the express purpose of managing an endpoint or a group of endpoints. An endpoint identifier, as its name suggests, identifies endpoints.

Endpoint identifiers consist of two parts: a local name of the endpoint in the context of the gateway and the domain name of the gateway itself. The two parts are separated by an “at” sign (@). If the local part represents a hierarchy, the subparts of the hierarchy are separated by a slash. In the graphic, the “local ID” may be representative of a particular “gateway/circuit #,” and the “circuit #”may in turn be representative of a “circuit ID/channel #.”

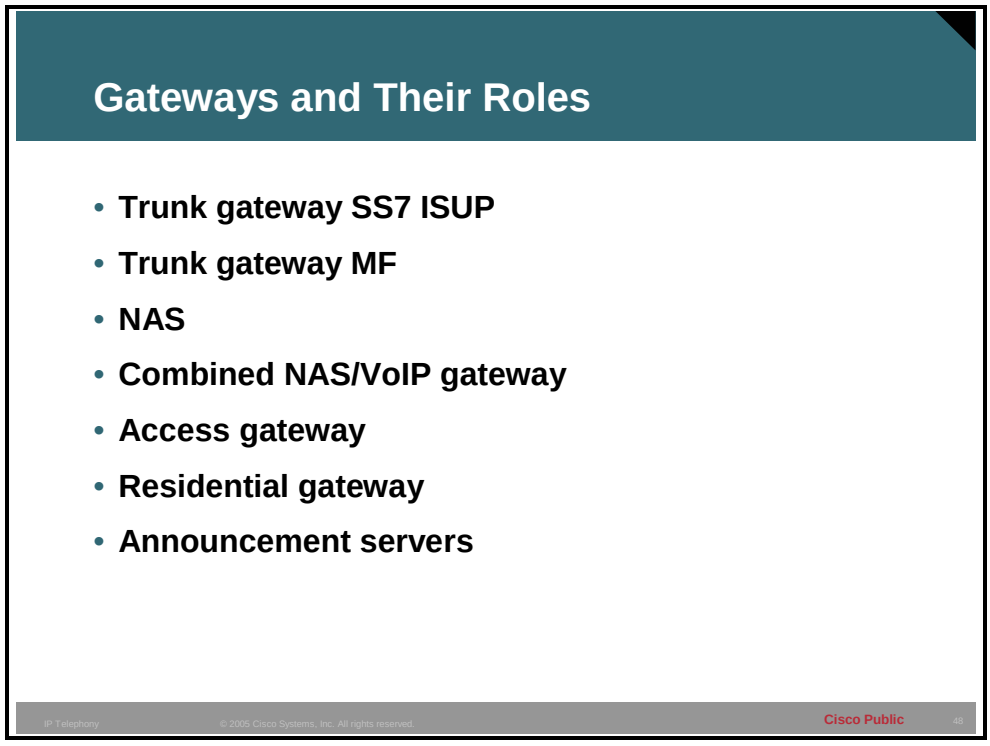
Example: Endpoint Identifiers

In the figure, **mgcp.gateway.cisco.com** is the domain name and **t1toSJ/17** refers to channel 17 in the T1 to San Jose.

 Copyright © 2005, Cisco Systems, Inc.

MGCP Gateways

This topic lists several standard gateways and describes their functions.



Gateways are clustering points for endpoints. Gateways handle the translation of audio between the SCN and the packet network.

Although gateways are implemented in real systems, from a modeling point of view gateways are logical components. In this context, gateways represent a clustering of a single type and profile of endpoints.

A gateway interacts with one call agent only; therefore, it associates with one call agent at a time.

RFC 2705 identifies the following seven types of gateways:

- **Trunk gateway SS7 ISUP:** Supports digital circuit endpoints subject to ISDN signaling
- **Trunk gateway multifrequency (MF):** Typically supports digital or analog circuit endpoints that are connected to a service provider of an enterprise switch that is subject to MF signaling
- **Network access server (NAS):** Supports an interconnect to endpoints over which data (modem) applications are provided
- **Combined NAS/VoIP gateway:** Supports an interconnect to endpoints over which a combination of voice and data access is provided
- **Access gateway:** Supports analog and digital endpoints connected to a PBX
- **Residential gateway:** Supports endpoints connected to traditional analog interfaces

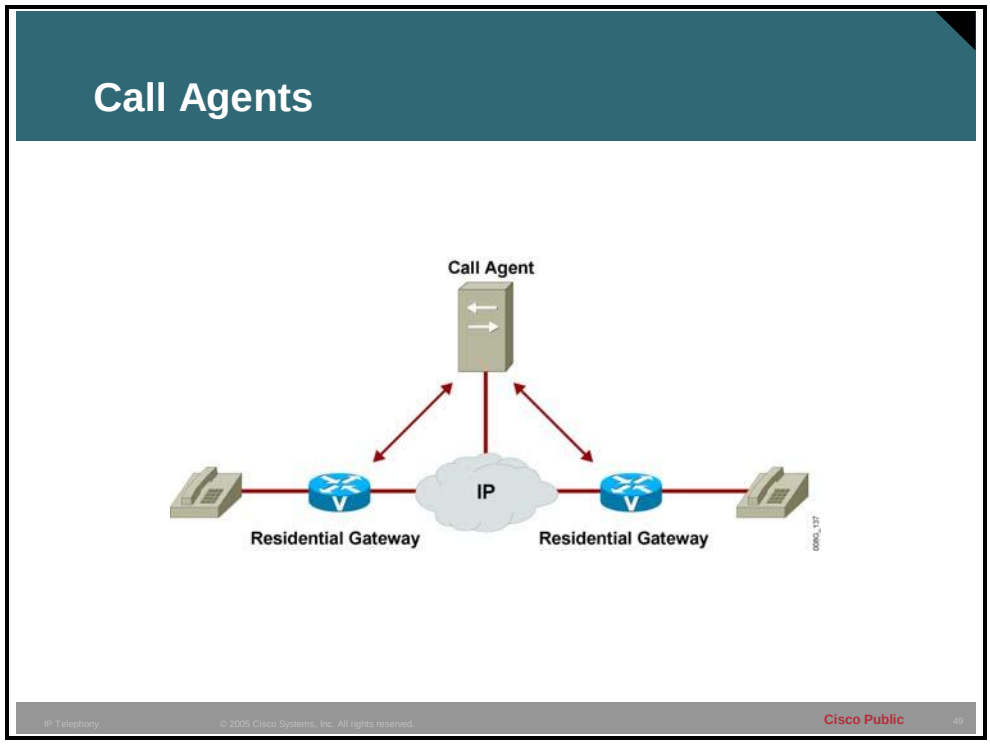
- **Announcement servers:** Supports endpoints that represent access to announcement services

Multiple gateway types, and multiple instances of the same type, can be incorporated into a single physical gateway implementation.

 Copyright © 2005, Cisco Systems, Inc.

MGCP Call Agents

This topic describes how a call agent controls gateways and endpoints.



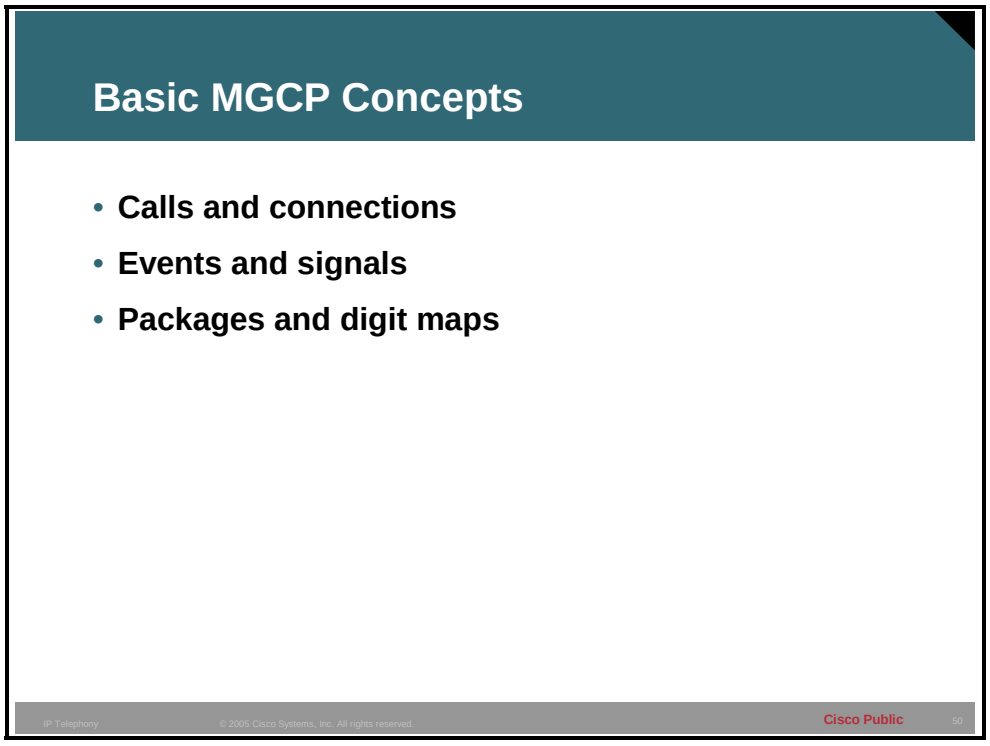
A call agent, or Media Gateway Controller (MGC), represents the central controller in an MGCP environment.

A call agent exercises control over the operation of a gateway and its associated endpoints by requesting that a gateway observe and report events. In response to the events, the call agent instructs the endpoint what signal, if any, the endpoint should send to the attached telephone equipment. This requires a call agent to recognize each endpoint type that it supports and the signaling characteristics of each physical and logical interface that is attached to a gateway.

A call agent uses its directory of endpoints and the relationship that each endpoint has with the dial plan to determine call routing. Call agents initiate all VoIP call legs.

Basic MGCP Concepts

This topic introduces the basic MGCP concepts.



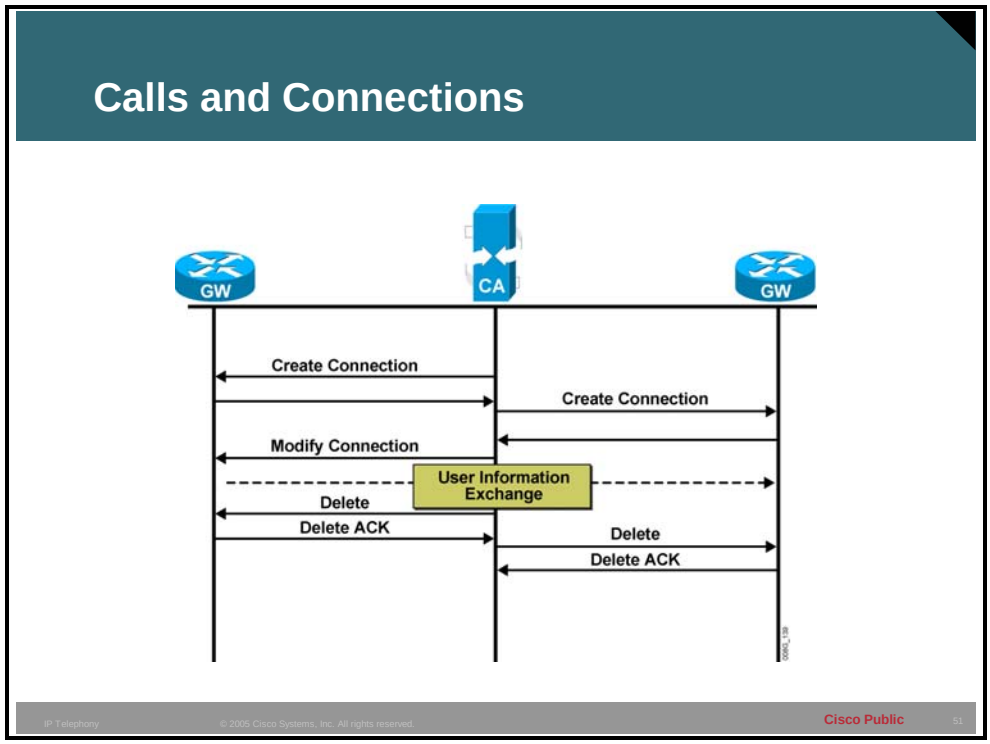
The basic MGCP concepts are listed below:

- **Calls and connections:** Allow end-to-end calls to be established by connecting two or more endpoints
- **Events and signals:** Fundamental MGCP concept that allows a call agent to provide instructions for the gateway
- **Packages and digit maps:** Fundamental MGCP concept that allows a gateway to determine the call destination

 Copyright © 2005, Cisco Systems, Inc.

MGCP Calls and Connections

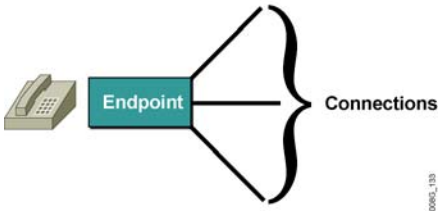
This topic discusses how end-to-end calls are established by connecting multiple endpoints.



End-to-end calls are established by connecting two or more endpoints. To establish a call, the call agent instructs the gateway that is associated with each endpoint to make a connection with a specific endpoint or an endpoint of a particular type. The gateway returns the session parameters of its connection to the call agent, which in turn sends these session parameters to the other gateway. With this method, each gateway acquires the necessary session parameters to establish RTP sessions between the endpoints. All connections that are associated with the same call will share a common call ID and the same media stream.

At the conclusion of a call, the call agent sends a delete connection request to each gateway.

Multipoint Calls



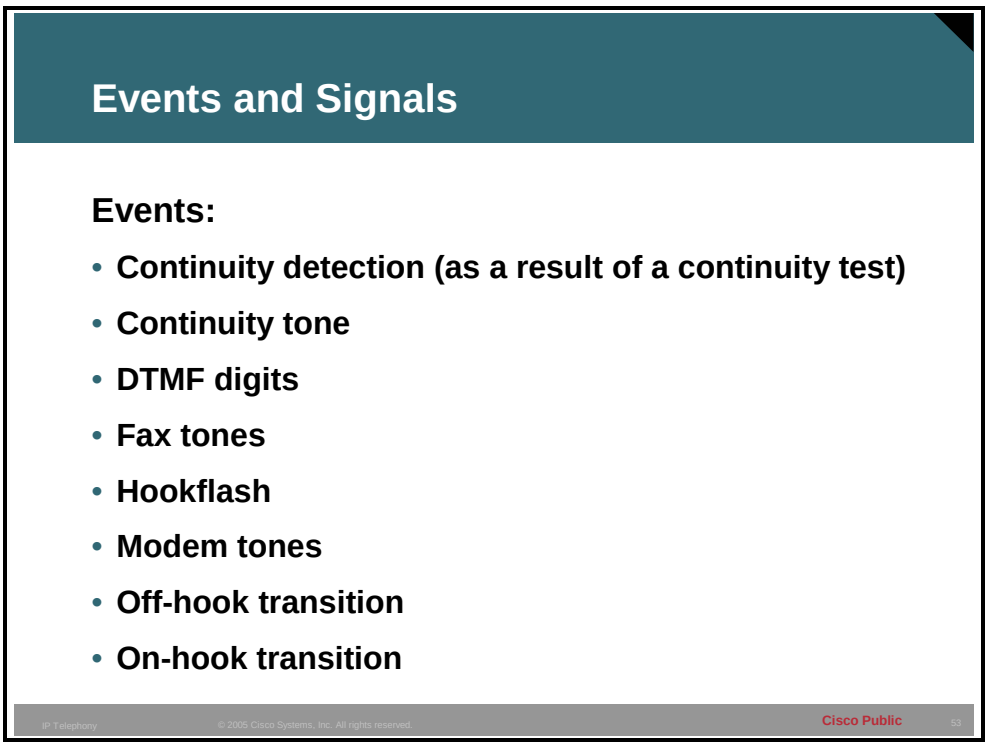
IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 52

To create a multipoint call, the call agent instructs an endpoint to create multiple connections. The endpoint is responsible for mixing audio signals.

 Copyright © 2005, Cisco Systems, Inc.

MGCP Events and Signals

This topic describes how a call agent uses events and signals to provide instruction to the gateway.

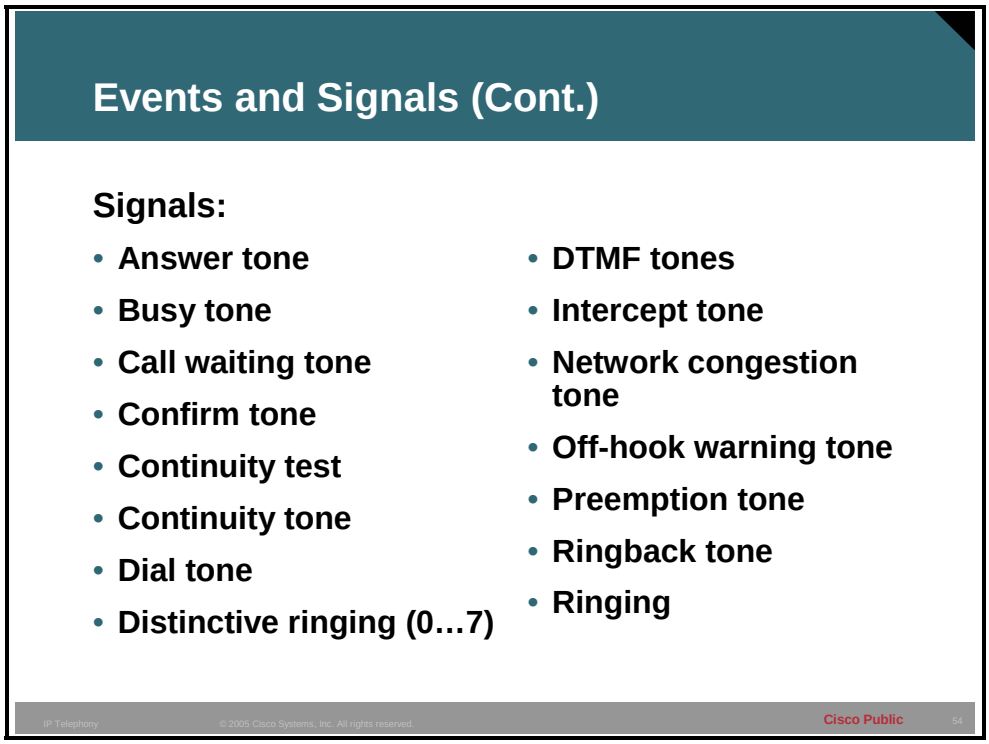


Events and signals help the call agent instruct the gateway on the call control and signaling procedures. The call agent has complete control over the gateway. The call agent informs the gateway of every action to take, including the following:

- Events that the gateway monitors on an endpoint
- What to do if an event occurs
- When to generate a notification to the call agent

An example of an event on an analog line is an off-hook condition. Using signals, the call agent requests that the gateway provide dial tone upon observing the off-hook event.

The figure lists examples of events used in MGCP environments. Events and signals are assigned simple, case-insensitive codes; for example, the code for an off-hook transition event is “hd”, and the code for the dial tone signal is “dl”.

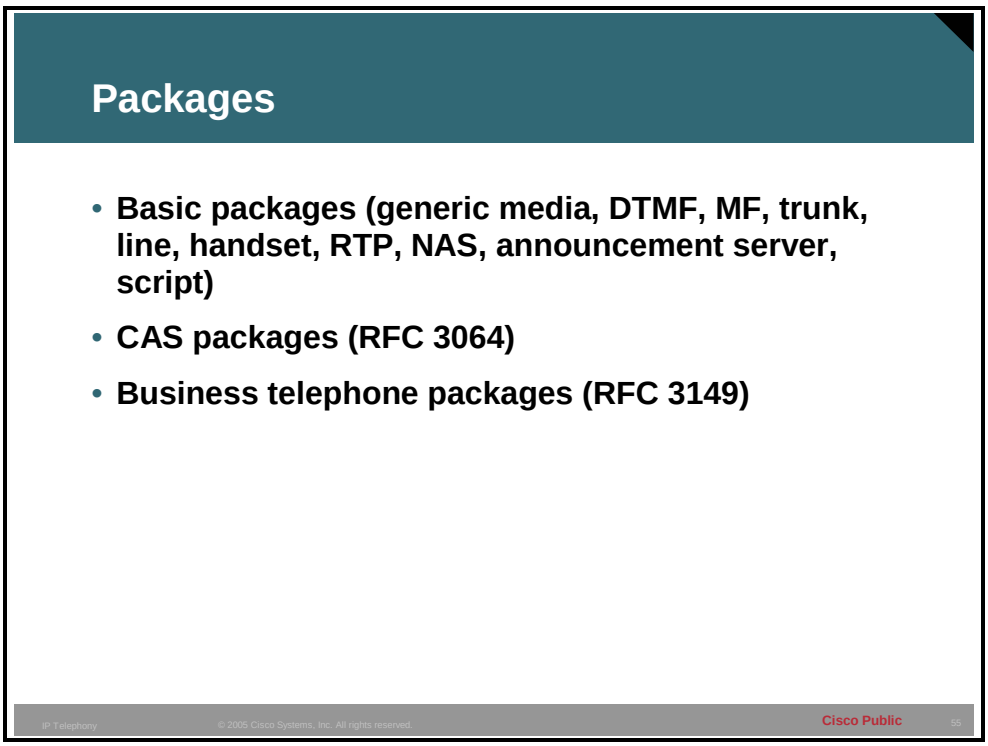


The figure gives examples of signals used in MGCP environments.

 Copyright © 2005, Cisco Systems, Inc.

MGCP Packages

This topic describes how events and signals are packaged in gateways and how they are used by digit maps and gateways.



Packages are collections of commonly occurring events and signals that are relevant to a specific type of endpoint; for example, “off hook,” an event, and “dial tone,” a signal, are unique to managing subscriber lines. Consequently, they are associated with the “line” package.

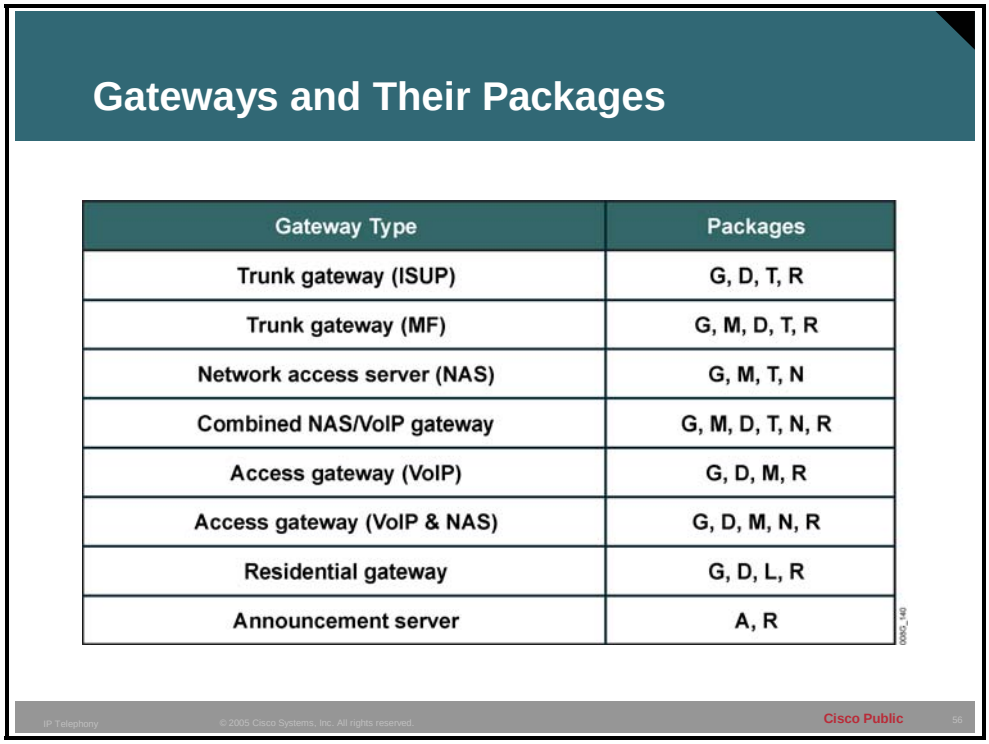
Each event and signal is placed in one particular package. The name of an event or signal acquires the code assigned to the package. The package code and the event code are separated by a slash. Therefore, the full specified name for the off-hook transition event is “L/hd”.

RFC 2705 defines packages, as shown in the table.

Packages

Reference	Package Name
G	Generic media
M	Multifrequency
D	DTMF
T	Trunk
N	Network access server
L	Line
A	Announcement server
R	RTP
H	Handset
S	Script

RFC 3064 defines CAS packages, while RFC 3149 defines business telephone packages. The CAS packages contain definitions for various CAS media gateways, including support for emulated E&M interfaces, direct inward dialing (DID) interfaces, FXO interfaces, and others. Business telephone packages contain support for business telephone functions (and buttons) such as hold, transfer, forward, conference, and others.

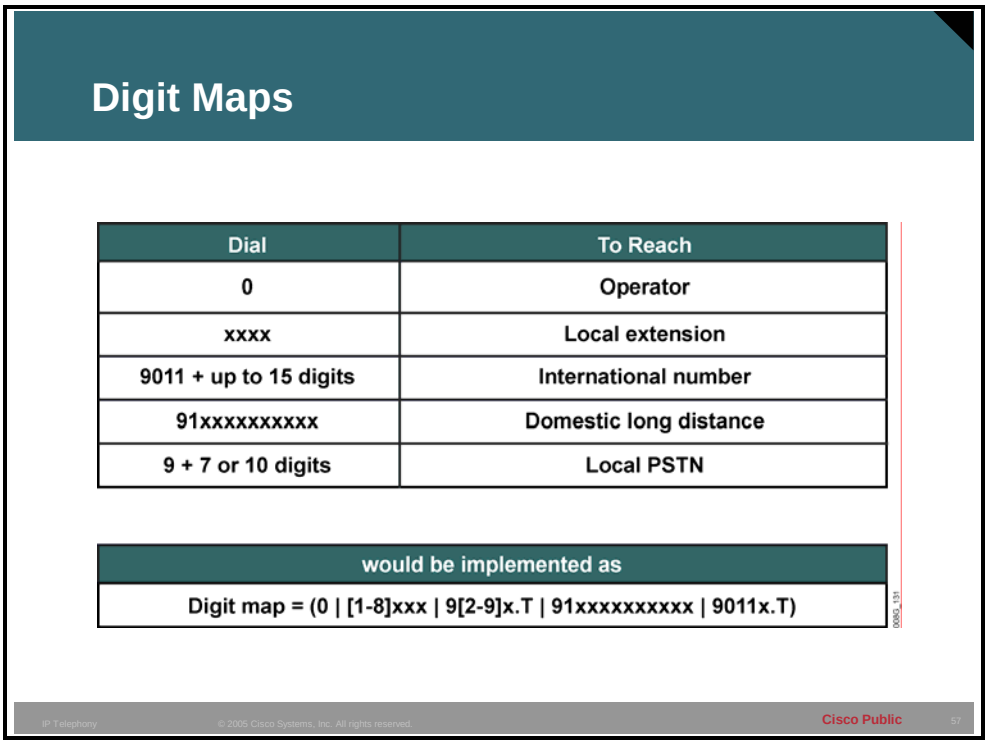


Packages cluster events and signals by their relevance to various types of endpoints. Conceptually, gateways also cluster endpoints of different types. It is appropriate then to associate packages with gateways. The table in the figure lists the gateways and identifies the packages that are associated with them.

 Copyright © 2005, Cisco Systems, Inc.

MGCP Digit Maps

This topic describes the function of digit maps in MGCP.



A digit map is a specification of the dial plan. When you download a digit map to a gateway for use on an endpoint or a group of endpoints, a digit map allows the gateway to collect digits until the gateway either finds a match or concludes that the dialed digits could not possibly match the specification. When either condition occurs, the gateway notifies the call agent.

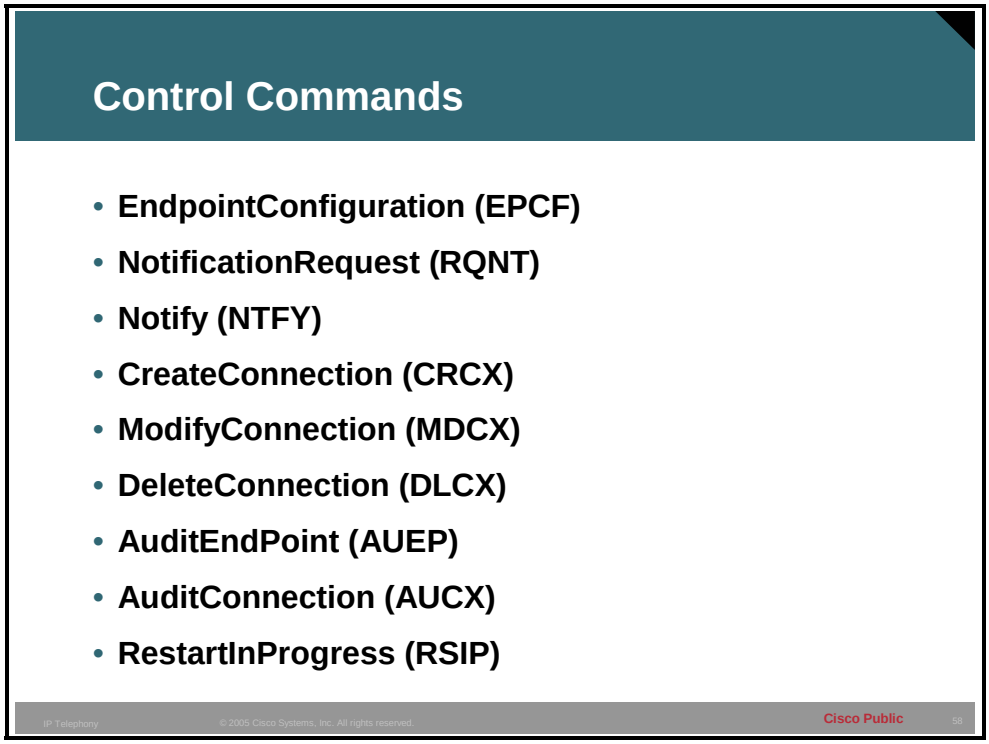
Without a digit map, a gateway must notify the call agent on each digit dialed, which places a heavy burden on the call agent and the network connecting the gateway and call agent. The figure shows an example of a digit map.

Example: Digit Map Translation

According to the figure, if a user dials 9 as the first digit, three of the possible digit maps may be invoked, depending on the next digit dialed. If the next digit is a 1, then the user is dialing domestic long distance, and the digit map 91*xxxxxxxxx* will be used.

MGCP Control Commands

MGCP defines nine messages to control and manage endpoints and their connections. This topic describes these control messages.



A call agent uses control commands or messages to direct its gateways and their operational behavior. Gateways use the following control commands in responding to requests from a call agent and notifying the call agent of events and abnormal behavior:

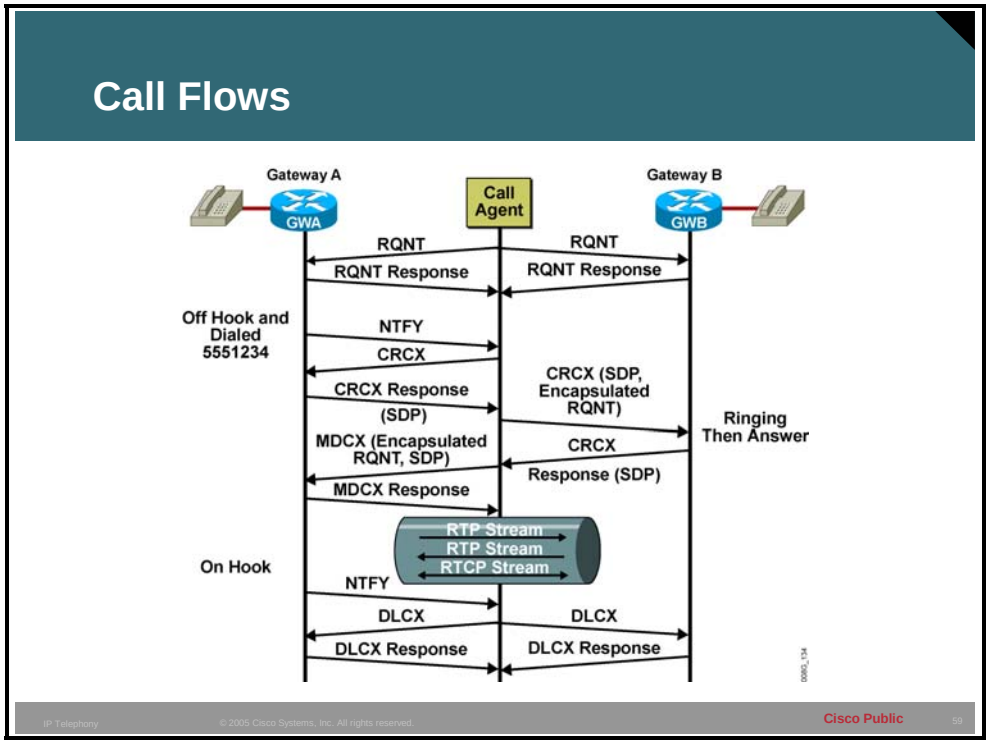
- **EndpointConfiguration (EPCF):** Identifies the coding characteristics of the endpoint interface on the line side of the gateway. The call agent issues the command.
- **NotificationRequest (RQNT):** Instructs the gateway to watch for events on an endpoint and the action to take when they occur. The call agent issues the command.
- **Notify (NTFY):** Informs the call agent of an event for which notification was requested. The gateway issues the command.
- **CreateConnection (CRCX):** Instructs the gateway to establish a connection with an endpoint. The call agent issues the command.
- **ModifyConnection (MDCX):** Instructs the gateway to update its connection parameters for a previously established connection. The call agent issues the command.
- **DeleteConnection (DLCX):** Informs the recipient to delete a connection. The call agent or the gateway can issue the command. The gateway or the call agent issues the command to advise that it no longer has the resources to sustain the call.
- **AuditEndpoint (AUEP):** Requests the status of an endpoint. The call agent issues the command.
- **AuditConnection (AUCX):** Requests the status of a connection. The call agent issues the command.

 Copyright © 2005, Cisco Systems, Inc.

- **RestartInProgress (RSIP):** Notifies the call agent that the gateway and its endpoints are removed from service or are being placed back in service. The gateway issues the command.

Call Flows

This topic illustrates and explains the interactions between a call agent and its associated gateways.



The figure illustrates a dialog between a call agent and two gateways. Although the gateways in this example are both residential gateways, the following principles of operation are the same for other gateway types:

1. The call agent sends a notification request (RQNT) to each gateway. Because they are residential gateways, the request instructs the gateways to wait for an off-hook transition (event). When the off-hook transition event occurs, the call agent instructs the gateways to supply dial tone (signal). The call agent asks the gateway to monitor for other events as well. By providing a digit map in the request, the call agent can have the gateway collect digits before it notifies the call agent.

2. The gateways respond to the request. At this point, the gateways and the call agent wait for a triggering event.

3. A user on gateway A goes off hook. As instructed by the call agent in its earlier request, the gateway provides dial tone. Because the gateway is provided with a digit map, it begins to collect digits (as they are dialed) until either a match is made or no match is possible. For the remainder of this example, assume that the digits *match* a digit map entry.

4. Gateway A sends a notify (NTFY) to the call agent to advise the call agent that a requested event was observed. The notify identifies the endpoint, the event, and, in this case, the dialed digits.

5. After confirming that a call is possible based on the dialed digits, the call agent instructs gateway A to create a connection (CRCX) with its endpoint.

 Copyright © 2005, Cisco Systems, Inc.

6. The gateway responds with a session description if it is able to accommodate the connection. The session description identifies at least the IP address and UDP port for use in a subsequent RTP session. The gateway does not have a session description for the remote side of the call, and the connection enters a wait state.

7. The call agent prepares and sends a connection request to gateway B. In the request, the call agent provides the session description obtained from gateway A. The connection request is targeted to a single endpoint—if only one endpoint is capable of handling the call—or to any one of a set of endpoints. The call agent also embeds a notification request that instructs the gateway about the signals and events that it should now consider relevant. In this example, in which the gateway is residential, the signal requests ringing and the event is an off-hook transition.

Note The interaction between gateway B and its attached user has been simplified.

---

8. Gateway B responds to the request with its session description. Notice that gateway B has both session descriptions and recognizes how to establish its RTP sessions.

9. The call agent relays the session description to gateway A in a modify connection request (MDCX). This request may contain an encapsulated notify request that describes the relevant signals and events at this stage of the call setup. Now gateway A and gateway B have the required session descriptions to establish the RTP sessions over which the audio travels.

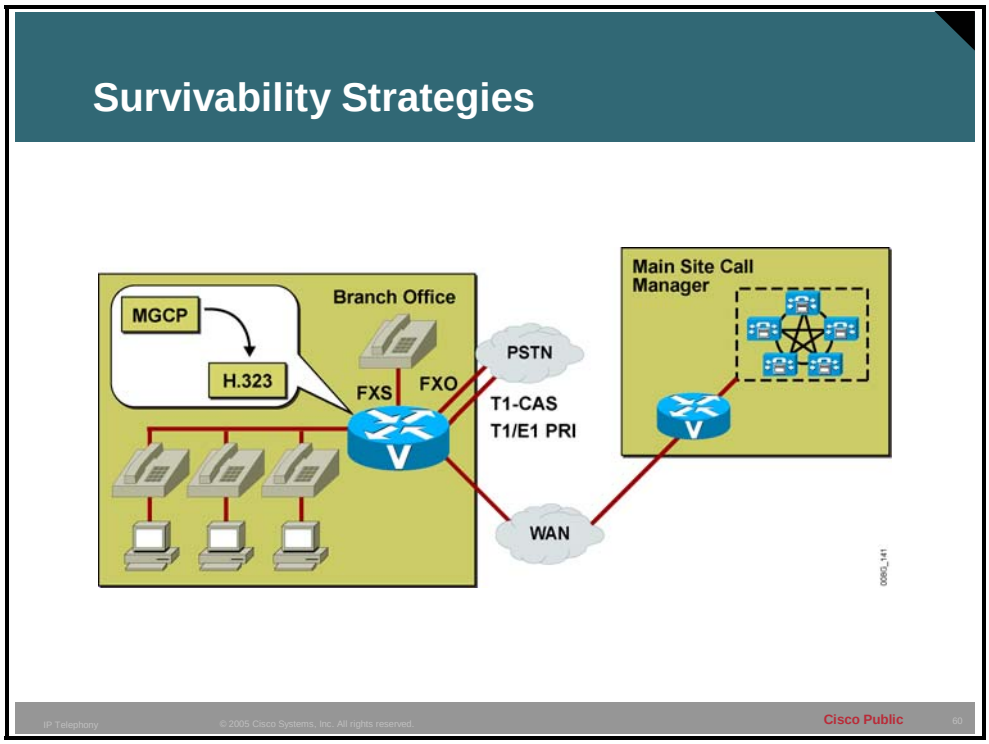
10. At the conclusion of the call, one of the endpoints recognizes an on-hook transition. In the example, the user on gateway A hangs up. Because the call agent requested the gateways to notify in such an event, gateway A notifies the call agent.

11. The call agent sends a delete connection (DLCX) request to each gateway.

12. The gateways delete the connections and respond.

Survivability Strategies

Maintaining high availability in an MGCP environment requires a design that accommodates the failure of a call agent. This topic describes two strategies for managing the loss of a call agent.



In the MGCP environment, the call agent controls all call setup processing on the IP and the telephony sides of a gateway. Because a gateway is associated with only one call agent at a time, if that call agent fails or is inaccessible for any reason, the gateway and its endpoints are left uncontrolled and, for all practical purposes, useless. Cisco Systems has developed two methods to handle lost communication between a call agent and its gateways: MGCP switchover and switchback and MGCP gateway fallback. These features operate in the following manner:

- **MGCP switchover and switchback:** MGCP switchover permits the use of redundant MGCP call agents. This feature requires two or more Cisco CallManager servers to operate as MGCP call agents. One Cisco CallManager server becomes the primary server and functions as the MGCP call agent. The other Cisco CallManager servers remain available as backup servers.

  The MGCP gateway monitors MGCP messages sent by the Cisco CallManager server. If traffic is undetected, the gateway transmits keepalive packets to which the Cisco CallManager server responds. If the gateway does not detect packets from the Cisco CallManager for a specified period, it tries to establish a new connection with a backup Cisco CallManager server.

  You can configure a Cisco voice gateway to reestablish connection with the primary Cisco CallManager server when it becomes available again. This is the switchback function.

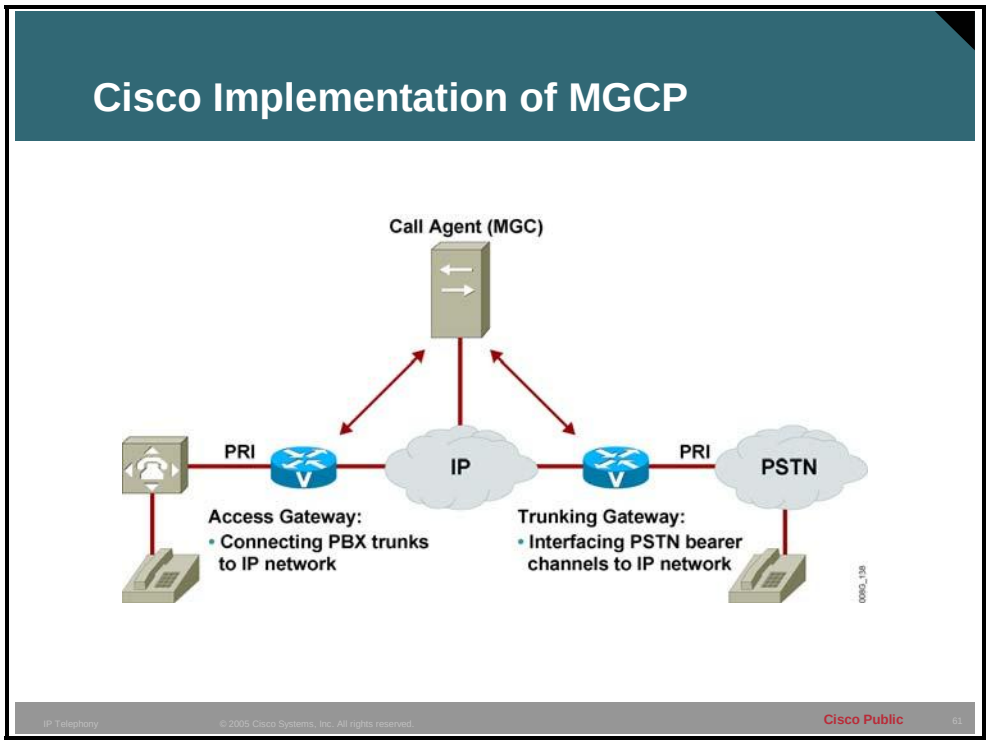
 Copyright © 2005, Cisco Systems, Inc.

- **MGCP gateway fallback:** MGCP gateway fallback is a feature that improves the reliability of MGCP branch networks. A WAN link connects the MGCP gateway at the remote site to the Cisco CallManager at the central sites (the MGCP call agent). If the WAN link fails, the fallback feature keeps the gateway working as an H.323 gateway.

  MGCP gateway fallback works in conjunction with the Survivable Remote Site Telephony (SRST) feature. SRST allows Cisco gateways and routers to manage connections temporarily for Cisco IP Phones when a connection to a Cisco CallManager is unavailable.

Cisco Implementation of MGCP

This topic describes how Cisco implements MGCP.



Cisco provides support for MGCP gateways and the call agent in the following way:

- **Gateways:** Cisco implements MGCP trunk gateway and residential gateway support in the following devices:
  - Cisco voice-enabled routers (first available in Cisco IOS Release 12.1)
  - Cisco PGW 2200 PSTN gateways
  - Cisco Voice Gateway 224 (VG224)
  - Voice-enabled AS5*xx*0 access servers
  - BTS 10200 Softswitch

Note	Cisco CallManager interworking requires Cisco IOS Release 12.2.

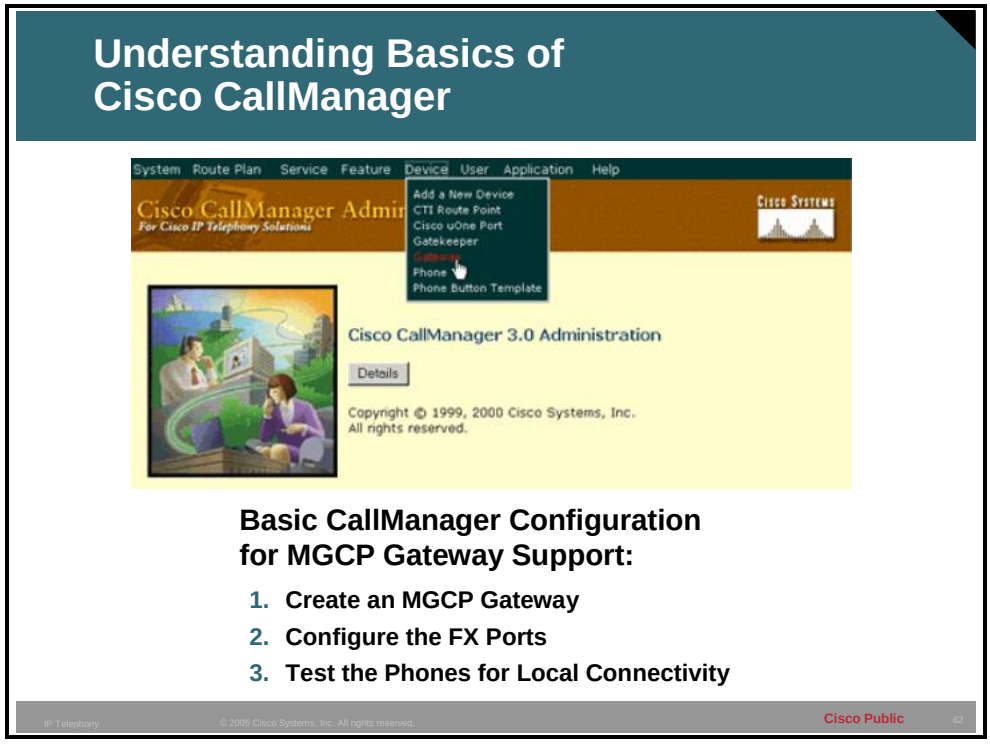
- **Call agent:** Cisco implements call agent support in the following applications:
  - Cisco CallManager
  - BTS 10200 Softswitch

Note	Residential gateway and trunk gateway support does *not* include all analog and digital signaling types on the telephone interfaces. Check Cisco.com for an up-to-date list.

 Copyright © 2005, Cisco Systems, Inc.

Understanding Basics of Cisco CallManager

This topic describes basic configuration of Cisco CallManager to support MGCP gateways. For detailed information regarding configuration of CallManager, refer to the *Cisco IP Telephony* (CIPT) course.



There are three basic tasks for configuring a Cisco CallManager for MGCP. The basic steps for each task are as follows:

- Task 1: Create an MGCP gateway

1. Use the Device Wizard to create an MGCP gateway. Select **Device** > **Gateway**.
2. Click **Add New Gateway**.
3. Select the appropriate gateway type (such as 26*xx*, 36*xx*, or 37*xx*).
4. Click **Next**.
5. For the **MGCP Domain Name**, use the actual host name you have assigned to the gateway. Specify the carrier module that the gateway has installed.
6. Click **Insert**.

- Task 2: Configure the FX ports

1. Identify the voice interface card (VIC) modules installed in the gateway.
2. Click **Update** to activate the changes.
3. The FXO and FXS ports appear at the bottom right of the next screen. These are also referred to as EndPoint Identifiers.
4. Select one of the ports.
5. Select the correct signaling type, **loop** or **ground start**.
6. Configure the parameters of the MGCP Member Configuration screen as required. For example, if this was an FXS port, you would be required to select loop or ground start signaling.
7. Click **Insert**.
8. For FXS ports only, click the **Add DN** text. Add the directory number (phone number) as appropriate, then click **Insert and Close**.
9. Select the **Back To MGCP Configuration** option.
10. Click **Reset Gateway**.

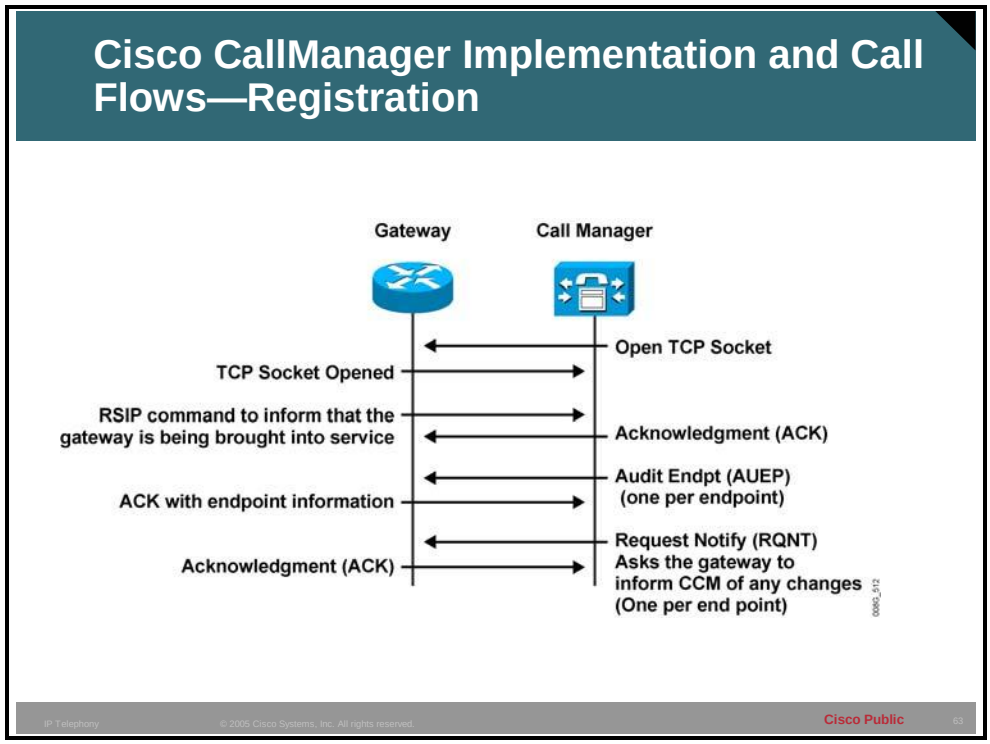
- Task 3: Test the phones for local connectivity

You should now have dial tone on the analog phones connected to the FXS ports. Try dialing from one FXS port to another. You should be able to make and receive calls between these ports.

Registration and FXS Call Flow

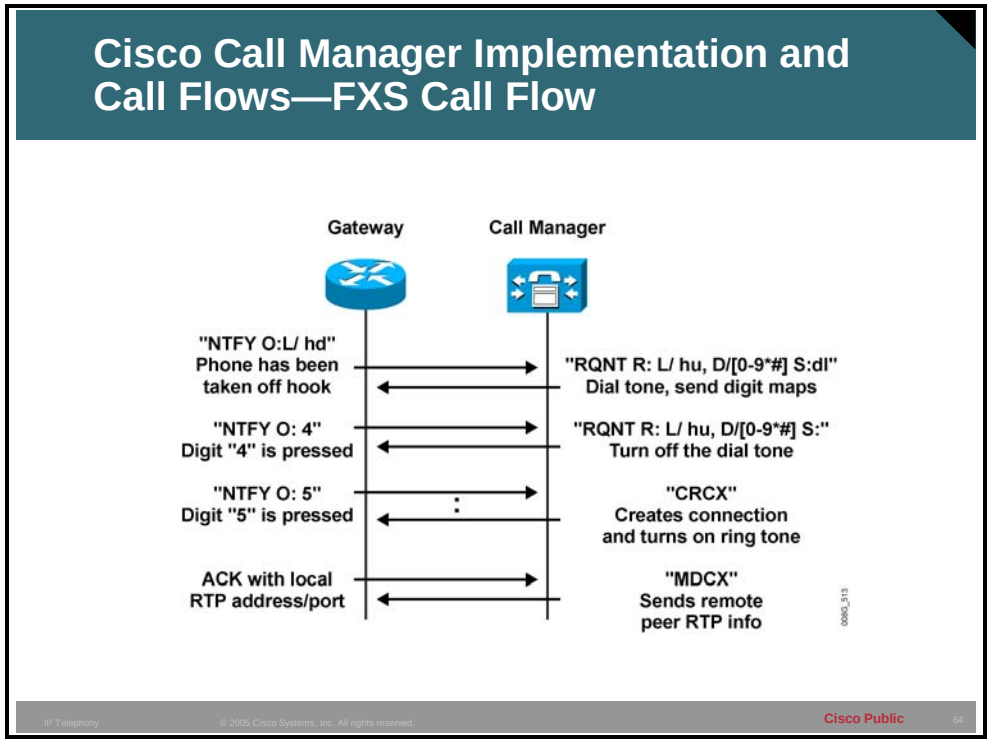
Cisco CallManager implementation of MGCP uses specific command sequences to perform a variety of tasks. The figures are examples of how calls are made and how the gateways are registered.

 Copyright © 2005, Cisco Systems, Inc.



Example: Registration

The figure describes how Cisco CallManager registers voice gateways in its database using MGCP. The ACK commands are standard TCP acknowledgments of the received command.

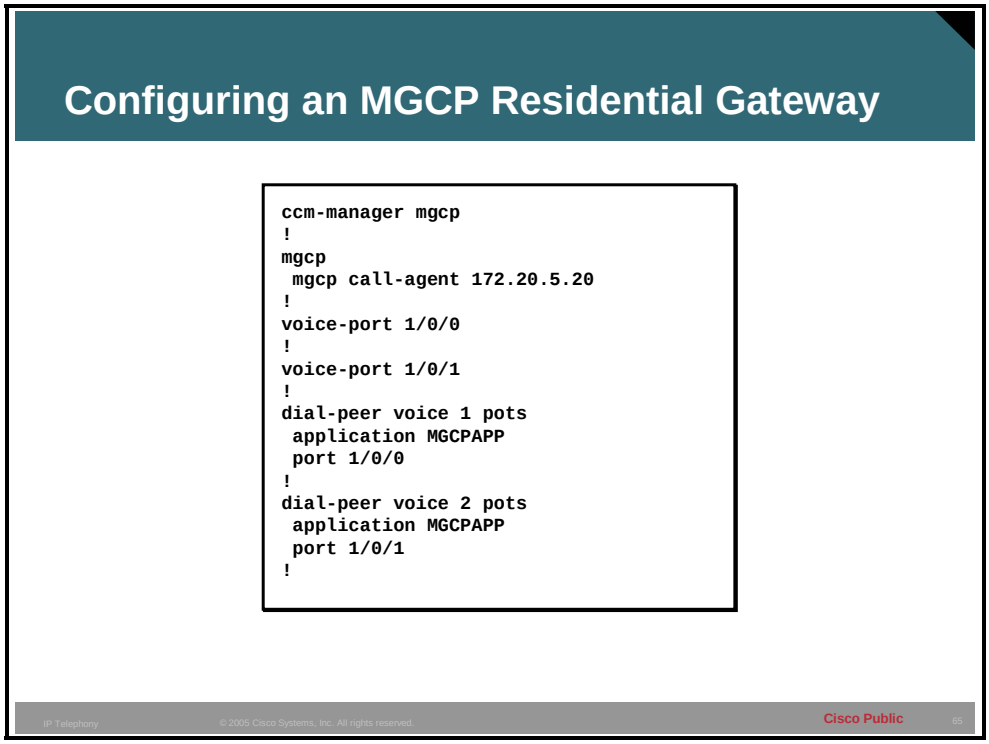


Example: FXS Call Flow

The figure shows a sample FXS call flow (dialing and connection).

Configuring MGCP

This topic illustrates the configuration commands that are required to implement MGCP residential gateway and trunk gateway capabilities on a Cisco router.



The figure highlights the commands required to configure an MGCP residential gateway.

MGCP is invoked with the **mgcp** command. If the call agent expects the gateway to use the default port (UDP 2427), the **mgcp** command is used without any parameters. If the call agent requires a different port, then the port must be configured as a parameter in the **mgcp** command; for example, **mgcp 5036** would tell the gateway to use port 5036 instead of the default port.

At least one **mgcp call-agent** command is required below the **mgcp** command. This command indicates the location of the call agent. The command identifies the call agent by an IP address or a host name. Using a host name adds a measure of fault tolerance in a network that has multiple call agents. When the gateway asks the DNS for the IP address of the call agent, the DNS may provide more than one address, in which case the gateway can use either one. If multiple instances of the **mgcp call-agent** command are configured, the gateway uses the first call agent to respond.

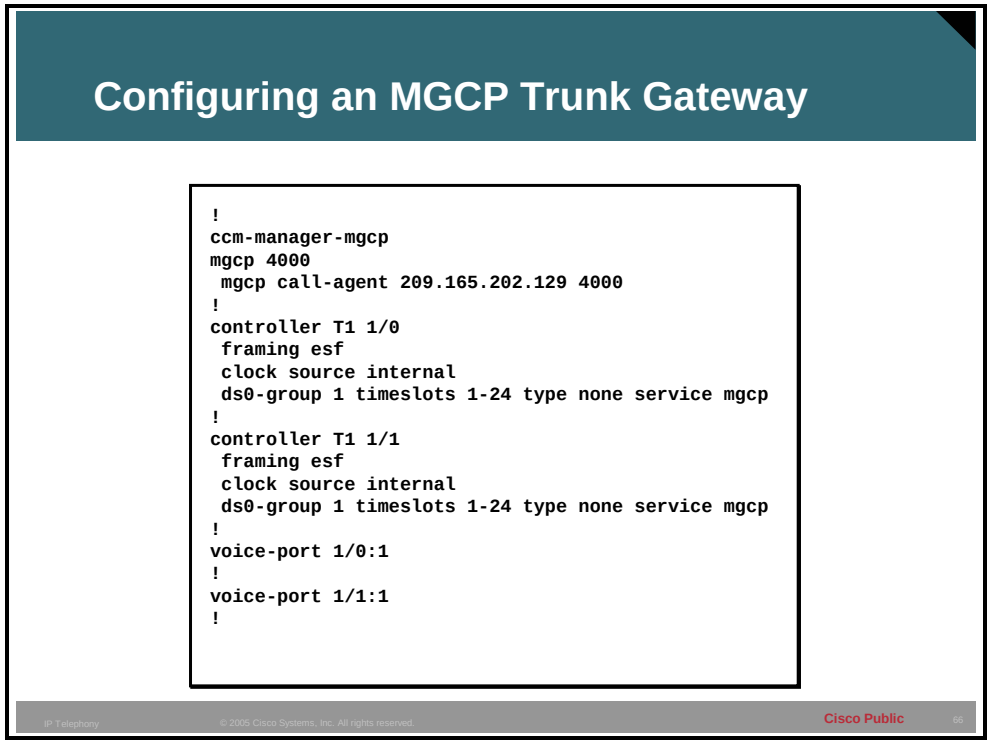
Other **mgcp** subcommands are optional.

Example: MGCP Residential Gateway Configuration

In the example, the configuration identifies the packages that the gateway expects the call agent to use when it communicates with the gateway. The last **mgcp** command specifies the default the gateway uses if the call agent does not share the capabilities. In this example, the command is redundant because the line package is the default for a residential gateway.

 Copyright © 2005, Cisco Systems, Inc.

When the parameters of the MGCP gateway are configured, the active voice ports (endpoints) are associated with the MGCP. Dial peer 1 illustrates an **application mgcpapp** subcommand. This command binds the voice port (**1/0/0** in this case) to the MGCP. Also, notice that the dial peer does not have a destination pattern. A destination pattern is not used because the relationship between the dial number and the port is maintained by the call agent.



The **ccm-manager-mgcp** command is required only if the call agent is a Cisco CallManager.

The second example illustrates the configuration of a trunk gateway.

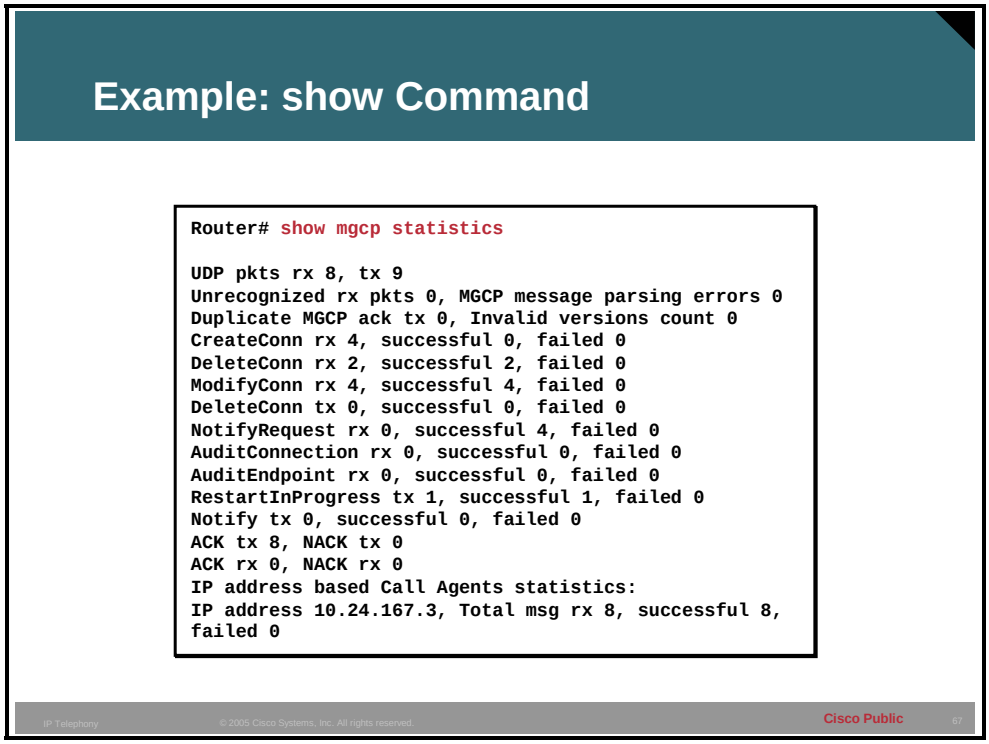
Configuring trunk gateways requires the address or the name of the call agent, which is a requirement common to a residential gateway (RGW). The trunk package is the default for a trunk gateway and does not need to be configured. Again, other parameters are optional.

Example: Configuring MGCP Trunk Gateway

The figure illustrates commands for configuring a trunk gateway. Instead of using the **application mgcpapp** command in a dial peer, a trunk endpoint identifies its association with MGCP using the **service mgcp** parameter in the **ds0-group** controller subcommand. As always in MGCP, the call agent maintains the relationship between the endpoint (in this case a digital trunk) and its address.

Monitoring and Troubleshooting MGCP

Several **show** and **debug** commands provide support for monitoring and troubleshooting MGCP. This topic lists many useful **show** and **debug** commands.



The figure illustrates the output of one of the **show** commands. The **show** and **debug** commands are valuable for examining the current status of the MGCP components and for troubleshooting. You should be familiar with the information provided from each command and how this information can help you.

The following **show** commands are useful for monitoring and troubleshooting MGCP:

- **show call active voice [brief]:** Displays the status, statistics, and parameters for all active voice calls. When the call is disconnected, this information is transferred to the history records.
- **show call history voice [last *n* | record | brief]:** Displays call records from the history buffer.
- **show mgcp:** Displays basic configuration information about the gateway.
- **show mgcp connection:** Displays details of the current connections.
- **show mgcp endpoint:** Displays a list of the voice ports that are configured for MGCP.
- **show mgcp statistics:** Displays a count of the successful and unsuccessful control commands (shown in the figure). You should investigate a high unsuccessful count.

 Copyright © 2005, Cisco Systems, Inc.

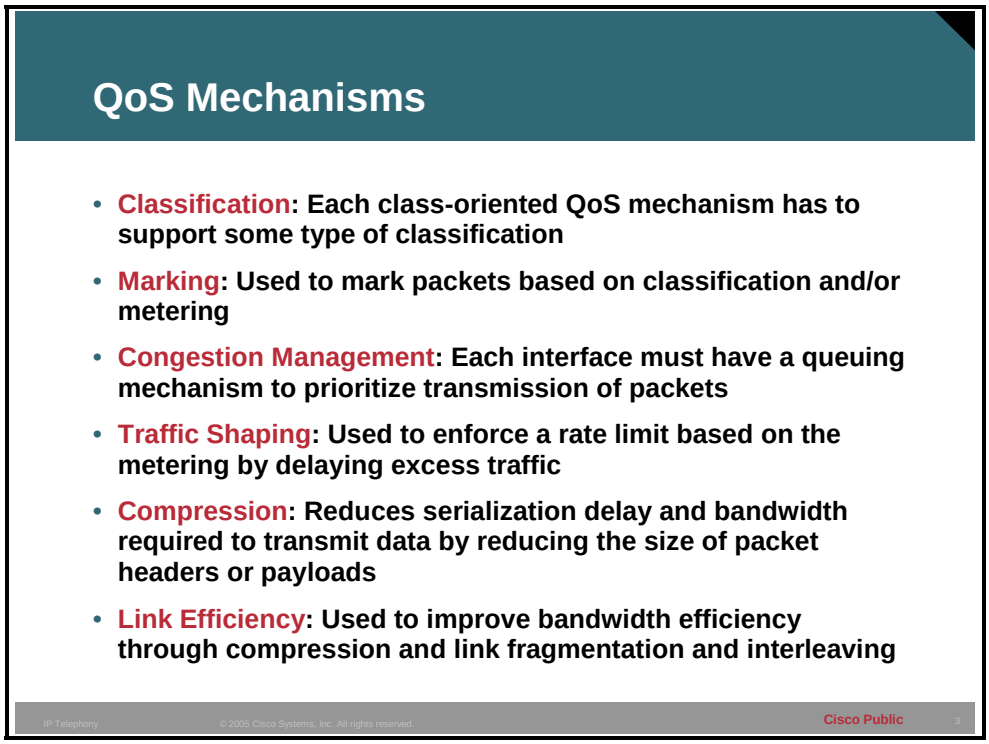
The following **debug** commands are useful for monitoring and troubleshooting MGCP:

- **debug voip ccapi inout:** Shows every interaction with the call control API on the telephone interface and the VoIP side. Watching the output allows users to follow the progress of a call from the inbound interface or VoIP peer to the outbound side of the call. This debug is very active; you must use it sparingly in a live network.
- **debug mgcp [all | errors | events | packets | parser]:** Reports all **mgcp** command activity. You must use this debug to trace the MGCP request and responses.

IP QoS Mechanisms

QoS Mechanisms

This topic lists the key mechanisms use to implement QoS in an IP network.



This slide shows the main categories of QoS tools used in IPTX implementations and describes in layman's terms how they contribute to QoS.

Classification and Marking is the identifying and splitting of traffic into different classes and the marking of traffic according to behavior and business policies.

Congestion management is the prioritizing, protection, and isolation of traffic based on markings.

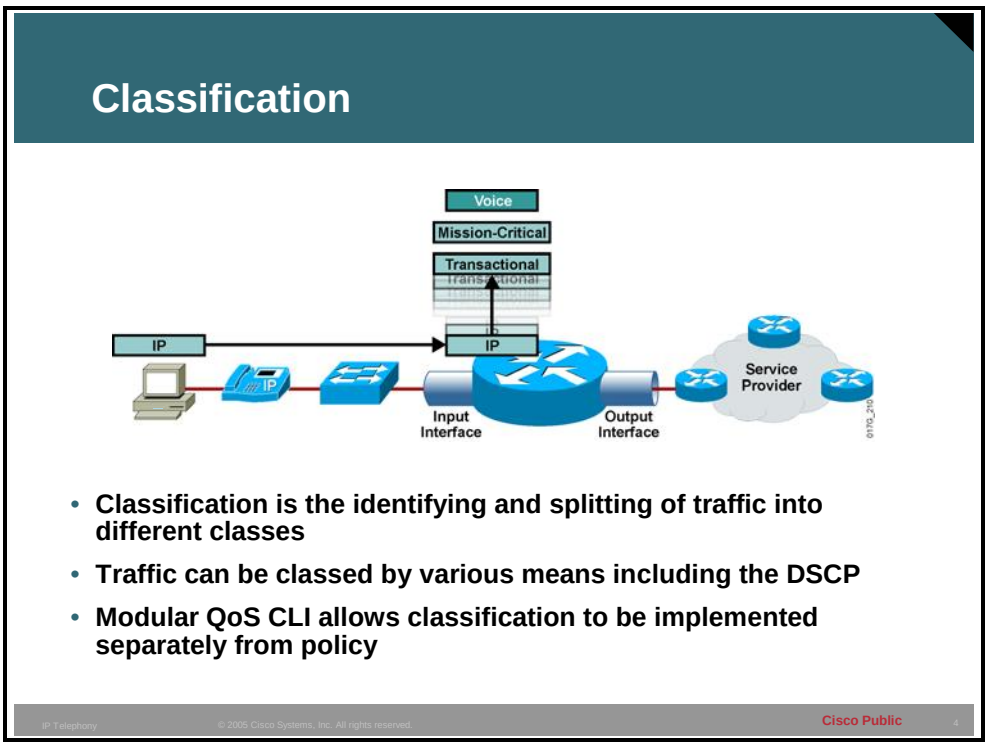
Traffic conditioning mechanisms shape traffic to control bursts by queuing traffic.

One type of link efficiency technology is packet header compression that improves the bandwidth efficiency of a link. Another technology is Link Fragmentation and Interleaving (LFI) that can decrease the "jitter" of voice transmission by reducing voice packet delay.

 Copyright © 2005, Cisco Systems, Inc.

Classification

This topic defines classification and identify where classification is commonly implemented in a network.



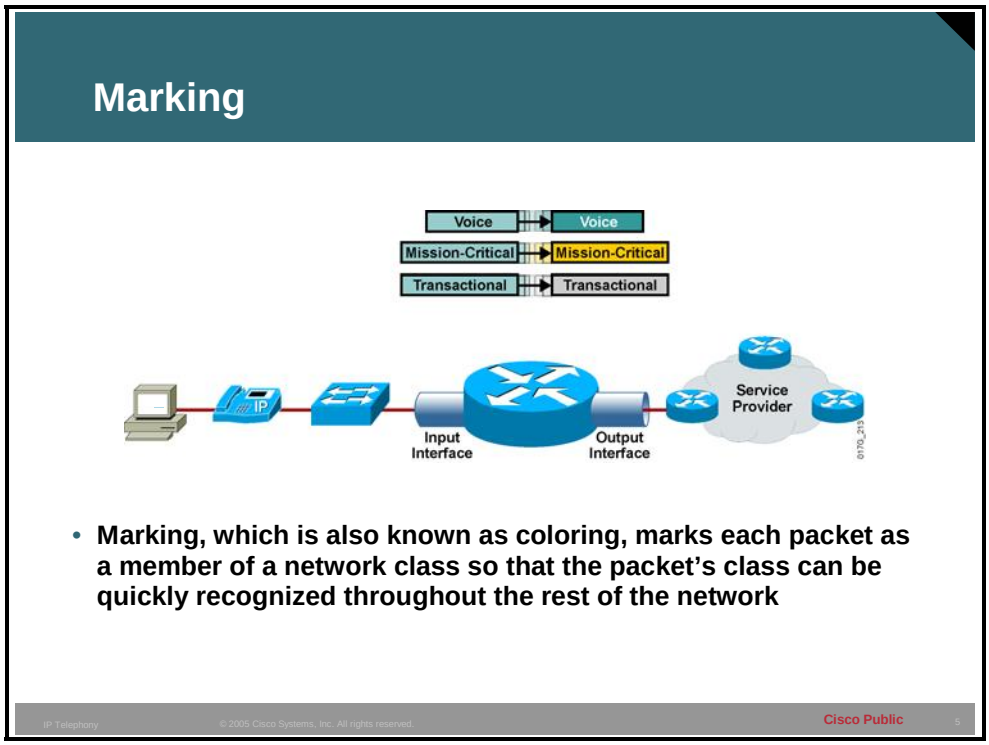
Classification is the identifying and splitting of traffic into different classes. In a QoS-enabled network, all traffic is classified at the input interface of every QoS-aware device. Packet classification can be recognized based on many factors including:

- DSCP
- IP precedence
- Source address
- Destination address

The concept of “trust” is key for deploying QoS. Once an end device (such as a workstation or an IP phone) marks a packet with CoS or DSCP, a switch or router has the option of accepting or not accepting values from the end device. If the switch or router chooses to accept the values, the switch or router “trusts” the end device. If the switch or router trusts the end device, it does not need to do any reclassification of packets coming from that interface. If the switch or router does not trust the interface, then it must perform a reclassification to determine the appropriate QoS value for packet coming from that interface. Switches and routers are generally set to “not trust” end devices and must specifically be configured to “trust” packets coming from an interface.

Marking

This topic defines marking and identify where marking is commonly implemented in a network.



Marking, which is also known as coloring, involves marking each packet as a member of a network class so that devices throughout the rest of the network can quickly recognize the packet's class. Marking is performed as close to the network edge as possible, and is typically done using the MQC.

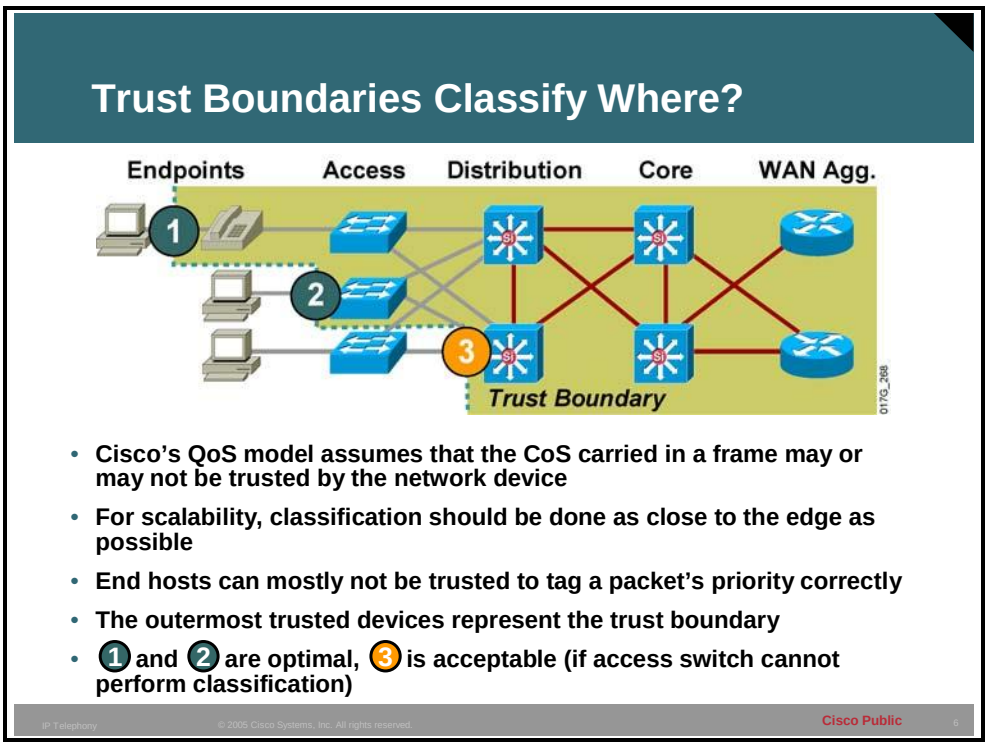
QoS mechanisms set bits in the DSCP or IP precedence fields of each IP packet according to the class which the packet is in. The settings for the DSCP field and their relationship to the IP precedence fields were discussed in the previous lesson. Other fields can also be marked to aid in the identification of a packet's class such as CoS or Frame-Relay Discard Eligibility bit.

Other QoS mechanisms use these bits to determine how to treat the packets when they arrive. If they are marked as high-priority voice packets, the packets will generally never be dropped by congestion avoidance mechanisms and be given immediate preference by congestion management queuing mechanisms. On the other hand, if the packets are marked as low-priority file transfer packets, they will be dropped when congestion is occurring and generally move to the end of the congestion management queues.

 Copyright © 2005, Cisco Systems, Inc.

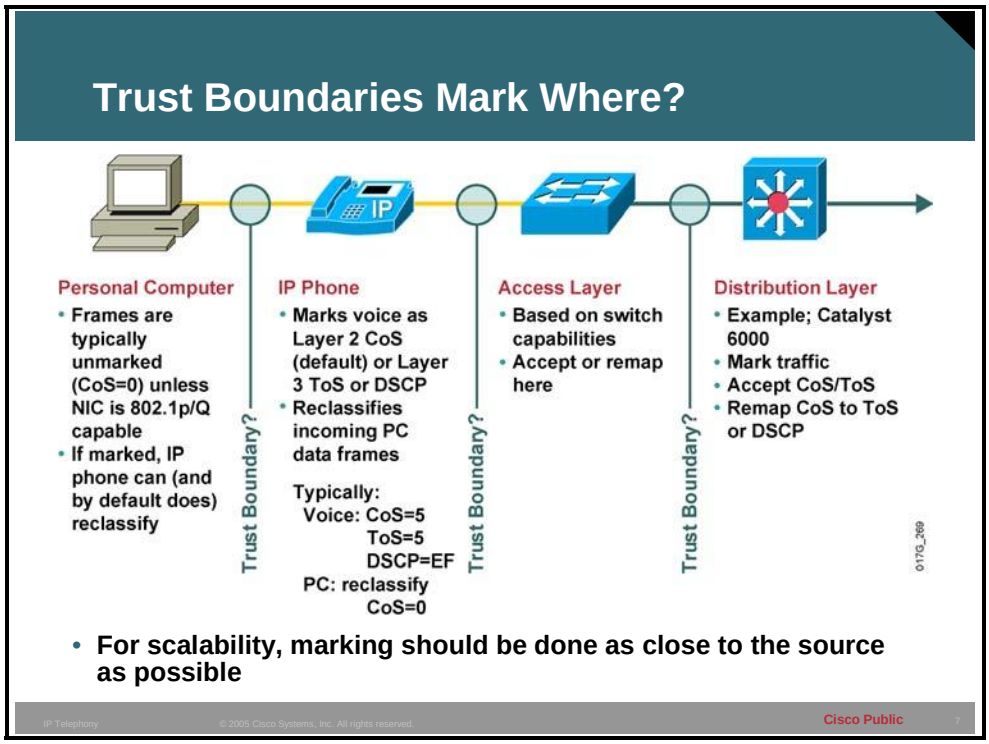
Trust Boundaries

This topic describes concept of trust boundaries and how they are used with classification and marking.



The concept of trust is important and integral to deploying QoS. After the end devices have set CoS or ToS values, the switch has the option of trusting them. If the switch trusts the values, it does not need to reclassify; if it does not trust the values, then it must perform reclassification for the appropriate QoS.

The notion of trusting or not trusting forms the basis for the trust boundary. Ideally, classification should be done as close to the source as possible. If the end device is capable of performing this function, the trust boundary for the network is at the end device. If the device is not capable of performing this function, or the wiring closet switch does not trust the classification done by the end device, the trust boundary might shift. How this shift happens depends on the capabilities of the switch in the wiring closet. If the switch can reclassify the packets, the trust boundary is in the wiring closet. If the switch cannot perform this function, the task falls to other devices in the network, going toward the backbone. In this case, one good rule is to perform reclassification at the distribution layer. This means that the trust boundary has shifted to the distribution layer. It is likely that there is a high-end switch in the distribution layer with features to support this function. If possible, try to avoid performing this function in the core of the network.



Classification should take place at the network edge, typically in the wiring closet or within endpoints (servers, hosts, video endpoints or IP telephony devices) themselves.

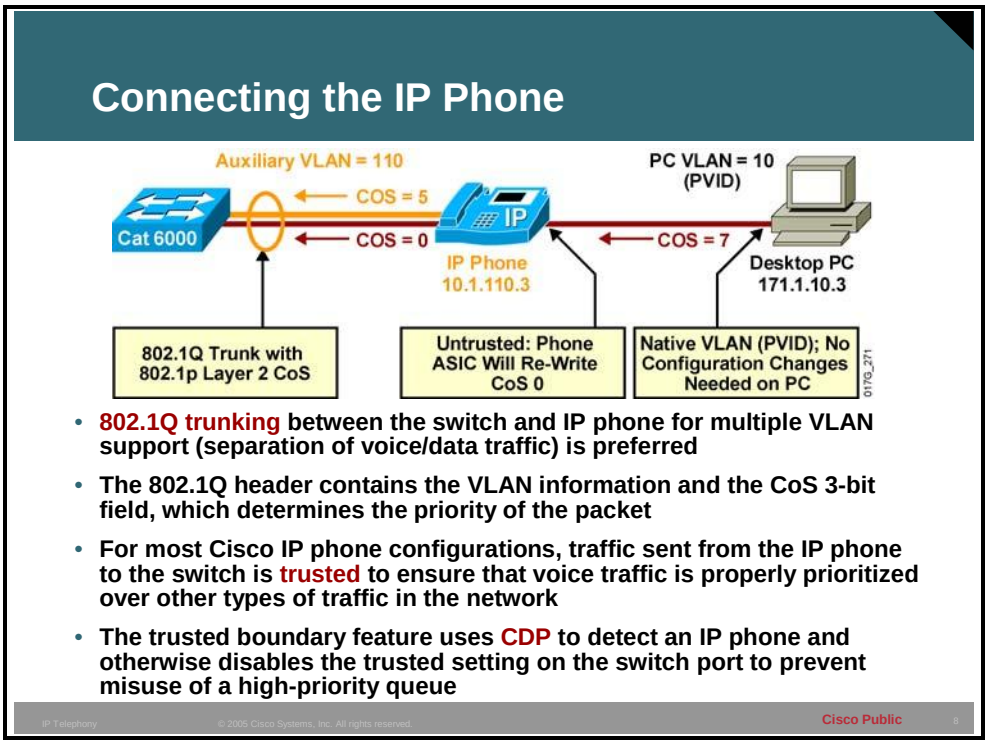
For example, consider the campus network containing IP telephony and host endpoints. Frames can be marked as important by using link layer CoS settings or the IP precedence/DSCP bits in the ToS/DS field in the IPv4 header. Cisco IP Phones can mark voice packets as high priority using CoS as well as ToS. By default, the IP Phone sends 802.1p tagged packets with the CoS and ToS set to a value of 5 for its voice packets. Because most PCs do not have an 802.1Q capable network interface card (NIC), they send packets untagged. This means that the frames do not have an 802.1p field. Also, unless the applications running on the PC send packets with a specific CoS value, this field is zero.

Note	A special case exists where the TCP/IP stack in the PC has been modified to send all packets with a ToS value other than zero. Typically this does not happen, and the ToS value is zero.

Even if the PC is sending tagged frames with a specific CoS value, Cisco IP Phones can zero out this value before sending the frames to the switch. This is the default behavior. Voice frames coming from the IP Phone have a CoS of 5 and data frames coming from the PC have a CoS of 0.

If the end device is not a trusted device, the reclassification function (setting/zeroing the bits in the CoS and ToS fields) can be performed by the access layer switch if that device is capable of doing so. If the device is not capable, then the reclassification task falls to the distribution layer device. If reclassification cannot be performed at one of these two layers, a hardware and/or Cisco IOS software upgrade may be necessary.

 Copyright © 2005, Cisco Systems, Inc.

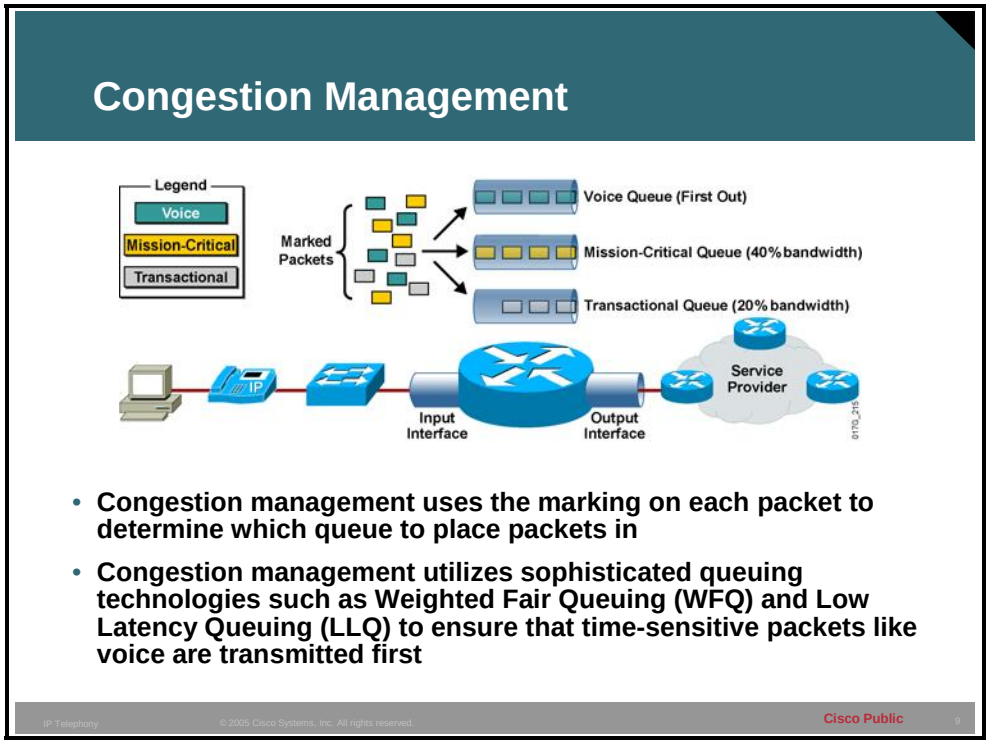


In a typical network, you connect a Cisco IP Phone to a switch port as shown in the figure. Traffic sent from the telephone to the switch is typically marked with a tag that uses the 802.1Q header. The header contains the VLAN information and the CoS 3-bit field, which determines the priority of the packet. For most Cisco IP Phone configurations, the traffic sent from the telephone to the switch is trusted to ensure that voice traffic is properly prioritized over other types of traffic in the network.

By using the **mls qos trust device cisco-phone** and the **mls qos trust cos** interface configuration commands, you can configure the switch port to which the telephone is connected to trust the CoS labels of all traffic received on that port.

Congestion Management

This topic defines congestion management and identify where congestion management is commonly implemented in a network.



Congestion management mechanisms (queuing algorithms) use the marking on each packet to determine which queue to place packets in. Different queues are given different treatment by the queuing algorithm based on the class of packets in the queue. Generally, queues with higher priority packets receive preferential treatment.

All output interfaces in a QoS-enabled network use some kind of congestion management (queuing) mechanism to manage the outflow of traffic. Each queuing algorithm was designed to solve a specific network traffic problem and has a particular effect on network performance.

The Cisco IOS software features for congestion management, or queuing, include:

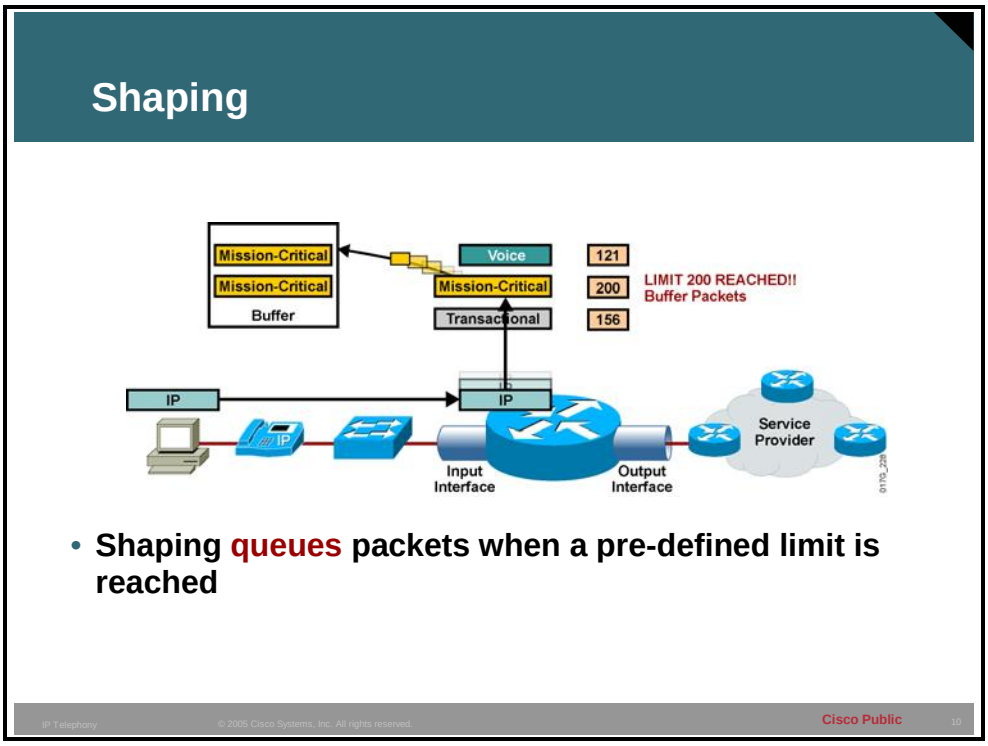
- FIFO (first-in, first-out)
- PQ (priority queuing)
- CQ (custom queuing)
- WFQ (weighted fair queuing)
- CB-WFQ (class-based WFQ)
- LLQ (low latency queuing)

LLQ (low latency queuing) is now the preferred method. It is a hybrid (Priority Queuing and Class Based-Weighted Fair Queuing) queuing method developed specifically to meet the requirements of real time traffic such as voice.

 Copyright © 2005, Cisco Systems, Inc.

Traffic Shaping

This topic defines traffic shaping and identifies where traffic shaping is commonly implemented in a network.



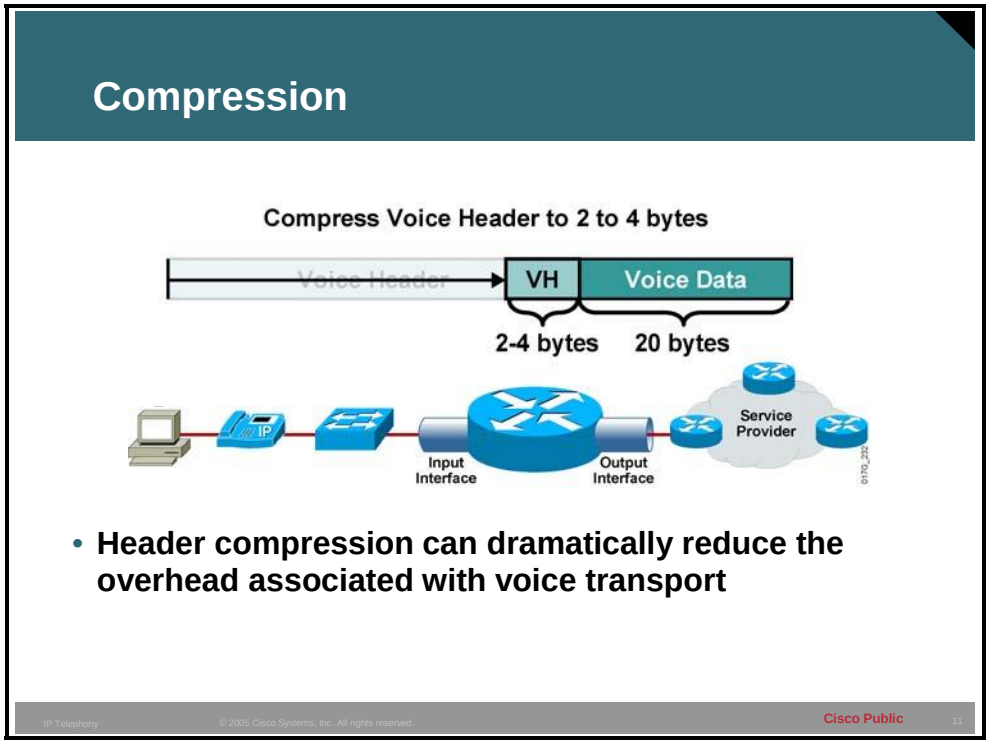
Shaping helps smooth out speed mismatches in the network and limits transmission rates.

Shaping mechanisms are used on output interfaces. They are typically used to limit the flow from a high-speed link to a lower speed link to ensure that the lower speed link does not become overrun with traffic. Shaping could also be used to manage the flow of traffic at a point in the network where multiple flows are aggregated.

Cisco's QoS software solutions include two traffic shaping tools to manage traffic and congestion on the network: generic traffic shaping (GTS) and Frame Relay traffic shaping (FRTS).

Compression

This topic explains the functions of compression and identify where compression is commonly implemented in the network.



Cisco IOS QoS software offers link-efficiency mechanisms that work in conjunction with queuing and traffic shaping to manage existing bandwidth more efficiently and predictably. One of these is Compressed Real-Time Transport Protocol (cRTP).

Real-Time Transport Protocol (RTP) is a host-to-host protocol used for carrying converged traffic, including packetized audio and video, over an IP network. RTP provides end-to-end network transport functions intended for applications transmitting real-time requirements, such as audio, video, simulation data multicast, or unicast network services.

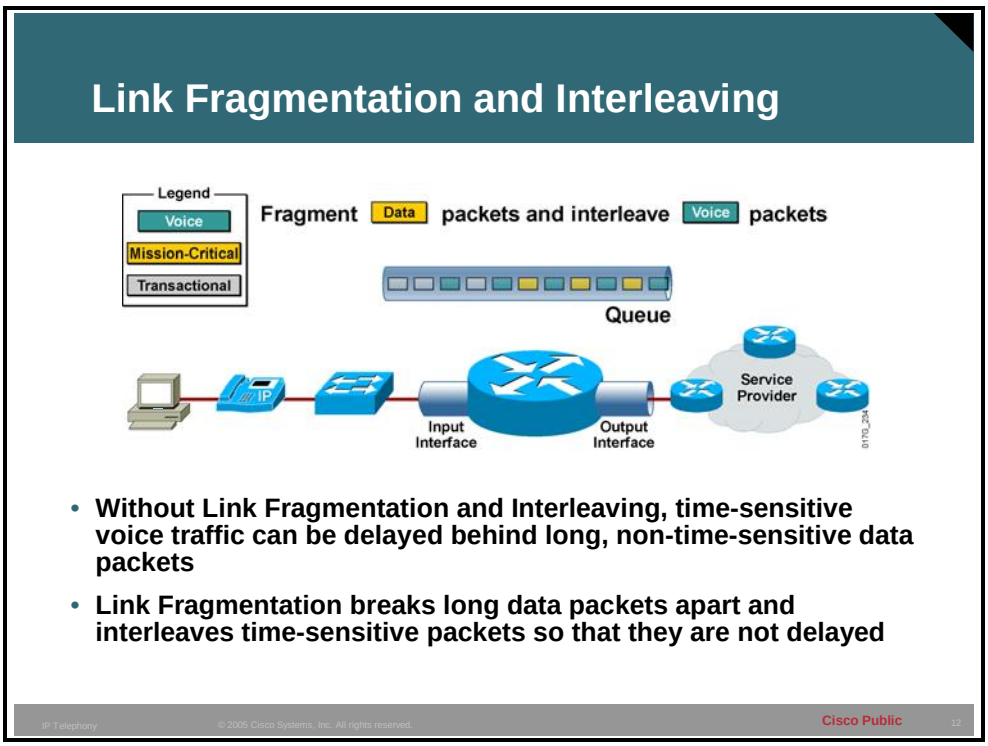
A voice packet carrying a 20-byte voice payload, for example, typically carries a 20-byte IP header, an 8-byte UDP header, and a 12-byte RTP header. By using cRTP, as shown in the graphic above, the three headers of a combined 40 bytes are compressed down to 2 or 4 bytes, depending on whether or not the CRC is transmitted. This compression can dramatically improve the performance of a link.

Compression would typically be used on WAN links between sites to improve bandwidth efficiency.

 Copyright © 2005, Cisco Systems, Inc.

Link Fragmentation and Interleaving

This topic explains the functions of link fragmentation and interleaving and identifies where LFI is commonly implemented in the network.



Interactive traffic, such as Telnet and Voice over IP, is susceptible to increased latency and jitter when the network processes large packets, such as LAN-to-LAN FTP Telnet transfers traversing a WAN link. This susceptibility increases as the traffic is queued on slower links.

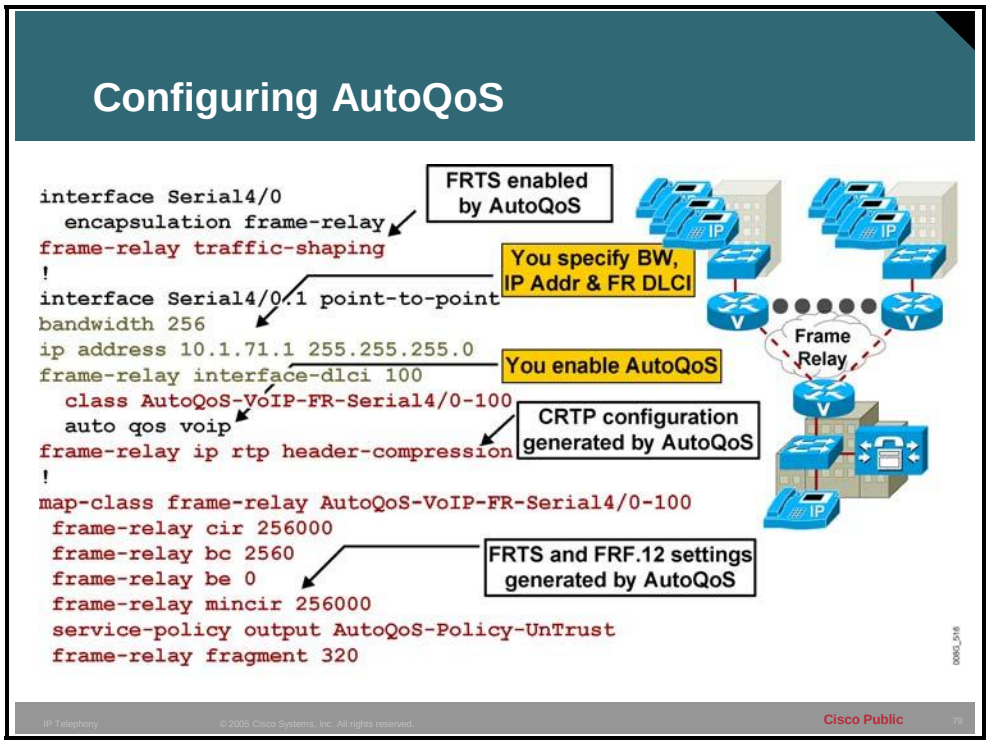
Link Fragmentation and Interleaving (LFI) can reduce delay and jitter on slower-speed links by breaking up large datagrams and interleaving low-delay traffic packets with the resulting smaller packets.

LFI would typically be used on WAN links between sites to ensure minimal delay for voice and video traffic.

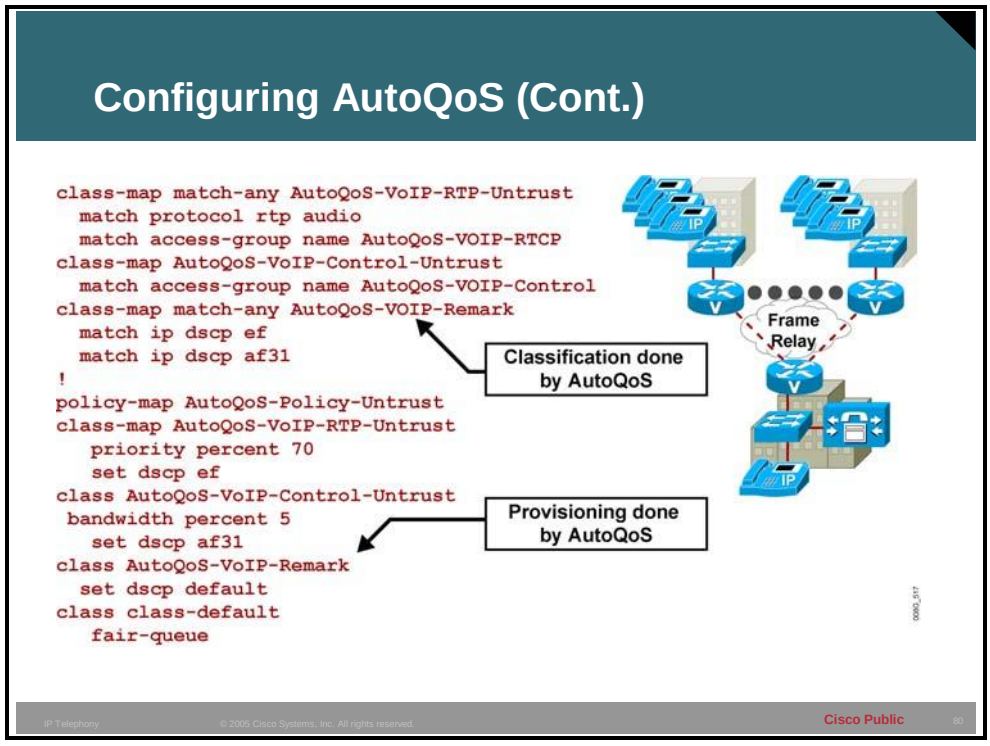
Configuring QoS in the WAN

Configuring AutoQoS

This topic describes Cisco AutoQoS and its associated command structure for routers.



 Copyright © 2005, Cisco Systems, Inc.



Cisco AutoQoS is innovative technology that minimizes the complexity, time, and operating cost of QoS deployment. Cisco AutoQoS incorporates value-added intelligence into Cisco IOS software and Cisco Catalyst Operating Service software to provision and manage large-scale QoS deployments.

The first phase of Cisco AutoQoS targets VoIP deployments for customers who want to deploy IP telephony, but who lack the expertise or staffing to plan and deploy IP QoS and IP services.

Cisco AutoQoS automates consistent deployment of QoS features across Cisco routers and switches. It enables various Cisco QoS components based on the network environment and Cisco best-practice recommendations. With the increased prominence of delay-sensitive applications (voice, video, and other multimedia applications) deployed in networks today, proper QoS configuration will ensure high-quality application performance.

Currently, this presupposes a deep understanding of various QoS features (that is, queuing, dropping, traffic conditioning, queue-depth, drop thresholds, burst parameters, LFI, and CRTP) and the complexities of configuring many parameters associated with these features. Cisco AutoQoS helps overcome these difficulties by automatically configuring the device for Cisco QoS features and variables with the correct parameters.

Users can subsequently tune parameters that are generated by Cisco AutoQoS to suit their particular application needs, as desired.

Cisco AutoQoS performs the following functions:

On WAN interfaces:

- Automatically classifies RTP payload and VoIP control packets (H.323, H.225 Unicast, Skinny, session initiation protocol [SIP], MGCP)

- Builds service policies for VoIP traffic that are based on Cisco Modular QoS Command Line Interface (MQC)
- Provisions LLQ—Priority Queuing for VoIP bearer and bandwidth guarantees for control traffic
- Enables WAN traffic shaping that adheres to Cisco best practices, where required
- Enables link efficiency mechanisms, such as LFI and RTP header compression (CRTP), where required
- Provides SNMP and SYSLOG alerts for VoIP packet drops

On LAN interfaces:

- Enforces the trust boundary on Cisco Catalyst switch access ports, uplinks, and downlinks
- Enables Cisco Catalyst strict priority queuing (also known as expedite queuing) with WRR scheduling for voice and data traffic, where appropriate
- Configures queue admission criteria (maps CoS values in incoming packets to the appropriate queues)
- Modifies queue sizes and weights where required

Note Cisco AutoQoS is available in the following Cisco IOS software releases: Cisco IOS Software Release 12.1E or later for the Cisco Catalyst 2950 and 3550 series switches; Cisco IOS Software Release 12.2T or later for the Cisco 2600, 2600XM, 3600, 3700, and 7200 series routers; Cisco IOS Software Release 12.1E or later for the Cisco Catalyst 4500 series switches; and Cisco Catalyst OS 7.5.1 or later for the Cisco Catalyst 6500 series switches.

Typically, QoS network design and implementation over multiple LAN and WAN sites is fairly complex and labor intensive. Customers wish to reduce deployment time, provisioning errors, and operating expenses to optimize their network for the applications, while retaining the flexibility to subsequently fine-tune QoS.

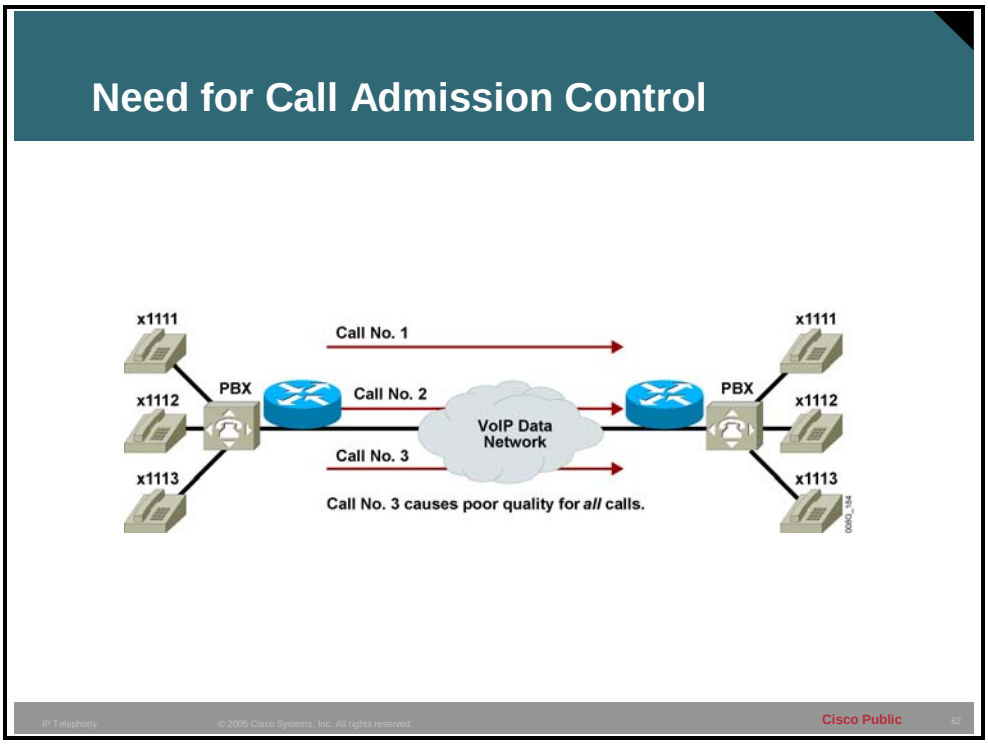
To expedite QoS deployment, the user interface must be simplified. Cisco AutoQoS addresses this by automating the five main aspects of QoS deployment (Application Classification, Policy Generation, Configuration, Monitoring and Reporting, and Consistency) while adding control plane intelligence to create a simple, accelerated, and tunable solution.

 Copyright © 2005, Cisco Systems, Inc.

Configuring CAC

Need for CAC

This topic explains why CAC is needed.



CAC is a concept that applies to voice traffic only, not data traffic. If an influx of data traffic oversubscribes a particular link in the network, queuing, buffering, and packet drop decisions resolve the congestion. The extra traffic is simply delayed until the interface becomes available to send the traffic, or, if traffic is dropped, the protocol or the end user initiates a timeout and requests a retransmission of the information.

Because real-time traffic is sensitive to latency and packet loss, resolving network congestion when real-time traffic is present will jeopardize the QoS. For real-time delay-sensitive traffic such as voice, it is better to deny network access under congestion conditions than to allow traffic on the network to be dropped and delayed. Dropped or delayed network traffic causes intermittent impaired QoS and results in customer dissatisfaction.

CAC is a determining and informed decision that is made before a voice call is established. CAC is based on whether the required network resources are available to provide suitable QoS for the new call.

Example: CAC Applied

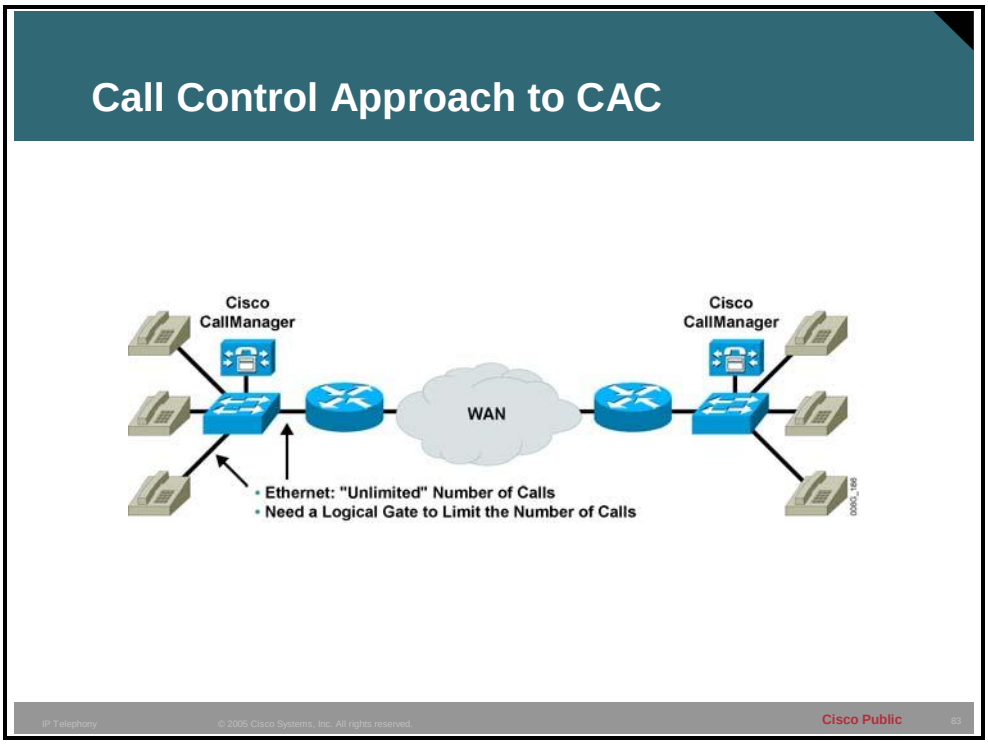
CAC mechanisms extend the capabilities of QoS tools to protect voice traffic from the negative effects of other voice traffic and to keep excess voice traffic off the network. The figure

illustrates the need for CAC. If the WAN access link between the two PBXs has the bandwidth to carry only two VoIP calls, admitting the third call impairs the voice quality of all three calls.

 Copyright © 2005, Cisco Systems, Inc.

CAC as Part of Call Control Services

This topic describes CAC as a function of call control services.



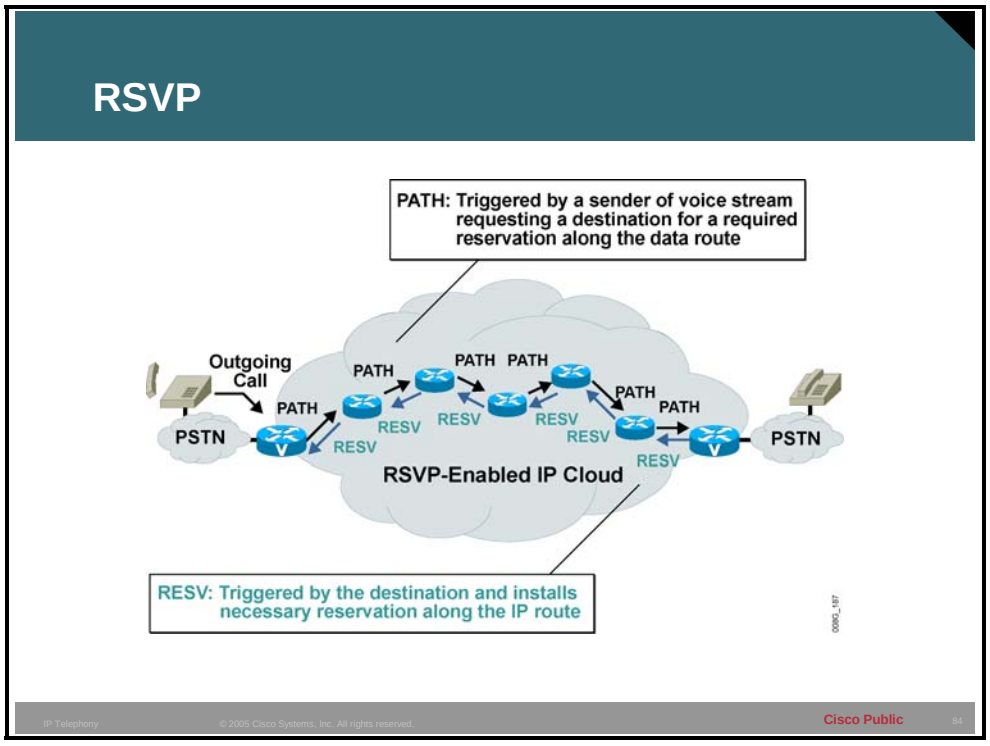
CAC, as part of call control services, functions on the outgoing gateway. CAC bases its decision on nodal information, such as the state of the outgoing LAN or WAN link. If the local packet network link is down, there is no point in executing complex decision logic based on the state of the rest of the network, because that network is unreachable. Local mechanisms include configuration items that disallow all calls that exceed a specified number.

Example: Call Control CAC

If the network designer already knows that bandwidth limitations allow no more than five calls across the outgoing WAN link, then the local node can be configured to allow no more than five calls. You can configure this type of CAC on outgoing dial peers.

RSVP

This topic describes Resource Reservation Protocol (RSVP).



RSVP is the only CAC mechanism that makes a bandwidth reservation and does not make a call admission decision based on a best guess before the call is set up. This gives RSVP the unique advantage of not only providing CAC for voice, but also guaranteeing the QoS against changing network conditions for the duration of the call. The RSVP reservation is made in both directions because a voice call requires a two-way speech path and bandwidth in both directions.

The terminating gateway ultimately makes the CAC decision based on whether both reservations succeed. At that point, the H.323 state machine continues with either an H.225 Alerting/Connect (the call is allowed and proceeds), or with an H.225 Reject/Release (the call is denied). The RSVP reservation is in place by the time the destination phone starts ringing and the caller hears ringback.

RSVP has the following important differences from other CAC methods discussed in this lesson:

- The ability to maintain QoS for the duration of the call.
- An awareness of topology. In concept, the RSVP reservation installs on every interface that the call will traverse through the network. RSVP ensures bandwidth over every segment without any requirement to know the actual bandwidth provisioning on each interface or the path on which the routing protocols direct the packets. RSVP, therefore, adjusts automatically to network configuration changes, and no manual calculations are necessary to keep different aspects of the configuration synchronized.
- To function correctly, RSVP is dependent on the correct configuration for all devices in the network. (It can have a scaling issue depending on how the network is designed.)

 Copyright © 2005, Cisco Systems, Inc.

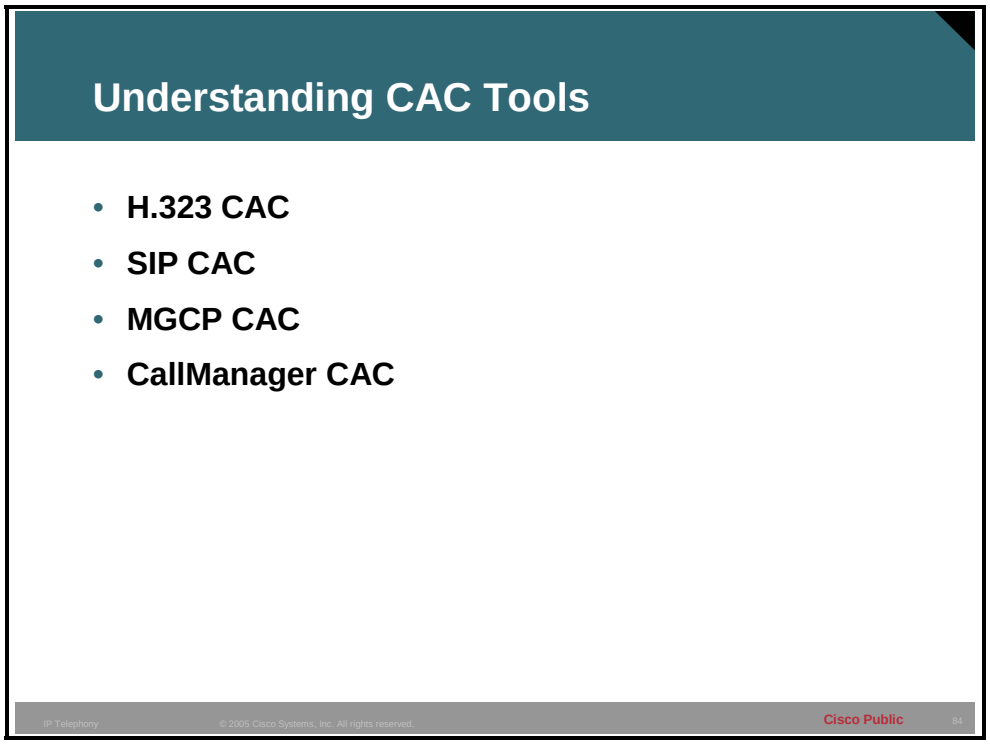
- RSVP provides end-to-end reservation per call and has visibility for that call only. RSVP is unaware of how many other calls are active from a site or across an interface, or the source or destination of any other call.

Example: RSVP

Configuring RSVP in Cisco routers allows the administrator to limit the amount of bandwidth requested per call and the total amount of bandwidth allowed for all calls. This configuration is entered directly against the interface that will permit or deny the calls. The configuration also requires RSVP to be configured on the dial peers for the calls that will be managed by RSVP.

Understanding CAC Tools

This topic describes CAC tools available for various protocols and systems.



As the many interesting aspects of CAC on packet networks have been considered, several different solutions have come into prominence. None of them solves the entire problem, but they all are useful to address a particular aspect of CAC. Unlike circuit-based networks, which reserve a free DS0 time slot on every leg of the path the call will take, determining whether a packet network has the resources to carry a voice call is not a simple undertaking.

There are four areas in which CAC may be implemented. These areas are:

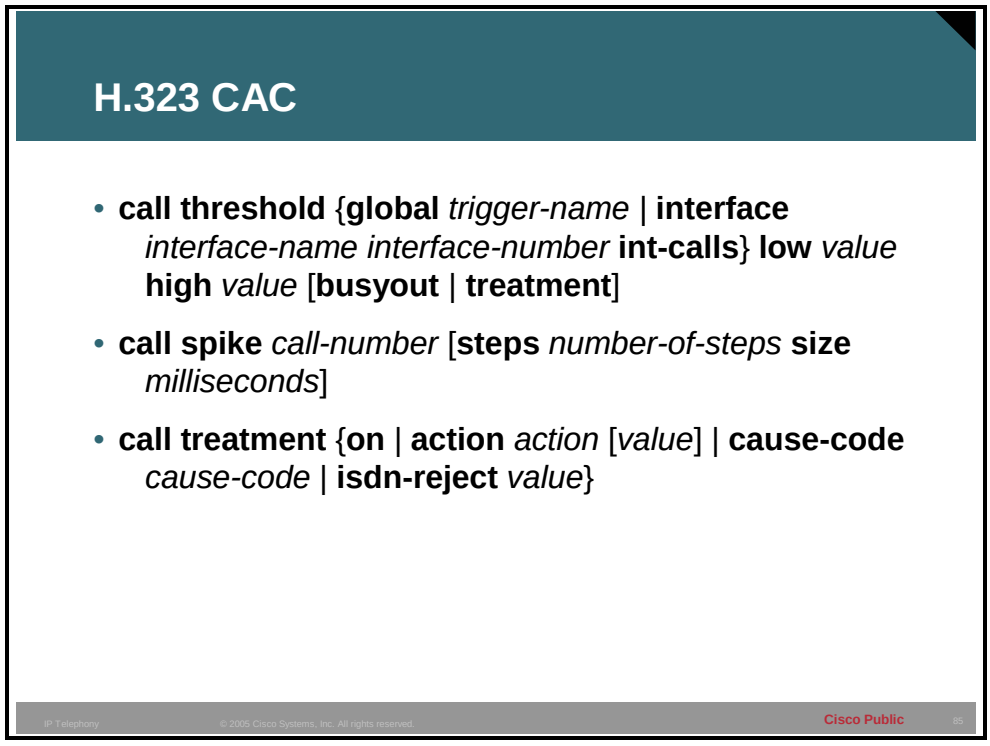
- H.323 CAC
- SIP CAC
- MGCP CAC
- CallManager CAC

Each area is associated with a specific protocol or system. Each of these areas will be explored in the following figures.

 Copyright © 2005, Cisco Systems, Inc.

H.323 CAC

This topic describes the configuration options available for H.323 CAC.



The CAC for the H.323 VoIP gateways feature allows you to configure thresholds for local resources, memory, and CPU resources.

With the **call threshold** command, you can configure two thresholds, high and low, for each resource. Call treatment is triggered when the current value of a resource exceeds the configured high. The call treatment remains in effect until the current resource value falls below the configured low. Having high and low thresholds prevents call admission flapping and provides hysteresis in call admission decision making.

With the **call spike** command, you can configure the limit for incoming calls during a specified time period. A call spike is the term for when a large number of incoming calls arrive from the PSTN in a very short period of time; for example, 100 incoming calls in 10 milliseconds.

With the **call treatment** command, you can select how the call should be treated when local resources are not available to handle the call. For example, when the current resource value for any one of the configured triggers for call threshold has exceeded the configured threshold, the call treatment choices are as follows:

- **Time-division multiplexing (TDM) hairpinning:** Hairpins the calls through the POTS dial peer
- **Reject:** Disconnects the call
- **Play message or tone:** Plays a configured message or tone to the user

To enable the global resources of this gateway, use the **call threshold** command in global configuration mode. To disable this command, use the **no** form of this command.

call threshold {**global** *trigger-name* | **interface** *interface-name interface-number* **int-calls**} **low** *value* **high** *value* [**busyout** | **treatment**]

no call threshold {**global** *trigger-name* | **interface interface-name int-calls**}

Call Threshold Commands

Command	Description
global *trigger-name*	Specifies the global resources on the gateway The *trigger-name* arguments are as follows: ■ **cpu-5sec:** CPU utilization in the last 5 seconds ■ **cpu-avg:** Average CPU utilization ■ **io-mem:** IO memory utilization ■ **proc-mem:** Processor memory utilization ■ **total-calls:** Total number of calls. The valid range is from 1 to 10,000. ■ **total-mem:** Total memory utilization
interface *interface-name interface-number*	Specifies the gateway. The types of interfaces and their numbers will depend upon the configured interfaces.
int-calls	Number of calls through the interface. The valid range is from 1 to 10,000 calls**.**
low *value*	Value of low threshold. The valid range is from 1 to 100 percent for the utilization triggers.
high *value*	Value of high threshold. The valid range is from 1 to 100 percent for the utilization triggers.
busyout	(Optional—global only) Automatically busies out the T1/E1 channels if the resource is not available.
treatment	(Optional—global only) Applies call treatment from session application if the resource is not available.

To configure the limit of incoming calls in a short period of time, use the **call spike** command in global configuration mode. To disable this command, use the **no** form of this command. The **call spike** command uses a sliding window to determine the period in which the spike is limited. The sliding window period is defined using the **size** command, with valid ranges from 100 to 250 ms. If a longer spike period is desired, the **steps** command is used as a multiplier for the **size** command. For example, if the **steps** were set to 2 and the **size** was set to 250, the spike period would be 500 ms.

call spike *call-number* [**steps** *number-of-steps* **size** *milliseconds*]

no call spike

 Copyright © 2005, Cisco Systems, Inc.

Call Spike Commands

Command	Description
call-number	Incoming call numbers for spiking threshold; valid range is from 1 to 2,147,483,647
steps *number-of-steps*	(Optional) Number of steps; valid range is from 3 to 10
size *milliseconds*	(Optional) Step size in milliseconds; valid range is from 100 to 2000

To configure how calls should be processed when local resources are unavailable, use the **call treatment** command in global configuration mode. To disable the call treatment triggers, use the **no** form of this command.

call treatment {**on** | **action** *action* [*value*] | **cause-code** *cause-code* | **isdn-reject** *value*}

no call treatment {**on** | **action** *action* [*value*] | **cause-code** *cause-code* | **isdn-reject** *value*}

Call Treatment Commands

Command	Description
on	Enables call treatment from default session application
action *action*	Action to take when call treatment is triggered. The *action* argument has the following possible values: ■ **hairpin:** Hairpin ■ **playmsg:** Specifies the audio file to play (URL) ■ **reject:** Disconnect the call and pass down cause code
value	(Optional) (For the *action* playmsg argument only) Specifies the audio file to play; URL format
cause-code *cause-code*	Specifies reason for disconnect to caller The *cause-code* argument can have the following values: ■ **busy:** Indicates that gateway is busy ■ **no-QoS:** Indicates that the gateway cannot provide QoS ■ **no-resource:** Indicates that the gateway has no resources available
isdn-reject *value*	Selects the ISDN reject cause-code. The *value* argument has the following: ■ 34–47 (ISDN cause code for rejection)

ISDN Cause Codes

Cause No.	Description	Function
34	No circuit available (circuit/channel congestion)	Indicates that there is no channel available to handle the call.
38	Net out of order	Indicates that the network is not functioning properly and it is likely to last a long time. Re-attempting the call is not likely to be successful.
41	Net problem, redial (temporary failure)	Indicates that the network is not functioning properly and it is not going to last a long time. Re-attempting the call is likely to be successful.
42	Net busy, redial (switching equipment congestion)	Indicates that the switching equipment is experiencing high traffic load.
43	Access/user information discarded	Indicates that the network is unable to deliver user information to the remote users as was requested.
44	No channel available (requested circuit/channel not available)	Indicates that the circuit or channel indicated by the requesting side cannot be used by the other side of the interface.
47	Resource unavailable/new destination	Indicates a resource unavailable event only when no other cause in the resource unavailable class applies.

Example: H.323 CAC Configuration

The following example will busyout the total-calls resource if 5 (low) or 5000 (high) is reached:

```
call threshold global total-calls low 5 high 5000 busyout
```

The following example enables thresholds of 5 (low) and 2500 (high) for interface calls on interface Ethernet 0:

```
call threshold interface Ethernet 0 int-calls low 5 high 2500
```

The following example will busyout the average CPU utilization if 5 percent (low) or 65 percent (high) is reached:

```
call threshold global cpu-avg low 5 high 65 busyout
```

The following configuration of the **call spike** command has a call number of 30, 10 steps, and a step size of 2000 milliseconds:

```
call spike 30 steps 10 size 2000
```

The following example enables the call treatment feature with a hairpin action:

```
call treatment on
call treatment action hairpin
```

The following example displays proper formatting of the **playmsg action** keyword:

```
call treatment action playmsg tftp://keyer/prompts/conjestion.
au
```

 Copyright © 2005, Cisco Systems, Inc.

Note	The **congestion.au** file plays when local resources are not available to handle the call.

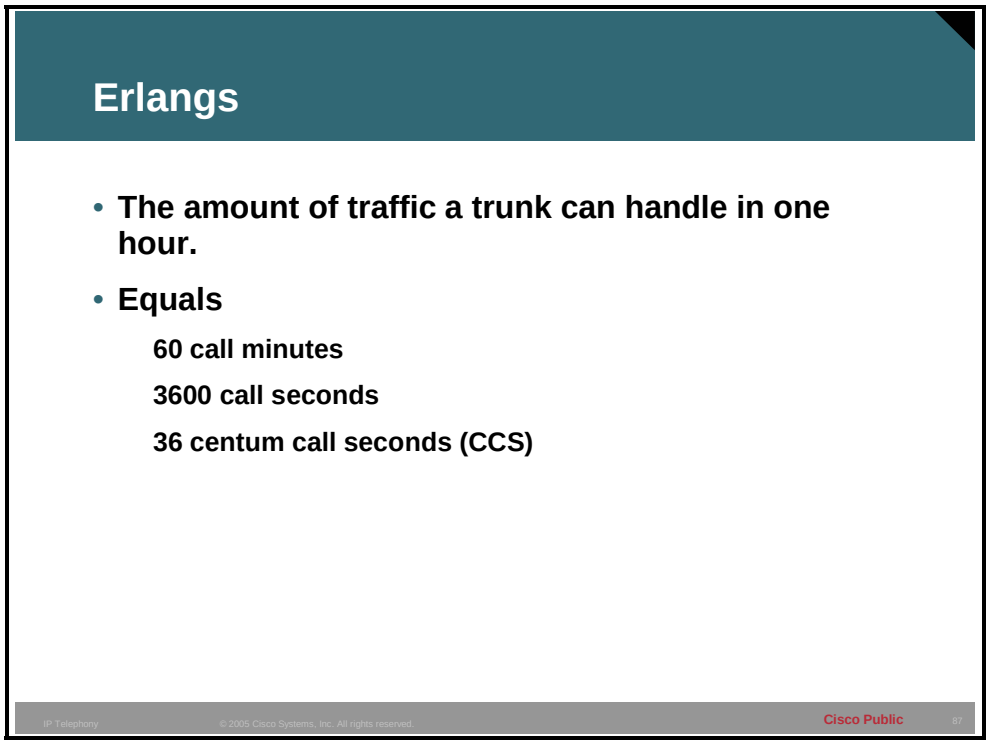
The following example configures a call treatment cause-code to display no-QoS when local resources are unavailable to process a call:

```
call treatment cause-code no-qos
```

Voice Bandwidth Engineering

Erlangs

This topic describes erlangs.



The traffic volume in telephone engineering is measured in units called erlangs. An erlang is the amount of traffic one trunk can handle in one hour. It is a nondimensional unit that has many functions.

Other equivalent measurements that you might encounter include the following:

1 erlang = 60 call minutes = 3600 call seconds = 36 centum call seconds (CCS)

Example: Erlang Calculation

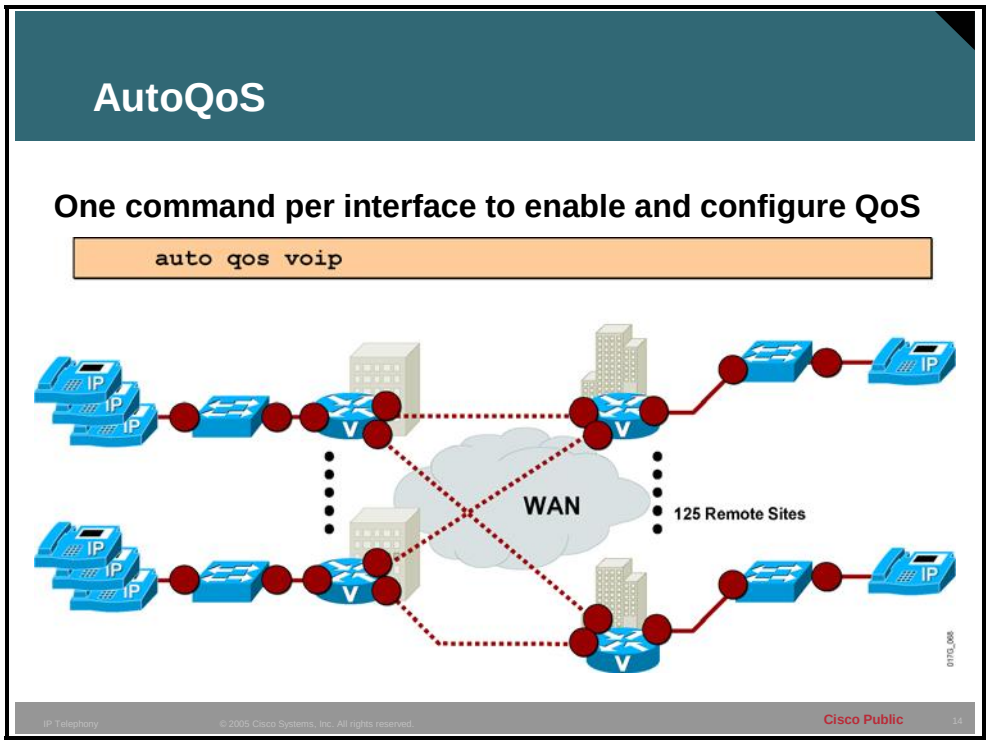
Assume that, on average, each user in a branch makes 10 calls with an average duration of 5 minutes during the busy hour. If the branch has 25 employees, the total number of minutes of call time during the busy hour is 10 calls per busy hour multiplied by 5 minutes per call multiplied by 25 employees per branch, or 1250 call minutes. However, erlangs is a measurement based on hours, so the number of erlangs is 1250 divided by 60, or 20.83 erlangs.

 Copyright © 2005, Cisco Systems, Inc.

Implementing AutoQoS

AutoQoS

This topic describes the basic purpose and function of AutoQoS.



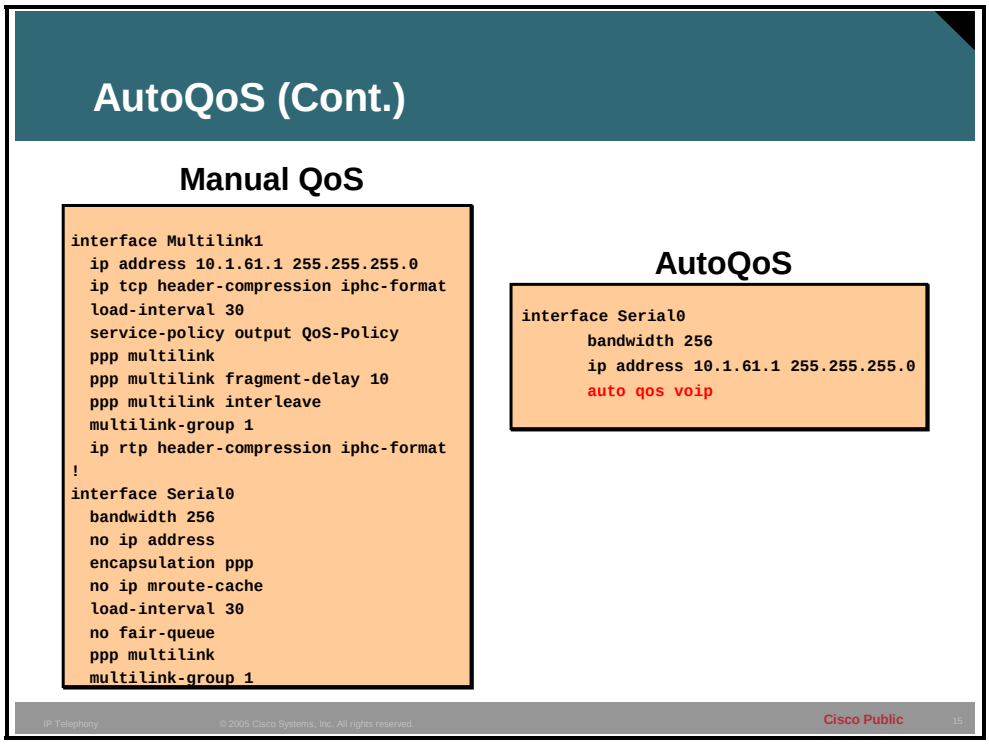
AutoQoS enables customer networks the ability to deploy QoS features for converged IP telephony (IPT) and data networks much faster and more efficiently. It simplifies and automates the Modular QoS CLI (MQC) definition of traffic classes, and the creation and configuration of traffic policies (Cisco AutoQoS generates traffic classes and policy maps CLI templates). Therefore, when AutoQoS is configured at the interface or PVC, the traffic receives the required QoS treatment automatically. In-depth knowledge of the underlying technologies, service policies, link efficiency mechanisms, and Cisco QoS best practice recommendations for voice requirements is not required to configure AutoQoS.

Cisco AutoQoS can be extremely beneficial for the following scenarios:

- Small-to-medium size businesses that need to deploy IPT quickly, but lack the experience and staffing to plan and deploy IP QoS services.
- Large customer enterprises that need to deploy Cisco AVVID on a large scale, while reducing the costs, complexity, and timeframe for deployment and ensuring that the appropriate QoS for voice applications is being set in a consistent fashion.
- International enterprises or service providers requiring QoS for VoIP where little expertise exists in different regions of the world and where provisioning QoS remotely and across different time zones is difficult.

 Copyright © 2005, Cisco Systems, Inc.

- Service providers requiring a template-driven approach to delivering managed services and QoS for voice traffic to large numbers of customer premise devices.



Cisco AutoQoS automatically creates the QoS-specific features required for supporting the underlying transport mechanism and link speed of an interface or PVC type. For example, traffic shaping (FRTS) would be automatically configured and enabled by Cisco AutoQoS for Frame Relay links. LFI and RTP header compression (cRTP) would be automatically configured via the Cisco AutoQoS template for slow link speeds (less than 768 kbps). Therefore, it is very important that the bandwidth statement be properly set on the interface prior to configuring AutoQoS as the resulting configuration will vary based on this configurable parameter.

Using Cisco AutoQoS, VoIP traffic is automatically provided with the required QoS template for voice traffic by configuring **auto qos voip** on an interface or PVC. Cisco AutoQoS enables the required QoS based on Cisco best practice methodologies (the configuration generated by Cisco AutoQoS can be modified if desired).

 Copyright © 2005, Cisco Systems, Inc.

AutoQoS (Cont.)

- **Application Classification**
  - **Automatically discovers applications and provides appropriate QoS treatment**
- **Policy Generation**
  - **Automatically generates initial an ongoing QoS policies**
- **Configuration**
  - **Provides high level business knobs, and multi-device / domain automation for QoS**
- **Monitoring & Reporting**
  - **Generates intelligent, automatic alerts and summary reports**
- **Consistency**
  - **Enables automatic, seamless interoperability among all QoS features and parameters across a network topology – LAN, MAN, and WAN**



© 2005 Cisco Systems, Inc. All rights reserved.

Cisco AutoQoS simplifies and shortens the Quality of Service deployment cycle. Cisco AutoQoS helps in all five major aspects of successful QoS deployments:

- **Application Classification:** Cisco AutoQoS leverages intelligent classification on routers, utilizing Cisco Network-Based Application Recognition (nBAR) to provide deep and stateful packet inspection. Cisco AutoQoS uses Cisco Discovery Protocol (CDP) for voice packets, ensuring that the device attached to the local area network (LAN) is really an IP phone.
- **Policy Generation:** Cisco AutoQoS evaluates the network environment and generates an initial policy. It automatically determines WAN settings for fragmentation, compression, encapsulation, and Frame Relay-ATM interworking, eliminating the need to understand QoS theory and design practices in various scenarios. Customers can meet additional or special requirements by modifying the initial policy as they normally would.

  The first release of Cisco AutoQoS provides the necessary AutoQoS-VoIP feature to automate QoS settings for VoIP deployments. This feature automatically generates interface configurations, policy maps, class maps, and ACLs. AutoQoS-VoIP will automatically employ Cisco nBAR to classify voice traffic, and mark it with the appropriate differentiated services code point (DSCP) value. AutoQoS-VoIP can be instructed to rely on, or trust, the DSCP markings previously applied to the packets.
- **Configuration:** With one command, Cisco AutoQoS configures the port to prioritize voice traffic without affecting other network traffic, while still offering the flexibility to adjust QoS settings for unique network requirements.

  Not only will Cisco AutoQoS automatically detect Cisco IP Phones and enable QoS settings, it will disable the QoS settings when a Cisco IP phone is relocated or moved to prevent malicious activity.

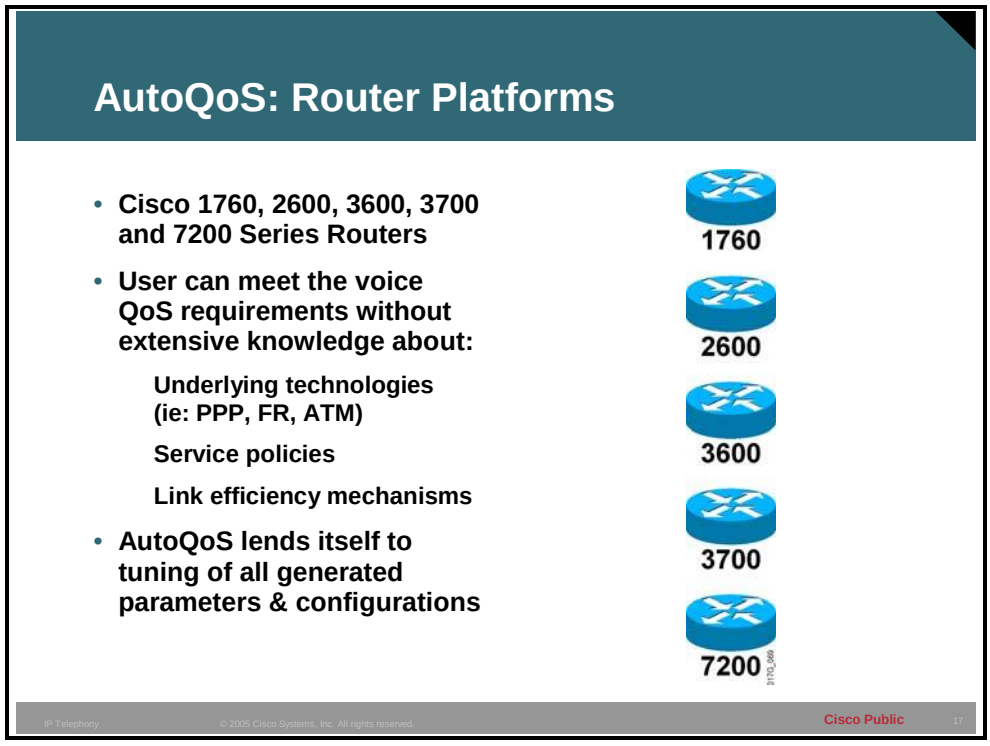
AutoQoS generated router and switch configurations are customizable using the standard Cisco IOS CLI.

- **Monitoring & Reporting:** Cisco AutoQoS provides visibility into the classes of service deployed via system logging and Simple Network Management Protocol (SNMP) traps, with notification of abnormal events (ie: VoIP packet drops).

 Copyright © 2005, Cisco Systems, Inc.

AutoQoS: Router Platforms

This topic identifies the router and switch platforms on which AutoQoS will operate.



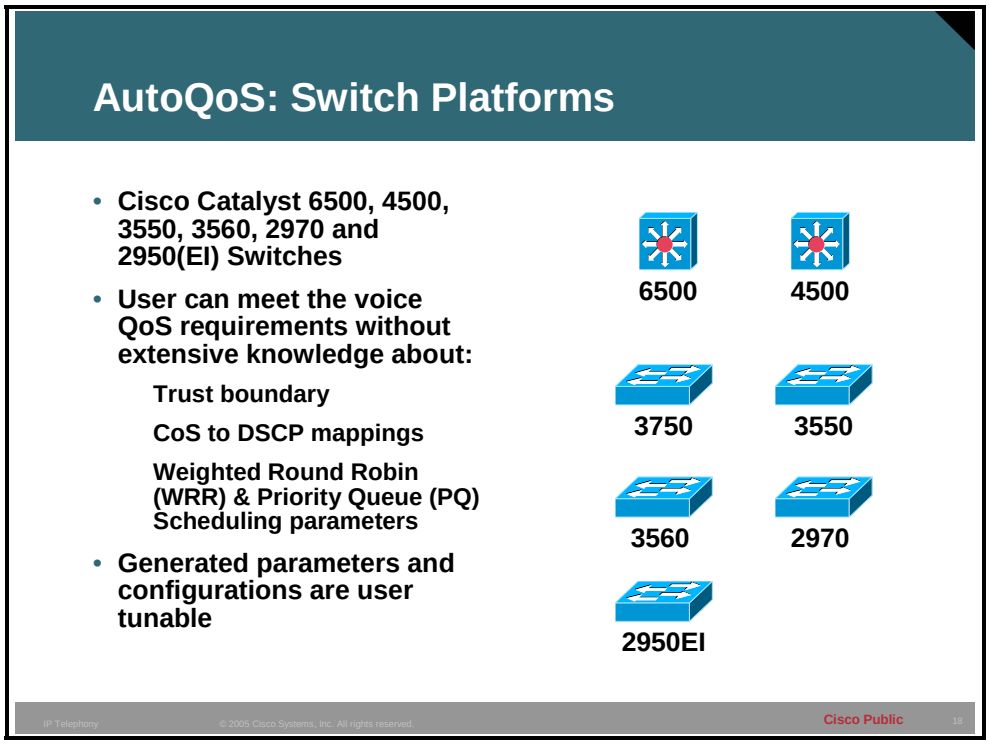
Initial support for AutoQoS includes the Cisco 2600, 2600-XM, 3600, 3700, and 7200 series routers. Support for additional platforms will become available.

Cisco AutoQoS VoIP feature is supported only on the following interfaces and PVCs:

- Serial interfaces with Point-to-Point (PPP) or High-Level Data Link Control (HDLC)
- Frame Relay DLCIs (point-to-point sub-interfaces only)
  - Cisco AutoQoS does not support Frame Relay multipoint interfaces
- ATM PVCs
  - Cisco AutoQoS VoIP is supported on low-speed ATM PVCs on point-to-point sub-interfaces only (link bandwidth less than 768 kbps)
  - Cisco AutoQoS VoIP is fully supported on high-speed ATM PVCs (link bandwidth greater than 768 kbps)

AutoQoS: Switch Platforms

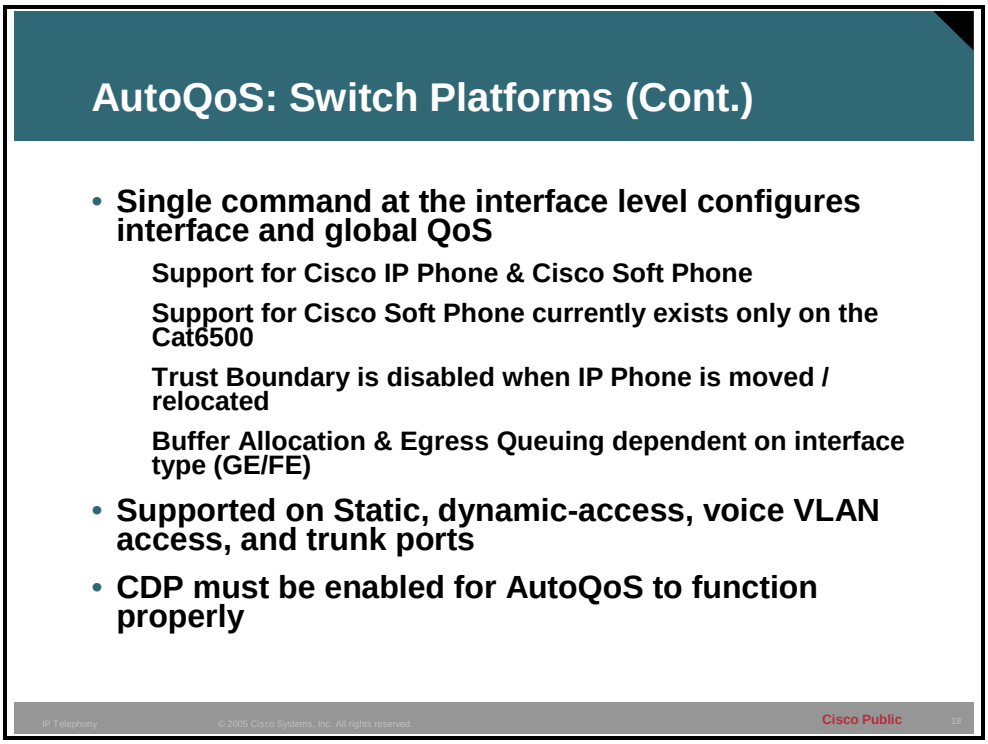
This topic identifies the switch platforms on which AutoQoS will operate.



Initial support for AutoQoS includes the Cisco Catalyst 6500, 4500, 3550, 3560, 2970 and 2950EI series switches. Support for additional platforms including the Cisco Catalyst 4000 will become available.

The Enhanced Image (EI) is required on the Cisco Catalyst 2950 Series Switches.

 Copyright © 2005, Cisco Systems, Inc.



To configure the QoS settings and the trusted boundary feature on the Cisco IP Phone, you must enable Cisco Discovery Protocol (CDP) version 2 or later on the port. If you enable the trusted boundary feature, a syslog warning message displays if CDP is not enabled or if CDP is running version 1.

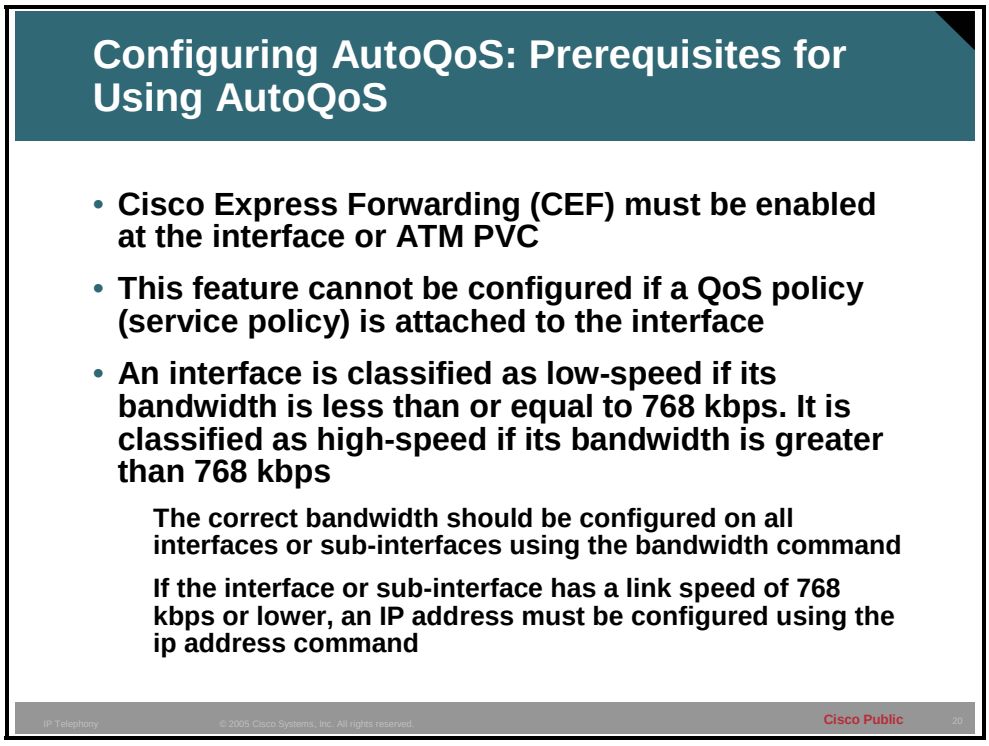
You need to enable CDP only for the **ciscoipphone** QoS configuration; CDP does not affect the other components of the automatic QoS features. When you use the **ciscoipphone** keyword with the port-specific automatic QoS feature, a warning displays if the port does not have CDP enabled.

When executing the port-specific automatic QoS command with the **ciscoipphone** keyword without the trust option, the trust-device feature is enabled. The trust-device feature is dependent on CDP. If CDP is not enabled or not running version 2, a warning message displays as follows:

```
Console> (enable) set port qos 4/1 autoqos voip ciscoipphone
Warning: CDP is disabled or CDP version 1 is in use. Ensure
that CDP version 2 is enabled globally, and also ensure that
CDP is enabled on the port(s) you wish to configure autoqos
on.
Port 4/1 ingress QoS configured for ciscoipphone.
It is recommended to execute the "set qos autoqos" global
command if not executed previously.
Console> (enable)
```

AutoQoS Prerequisites

This topic describes some of the key prerequisites for using AutoQoS.



Before configuring AutoQoS, the following prerequisites must be met:

- Cisco Express Forwarding (CEF) must be enabled at the interface or ATM PVC. Cisco AutoQoS uses Network Based Application Recognition (NBAR) to identify various applications and traffic types and CEF is a prerequisite for NBAR.
- Ensure that no QoS policies (service policies) are attached to the interface. This feature cannot be configured if a QoS policy (service policy) is attached to the interface.
- AutoQoS classifies links as either low-speed or high-speed depending upon the link bandwidth. Remember that on a serial interface, the default bandwidth if not specified is 1.544 Mbps. Therefore, it is important that the correct bandwidth be specified on the interface or sub-interface where AutoQoS is to be enabled.
  - For all interfaces or sub-interfaces, be sure to properly configure the bandwidth by using the bandwidth command. The amount of bandwidth allocated should be based on the link speed of the interface.
  - If the interface or sub-interface has a link speed of 768 kbps or lower, an IP address must be configured on the interface or sub-interface using the **ip address** command. By default, AutoQoS will enable multilink PPP and copy the configured IP address to the multilink bundle interface.

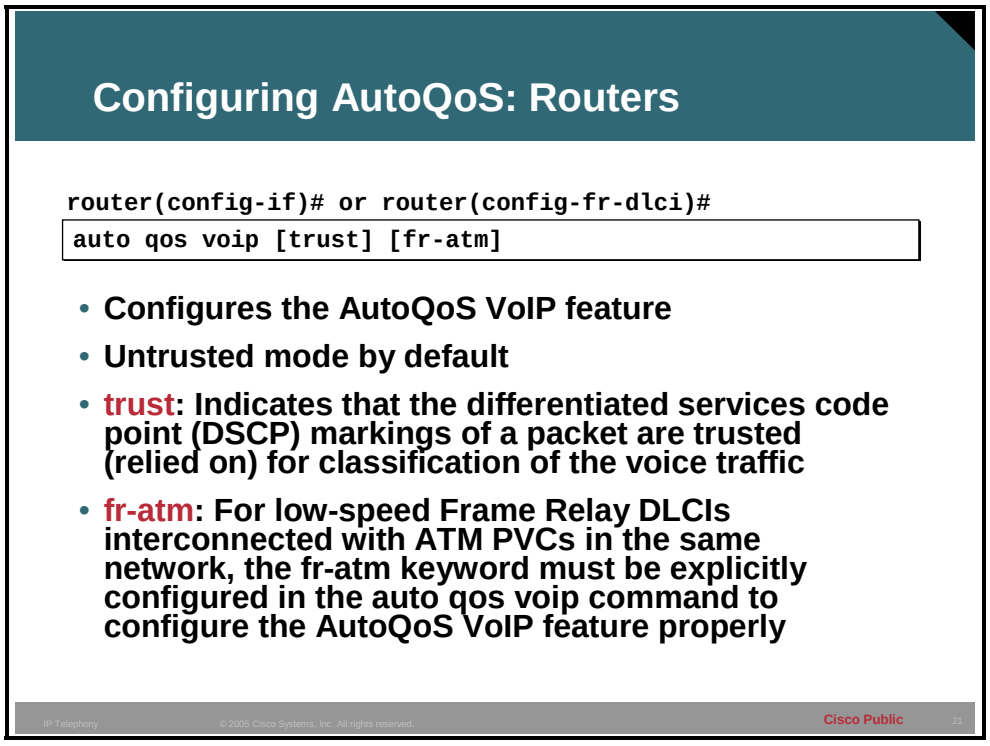
In addition to the AutoQoS prerequisites, the following are recommendations and requirements when configuring AutoQoS. Be aware that these may change with Cisco IOS releases and should be verified before implementing AutoQoS in your environment.

 Copyright © 2005, Cisco Systems, Inc.

- Cisco AutoQoS VoIP feature is supported only on the following interfaces and PVCs:
  - Serial interfaces with Point-to-Point (PPP) or High-Level Data Link Control (HDLC)
  - Frame Relay DLCIs (point-to-point sub-interfaces only)
    - Cisco AutoQoS does not support Frame Relay multipoint interfaces
  - ATM PVCs
- Configuration template (CLI) generated by configuring Cisco AutoQoS on an interface or PVC can be tuned manually (via CLI configuration) if desired.
- Cisco AutoQoS cannot be configured if a QoS service-policy is already configured and attached to the interface or PVC.
- Multi-link PPP (MLP) is configured automatically for a serial interface with low-speed link. The serial interface must have an IP address and this IP address is removed and put on the MLP bundle. Cisco AutoQoS VoIP must also be configured on the other side of the link
- The **no auto qos voip** command removes Cisco AutoQoS. However, if the interface or PVC Cisco AutoQoS generated QoS configuration is deleted without configuring the **no auto qos voip** command, Cisco AutoQoS VoIP will not be completely removed from the configuration properly.
- Cisco AutoQoS SNMP traps are only delivered when an SNMP server is used in conjunction with Cisco AutoQoS.
- The SNMP community string "AutoQoS" should have "write" permissions.
- If the device is reloaded with the saved configuration after configuring Cisco AutoQoS and saving the configuration to NVRAM, some warning messages may be generated by RMON threshold commands. These warnings messages can be ignored (to avoid further warning messages, save the configuration to NVRAM again without making any changes to the QoS configuration).
- By default, Cisco 7200 Series routers and below that support MQC QoS, reserve up to 75% of the interface bandwidth for user defined classes. The remaining bandwidth is used for the default class. However, the entire remaining bandwidth is not guaranteed to the default class. This bandwidth is shared proportionately between the different flows in the default class and excess traffic from other bandwidth classes. At least one percent of the available bandwidth is reserved and guaranteed for class default traffic by default (up to 99% can be allocated to the other classes) on Cisco 7500 Series Routers

Configuring AutoQoS

This topic describes how to configure AutoQoS.



To configure the AutoQoS VoIP feature on an interface, use the **auto qos voip** command in interface configuration mode or Frame Relay DLCI configuration mode. To remove the AutoQoS VoIP feature from an interface, use the **no** form of the **auto qos voip** command.

auto qos voip [trust] [fr-atm]

no auto qos voip [trust] [fr-atm]

Syntax Description

Parameter	Description
trust	(Optional) Indicates that the differentiated services code point (DSCP) markings of a packet are trusted (relied on) for classification of the voice traffic. If the optional trust keyword is not specified, the voice traffic is classified using Network-Based Application Recognition (NBAR), and the packets are marked with the appropriate DSCP value.
fr-atm	(Optional) Enables the AutoQoS – VoIP feature for the Frame Relay-to-ATM links. This option is available on the Frame Relay data-link connection identifiers (DLCIs) for Frame Relay-to-ATM interworking only.

 Copyright © 2005, Cisco Systems, Inc.

The bandwidth of the serial interface is used to determine the speed of the link. The speed of the link is one element used to determine the configuration generated by the AutoQoS VoIP feature. The AutoQoS VoIP feature uses the bandwidth at the time the feature is configured and does not respond to changes made to bandwidth after the feature is configured.

For example, if the auto **qos voip** command is used to configure the AutoQoS VoIP feature on an interface with 1000 Kbps, the AutoQoS VoIP feature generates configurations for high-speed interfaces. However, if the bandwidth is later changed to 500 Kbps, the AutoQoS VoIP feature will not use the lower bandwidth. The AutoQoS VoIP feature retains the higher bandwidth and continues to use the generated configurations for high-speed interfaces.

To force the AutoQoS VoIP feature to use the lower bandwidth (and thus generate configurations for the low-speed interfaces), use the **no auto qos voip** command to remove the AutoQoS VoIP feature and then reconfigure the feature.

Example: Configuring the AutoQoS VoIP Feature on a High-Speed Serial Interface

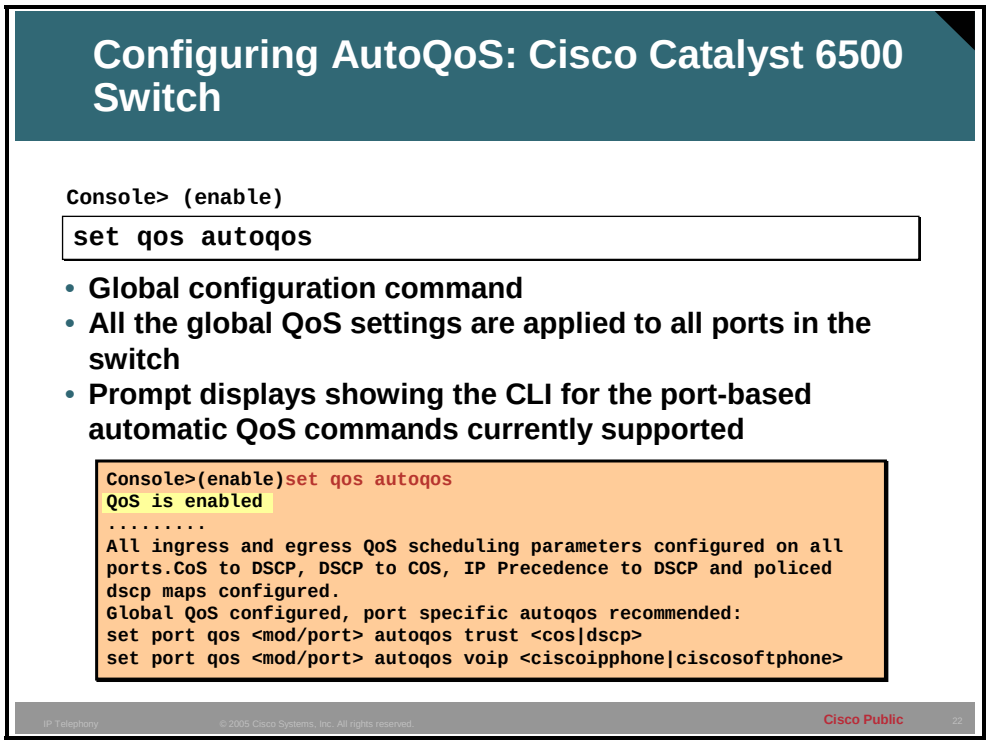
In this example, the AutoQoS VoIP feature is configured on the high-speed serial interface s1/2.

```
Router> enable
Router# configure terminal
Router(config)# interface s1/2
Router(config-if)# bandwidth 1540
Router(config-if)# ip address 10.10.100.1 255.255.255.0
Router(config-if)# auto qos voip
Router(config-if)# exit
```

Example: Configuring the AutoQoS VoIP Feature on a Low-Speed Serial Interface Example

In this example, the AutoQoS VoIP feature is configured on the low-speed serial interface s1/3.

```
Router# configure terminal
Router(config)# interface s1/3
Router(config-if)# bandwidth 512
Router(config-if)# ip address 10.10.100.1 255.255.255.0
Router(config-if# auto qos voip
Router(config-if)# exit
```



When you execute the global automatic QoS macro, all the global QoS settings are applied to all ports in the switch. After completion, a prompt displays showing the CLI for the port-based automatic QoS commands currently supported.

 Copyright © 2005, Cisco Systems, Inc.

Configuring AutoQoS: Cisco Catalyst 6500 Switch (Cont.)

```
Console> (enable)
set port qos autoqos <mod/port> trust [cos|dscp]
```

- **trust dscp and trust cos are automatic QoS keywords used for ports requiring a "trust all" type of solution.**
- **trust dscp should be used only on ports that connect to other switches or known servers as the port will be trusting all inbound traffic marking Layer 3 (DSCP)**
- **trust cos should only be used on ports connecting other switches or known servers as the port trusts all inbound traffic marking in Layer 2 (CoS).**
- **The trusted boundary feature is disabled and no QoS policing is configured on these types of ports**

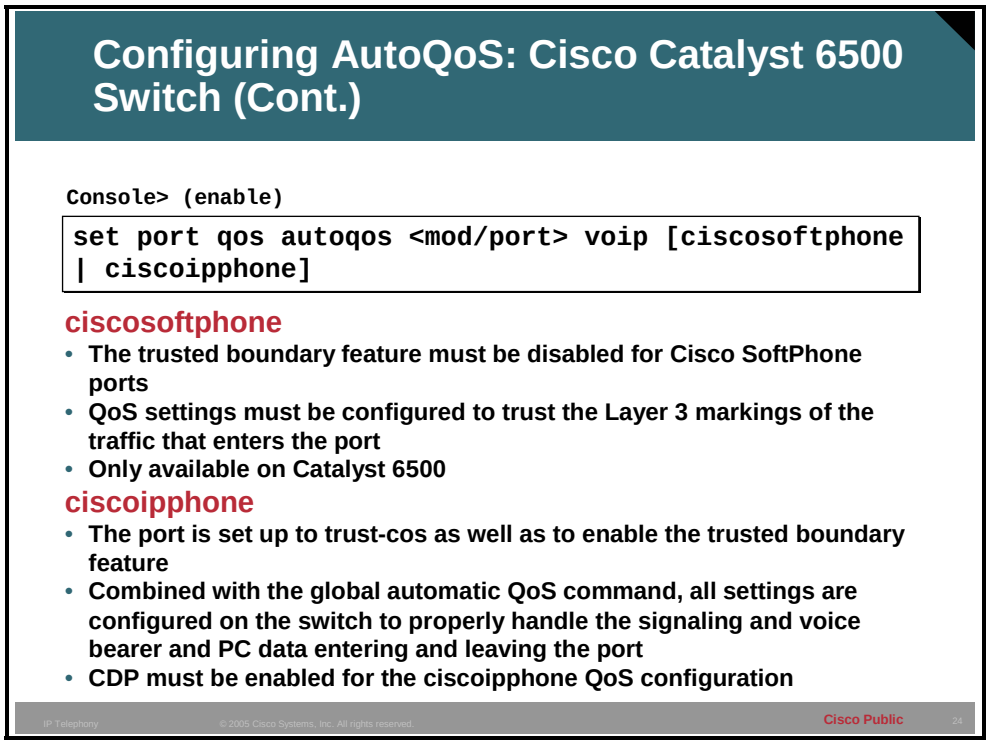
IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 23

The port-specific automatic QoS macro handles all inbound QoS configuration that is specific to a particular port.

The QoS ingress port specific settings include port trust, default CoS, classification, and policing but does not include scheduling. Input scheduling is programmed through the global automatic QoS macro. Together with the global automatic QoS macro command, all QoS settings are configured properly for a specific QoS traffic type.

Any existing QoS ACLs that are already associated with a port are removed if AutoQoS modifies ACL mappings on that port. The ACL names and instances are not changed.

If the trust dscp or trust cos keywords are used, the trusted boundary feature is disabled. This means an IP Phone will not rewrite the dscp or cos values from an attached PC.



The port-specific automatic QoS macro accepts a *mod/port* combination and must include an AVVID-type keyword. The **ciscoipphone**, **ciscosoftphone**, and **trust** keywords are supported.

With the **ciscoipphone** keyword, the port is set up to trust-cos as well as to enable the trusted boundary feature. Combined with the global automatic QoS command, all settings are configured on the switch to properly handle the signaling and voice bearer and PC data entering and leaving the port.

In addition to the switch-side QoS settings covered by the global automatic QoS command, the phone has a few QoS features that need to be configured for proper labeling to occur. QoS configuration information is sent to the phone through CDP from the switch. The QoS values that need to be configured are the trust settings of the "PC port" on the phone (trust or untrusted) and the CoS value that is used by the phone to remark packets in case the port is untrusted (ext-cos).

Only the Catalyst 6500 supports AutoQoS for Cisco SoftPhone. On the ports that connect to a Cisco SoftPhone, QoS settings must be configured to trust the Layer 3 markings of the traffic that enters the port. Trusting all Layer 3 markings is a security risk because PC users could send non-priority traffic with DSCP 46 and gain unauthorized performance benefits. Although not configured by AutoQos, policing on all inbound traffic can be used to prevent malicious users from obtaining unauthorized bandwidth from the network. Policing is accomplished by rate limiting the DSCP 46 (EF) inbound traffic to the codec rate used by the Cisco SoftPhone application (worst case G.723). Any traffic that exceeds this rate is marked down to the default traffic rate (DSCP 0 - BE). Signaling traffic (DSCP 24) is also policed and marked down to zero if excess signaling traffic is detected. All other inbound traffic types are reclassified to default traffic (DSCP 0 - BE).

Note	You must disable the trusted boundary feature for Cisco SoftPhone ports.

 Copyright © 2005, Cisco Systems, Inc.

Example: Using the Port-Specific AutoQoS Macro

This example shows how to use the **ciscoipphone** keyword:

```
Console> (enable) set port qos 3/1 autoqos help
Usage: set port qos <mod/port> autoqos trust <cos|dscp>
set port qos <mod/port> autoqos voip
<ciscoipphone|ciscosoftphone>
Console> (enable) set port qos 3/1 autoqos voip ciscoipphone
Port 3/1 ingress QoS configured for Cisco IP Phone.
It is recommended to execute the "set qos autoqos" global
command if not executed previously.
Console> (enable)
```

This example shows how to use the **ciscosoftphone** keyword:

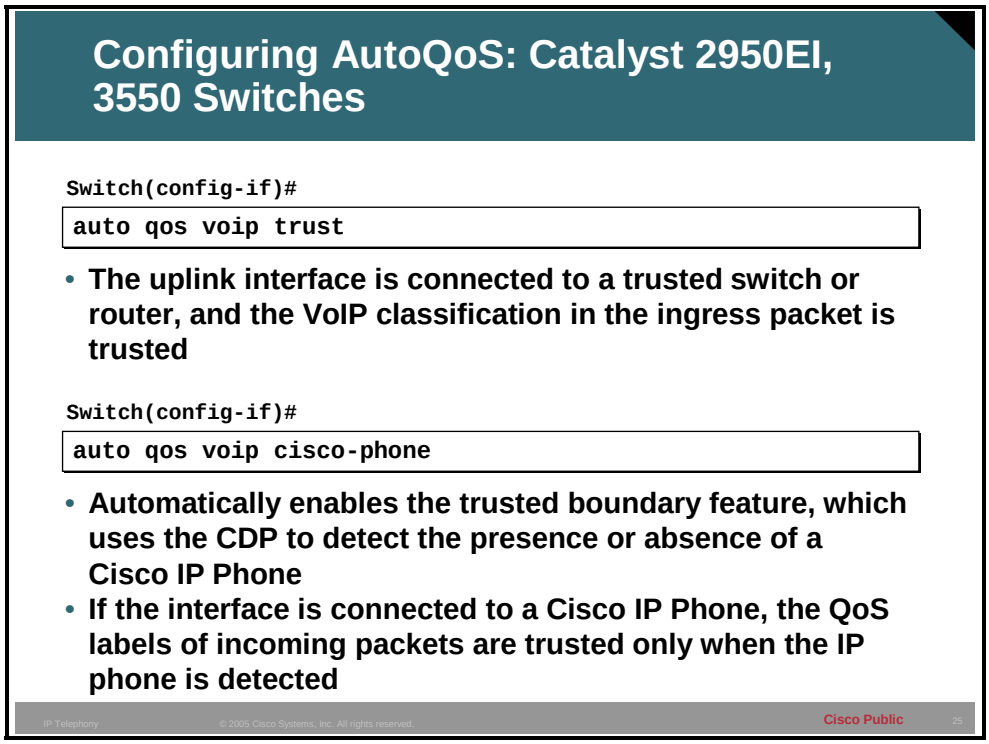
```
Console> (enable) set port qos 3/1 autoqos voip ciscosoftphone
Port 3/1 ingress QoS configured for Cisco Softphone.
It is recommended to execute the "set qos autoqos" global
command if not executed previously.
Console> (enable)
```

This example shows how to use the **trust cos** keyword:

```
Console> (enable) set port qos 3/1 autoqos trust cos
Port 3/1 QoS configured to trust all incoming CoS marking.
It is recommended to execute the "set qos autoqos" global
command if not executed previously.
Console> (enable)
```

This example shows how to use the **trust dscp** keyword:

```
Console> (enable) set port qos 3/1 autoqos trust dscp
Port 3/1 QoS configured to trust all incoming DSCP marking.
It is recommended to execute the "set qos autoqos" global
command if not executed previously.
Console> (enable)
```



When you enable the AutoQoS feature on the first interface, QoS is globally enabled (**mls qos** global configuration command).

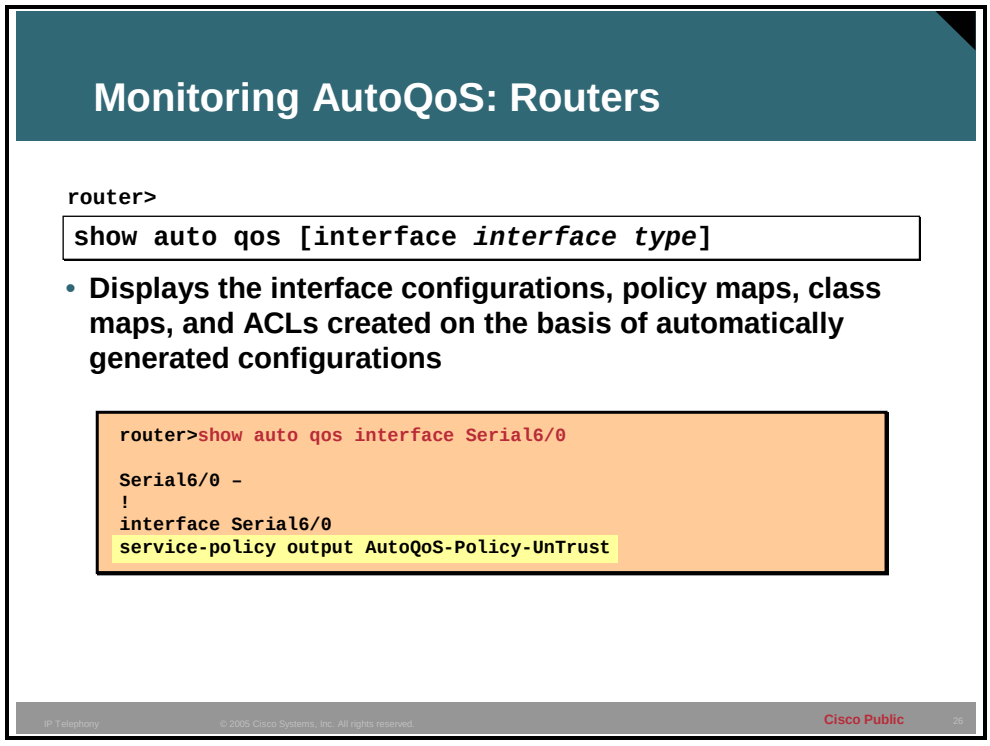
When you enter the **auto qos voip trust** interface configuration command, the ingress classification on the interface is set to trust the CoS QoS label received in the packet, and the egress queues on the interface are reconfigured. QoS Labels in ingress packets are trusted

When you enter the **auto qos voip cisco-phone** interface configuration command, the trusted boundary feature is enabled. It uses the Cisco Discovery Protocol (CDP) to detect the presence or absence of a Cisco IP phone. When a Cisco IP phone is detected, the ingress classification on the interface is set to trust the QoS label received in the packet. When a Cisco IP phone is absent, the ingress classification is set to not trust the QoS label in the packet. The egress queues on the interface are also reconfigured. This command extends the trust boundary if IP Phone detected.

 Copyright © 2005, Cisco Systems, Inc.

Monitoring AutoQoS

This topic describes the commands used to monitor AutoQoS configurations.



When the **auto qos voip** command is used to configure the AutoQoS VoIP feature, configurations are generated for each interface or permanent virtual circuit (PVC). These configurations are then used to create the interface configurations, policy maps, class maps, and access control lists (ACLs). The **show auto qos** command can be used to verify the contents of the interface configurations, policy maps, class maps, and ACLs.

The **show auto qos interface** command can be used with Frame Relay data-link connection identifiers (DLCIs) and ATM PVCs.

When the **interface** keyword is used along with the corresponding interface type argument, the **show auto qos interface** [*interface type*] command displays the configurations created by the AutoQoS VoIP feature on the specified interface.

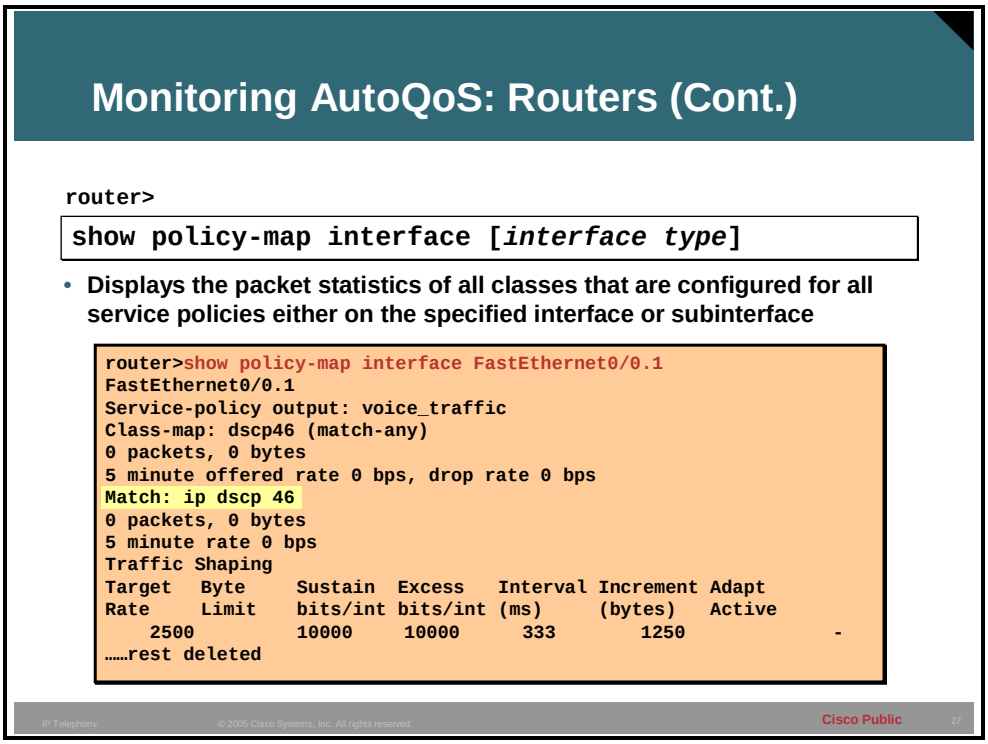
When the **interface** keyword is used but an interface type is not specified, the **show auto qos interface** command displays the configurations created by the AutoQoS VoIP feature on all the interfaces or PVCs on which the AutoQoS VoIP feature is enabled.

Example: Show Auto QoS and Show Auto QoS Interface

The **show auto qos** command displays all of the configurations created by the AutoQoS VoIP feature.

```
Router# show auto qos
Serial6/1.1: DLCI 100 -
!
interface Serial6/1
frame-relay traffic-shaping
!
interface Serial6/1.1 point-to-point
frame-relay interface-dlci 100
class AutoQoS-VoIP-FR-Serial6/1-100
frame-relay ip rtp header-compression
!
map-class frame-relay AutoQoS-VoIP-FR-Serial6/1-100
frame-relay cir 512000
frame-relay bc 5120
frame-relay be 0
frame-relay mincir 512000
service-policy output AutoQoS-Policy-UnTrust
frame-relay fragment 640
```

 Copyright © 2005, Cisco Systems, Inc.



To display the configuration of all classes configured for all service policies on the specified interface or to display the classes for the service policy for a specific permanent virtual circuit (PVC) on the interface, use the **show policy-map interface** EXEC or privileged EXEC command.

show policy-map interface interface-name [**vc** [***vpi/***] ***vci***][**dlci** ***dlci***] [**input | output**]

Monitoring AutoQoS: Switches

```
Switch#
show auto qos [interface interface-id]
```

- **Displays the auto-QoS configuration that was initially applied**
- **Does not display any user changes to the configuration that might be in effect**

```
Switch#show auto qos
Initial configuration applied by AutoQoS:
wrr-queue bandwidth 20 1 80 0
no wrr-queue cos-map
wrr-queue cos 1 0 1 2 4
wrr-queue cos 3 3 6 7
wrr-queue cos 4 5
mls qos map cos-dscp 0 8 16 26 32 46 48 56
!
interface FastEthernet0/3
mls qos trust device cisco-phone
mls qos trust cos
```

IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 28

To display the inital auto-QoS configuration, use the **show auto qos** [**interface** [*interface-id*]] privileged EXEC command. To display any user changes to that configuration, use the **show running-config** privileged EXEC command. You can compare the **show auto qos** and the **show running-config** command output to identify the user-defined QoS settings.

 Copyright © 2005, Cisco Systems, Inc.

Monitoring AutoQoS: Switches (Cont.)

```
Switch#
show mls qos interface [interface-id | vlan vlan-id]
[buffers | policers | queueing | statistics]
[ | {begin | exclude | include} expression]
```

- **Displays QoS information at the interface level**

```
Switch#show mls qos interface gigabitethernet0/1 statistics
Ingress
    dscp: incoming  no_change     classified      policed        dropped (in bytes)
      1 : 0         0             0               0              0
Others: 203216935   24234242      178982693       0              0

Egress
    dscp: incoming  no_change     classified      policed       dropped (in bytes)
      1 : 0         n/a           n/a             0             0

WRED drop counts:
      qid           thresh1   thresh2   FreeQ
     1 :  0         0         1024
     2 :  0         0         1024
……rest deleted
```

IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 29

Display QoS information at the interface level, including the configuration of the egress queues and the CoS-to-egress-queue map, which interfaces have configured policers, and ingress and egress statistics (including the number of bytes dropped).

If no keyword is specified with the **show mls qos interface** command, the port QoS mode (DSCP trusted, CoS trusted, untrusted, and so forth), default class of service (CoS) value, DSCP-to-DSCP-mutation map (if any) attached to the port, and policy map (if any) attached to the interface are displayed. If a specific interface is not specified, the information for all interfaces is displayed.

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* are not displayed, but the lines that do not contain *output* are displayed.

Monitoring AutoQoS: Switches (Cont.)

```
Switch#
show mls qos maps [cos-dscp | dscp-cos | dscp-
mutation dscp-mutation-name | dscp-switch-priority |
ip-prec-dscp | policed-dscp] [ | {begin | exclude |
include} expression
```

- **Maps are used to generate an internal Differentiated Services Code Point (DSCP) value, which represents the priority of the traffic**

```
Switch#show mls qos maps dscp-cos

Dscp-cos map:
   dscp: 0 8 10 16 18 24 26 32 34 40 46 48 56
         ------------------------------------------
    cos: 0 1 1 2 2 3 7 4 4 5 5 7 7
```

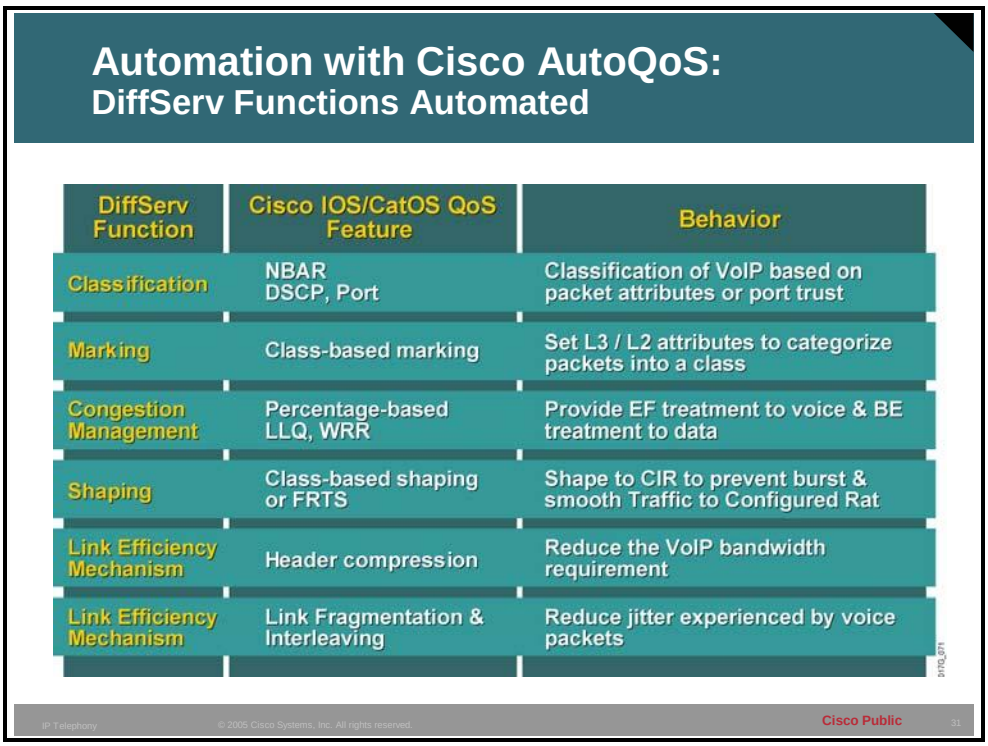
IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 30

This command shows the current mapping of DSCP to CoS.

 Copyright © 2005, Cisco Systems, Inc.

Automation with Cisco AutoQoS

This topic identifies several of the QoS technologies that are automatically implemented on the network when using AutoQoS.



Cisco AutoQoS performs the following functions:

WAN:

- Automatically classify RTP payload and VoIP control packets (H.323, H.225 Unicast, Skinny, SIP, MGCP)
- Build service policies for VoIP traffic that are based on Cisco Modular QoS CLI (MQC)
- Provision Low Latency Queuing (LLQ) - Priority Queuing for VoIP bearer and bandwidth guarantees for control traffic
- Enable WAN traffic shaping that adheres to Cisco best practices, where required
- Enable link efficiency mechanisms, such as Link Fragmentation and Interleaving (LFI), and RTP header compression (cRTP) where required
- Provide SNMP and SYSLOG alerts for VoIP packet drops

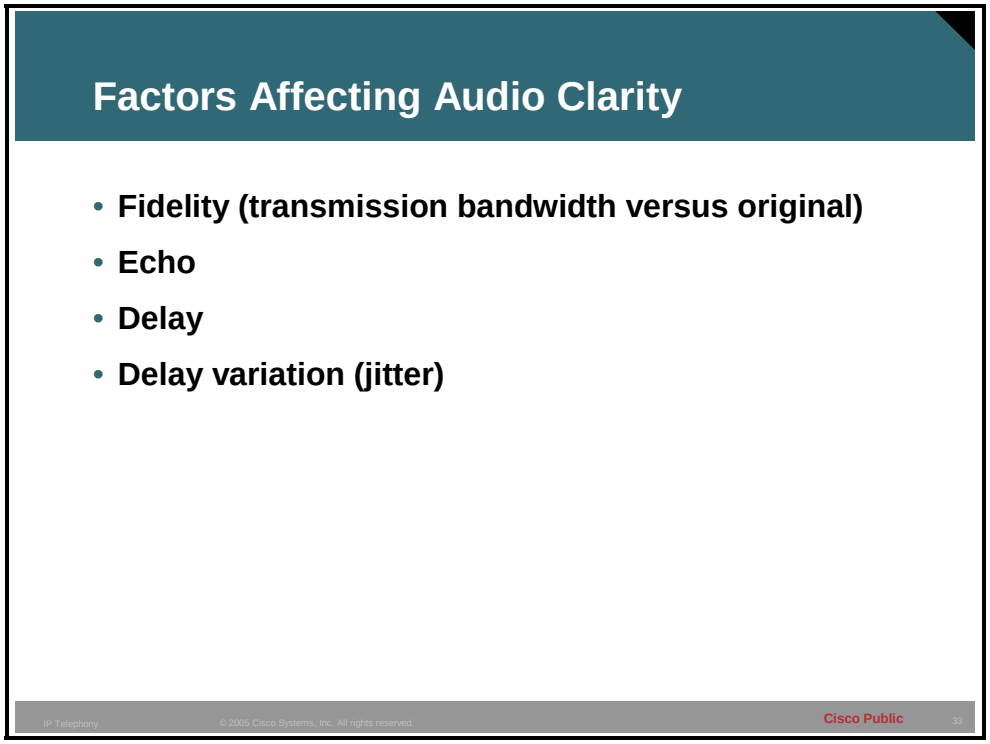
LAN:

- Enforce the trust boundary on Cisco Catalyst switch access ports and uplinks/downlinks
- Enable Cisco Catalyst strict priority queuing (also known as expedite queuing) with weighted round robin (WRR) scheduling for voice and data traffic, where appropriate
- Configure queue admission criteria (Map CoS values in incoming packets to the appropriate queues)
- Modify queue sizes and weights where required

Comparing Voice Quality Measurement Standards

Audio Clarity

The effectiveness of a telephone conversation depends on its clarity. If the conversation does not sound good, the listener is annoyed and the speaker is unable to express the message. The clarity of the conversation must be maintained end-to-end, from the speaker to the listener. This topic lists the factors affecting audio clarity.



The clarity, or cleanliness and crispness, of the audio signal is of utmost importance. The listener should recognize the identity of the speaker and sense the mood. Factors that can affect clarity include:

- **Fidelity:** Consistency of transmission bandwidth to the original bandwidth. The bandwidth of the transmission medium almost always limits the total bandwidth of the spoken voice. Human speech typically requires a bandwidth from 100 to 10,000 Hz, although 90 percent of speech intelligence is contained between 100 and 3000 Hz.
- **Echo:** A result of electrical impedance mismatches in the transmission path. Echo is always present. The two components that affect echo are amplitude (loudness of the echo) and delay (the time between the spoken voice and the echoed sound). You can control echo using suppressors or cancellers.
- **Delay:** The time between the spoken voice and the arrival of the electronically delivered voice at the far end. Delay is affected by a number of factors, including distance (propagation delay), coding, compression, serialization, and buffers.

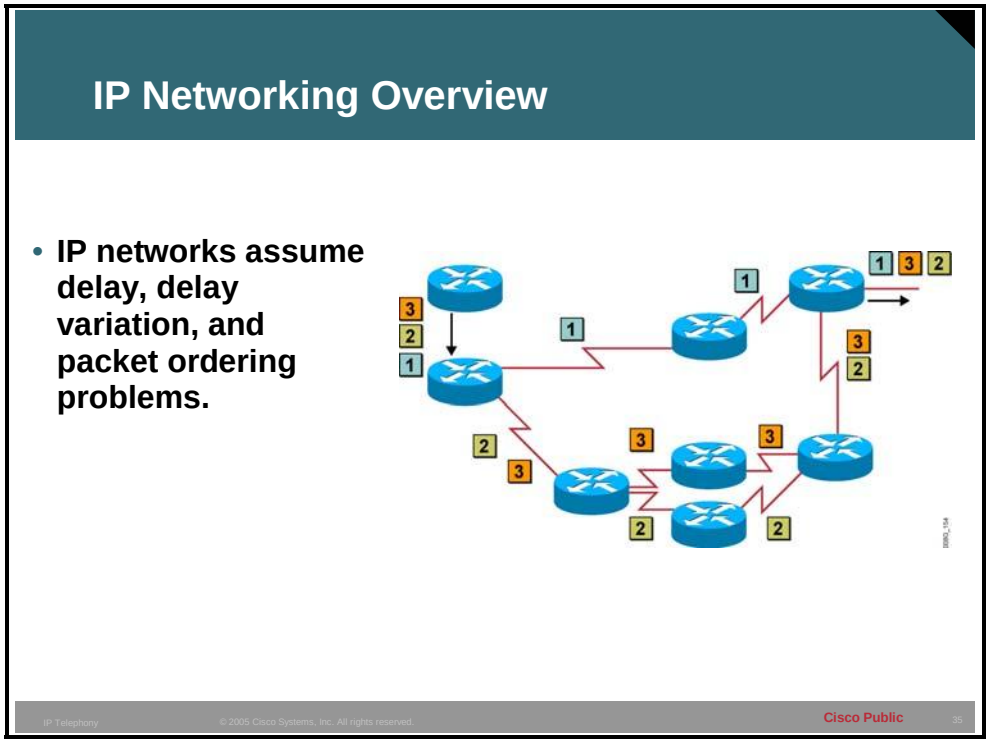
 Copyright © 2005, Cisco Systems, Inc.

- **Delay variation:** Because of the nature of an IP delivery network, the arrival of coded speech at the far end of a Voice over IP (VoIP) network can vary. The varying arrival time of the packets can cause gaps in the re-creation and playback of the voice signal. These gaps are undesirable and cause the listener great annoyance. Delay is induced in the network by variation in the routes of individual packets, contention, or congestion. You can solve variable delay by using dejitter buffers.

VoIP Challenges

IP Networking Overview

This topic provides an overview of IP networking and some of the inherent challenges when conveying voice over an IP network.



IP is a connectionless network protocol. Connectionless networks generally do not participate in signaling. The concept of session establishment exists between end systems, although the connectionless network remains unaware of the virtual circuit (VC).

IP resides at the network layer of the Open System Interconnection (OSI) protocol stack. Therefore, it can transport IP packets over deterministic and nondeterministic Layer 2 protocols, such as Frame Relay or ATM. IP can be used to communicate across any set of interconnected networks and is equally suited to both LAN and WAN communication.

IP information is transferred in a sequence of datagrams. A message is sent as a series of datagrams that are reassembled into the completed message at the receiving location. Because a voice conversation that is transported in IP can be considered a continuous audio file, all packets must be received in sequence immediately and without interpacket variable delay.

Traditionally, IP traffic transmits on a FIFO basis. Different packet types vary in size, allowing large file transfers to take advantage of the efficiency that is associated with larger packet sizes. FIFO queuing affects the way that voice packets transmit, causing delay and delay variation at the receiving end.

 Copyright © 2005, Cisco Systems, Inc.

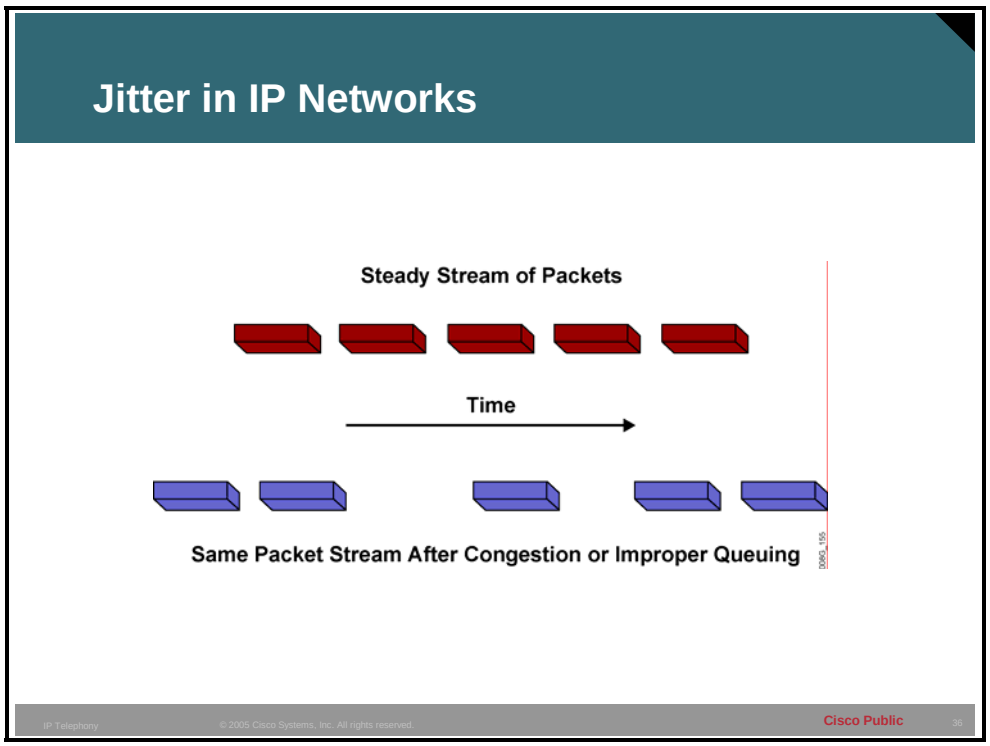
UDP is the connectionless transport layer protocol used for VoIP. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery. UDP requires that other protocols handle error processing and retransmission. The figure shows how packets may be received out of sequence or become completely lost at the receiving end.

Example: IP Networking

Due to the very nature of IP networking, voice packets sent across IP will be subject to certain transmission problems. These problems include jitter, delay, and packet ordering. In the figure, packets sent from the originating router on the left are in sequence and sent with predictable transmission intervals. As they traverse the IP network, the routing protocol may send some of the packets through one path, while other packets traverse a different path. As the packets arrive at the destination router on the right, they arrive with varying delays and out of sequence. These problems must be addressed with QoS mechanisms explained further in this lesson.

Jitter

This topic describes the occurrence of jitter in IP networks and the Cisco Systems solution to this problem.



Jitter is defined as a variation in the delay of received packets. On the sending side, packets are sent in a continuous stream with the packets spaced evenly apart. Because of network congestion, improper queuing, or configuration errors, this steady stream can become lumpy, or the delay between each packet can vary instead of remaining constant, as displayed in the figure.

When a router receives an audio stream for VoIP, it must compensate for the jitter that is encountered. The mechanism that handles this function is the playout delay buffer, or dejitter buffer. The playout delay buffer must buffer these packets and then play them out in a steady stream to the digital signal processors (DSPs) to be converted back to an analog audio stream. The playout delay buffer, however, affects overall absolute delay.

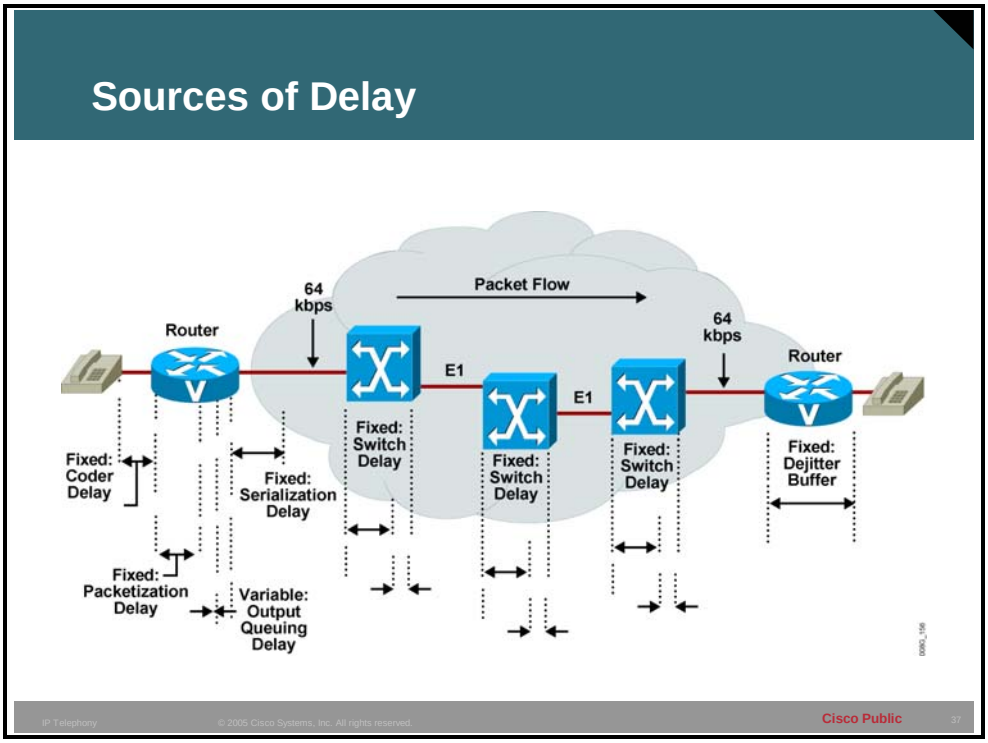
Example: Jitter in Voice Networks

When a conversation is subjected to jitter, the results can be clearly heard. If the talker says, “Watson, come here. I want you,” the listener might hear, “Wat….s…on…….come here, I……wa……nt……..y……ou.” The variable arrival of the packets at the receiving end causes the speech to be delayed and garbled.

 Copyright © 2005, Cisco Systems, Inc.

Delay

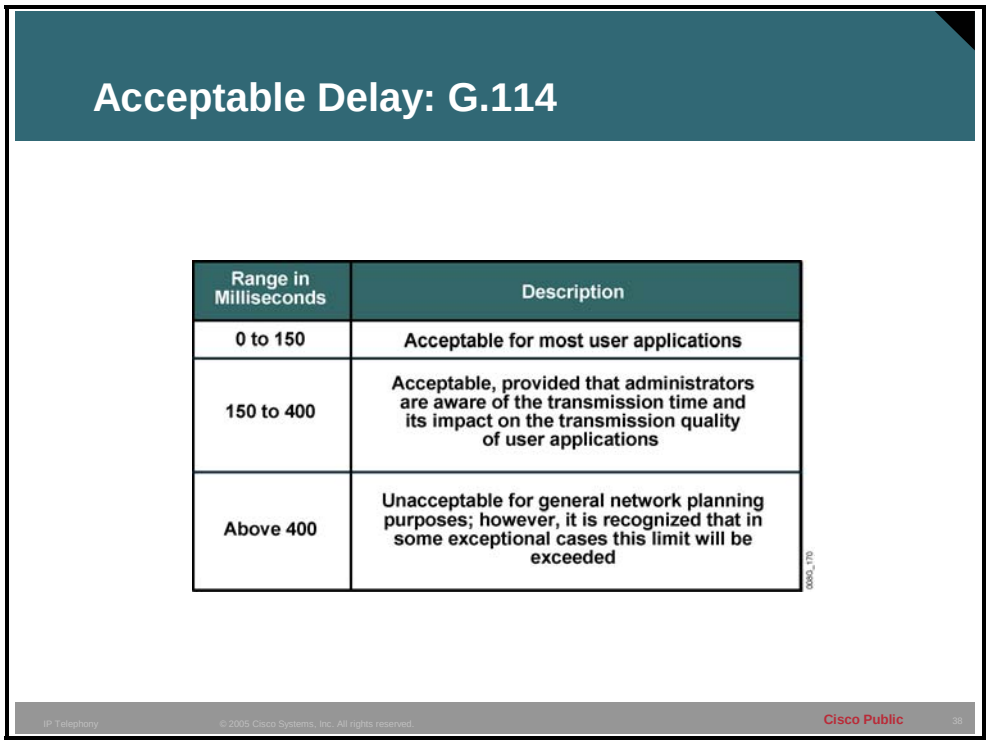
Overall or absolute delay can affect VoIP. You might have experienced delay in a telephone conversation with someone on a different continent. The delays can be very frustrating, causing words in the conversation to be cut off. This topic describes the causes of packet delay and the Cisco solution to this problem.



When you design a network that transports voice over packet, frame, or cell infrastructures, it is important to understand and account for the delay components in the network. You must also correctly account for all potential delays to ensure that overall network performance is acceptable. Overall voice quality is a function of many factors, including the compression algorithm, errors and frame loss, echo cancellation, and delay.

There are two distinct types of delay:

- Fixed-delay components add directly to the overall delay on the connection.
- Variable delays arise from queuing delays in the egress trunk buffers that are located on the serial port that is connected to the WAN. These buffers create variable delays, called jitter, across the network.



The ITU considers network delay for voice applications in Recommendation G.114. This recommendation defines three bands of one-way delay, as shown in the table in the figure.

Note	This recommendation is for connections with echo that are adequately controlled, implying that echo cancellers are used. Echo cancellers are required when one-way delay exceeds 25 ms (G.131).

This recommendation is oriented toward national telecommunications administrations, and therefore is more stringent than recommendations that would normally be applied in private voice networks. When the location and business needs of end users are well known to a network designer, more delay may prove acceptable. For private networks, a 200-ms delay is a reasonable goal and a 250-ms delay is a limit. This goal is what Cisco Systems proposes as reasonable as long as jitter does not impact voice quality. However, all networks must be engineered so that the maximum expected voice connection delay is known and minimized.

Example: Acceptable Delay

The G.114 recommendation is for one-way delay only and does not account for round-trip delay. Network design engineers must consider all delays, variable and fixed. Variable delays include queuing and network delays, while fixed delays include coder, packetization, serialization, and dejitter buffer delays. The table is an example of calculating delay budget.

 Copyright © 2005, Cisco Systems, Inc.

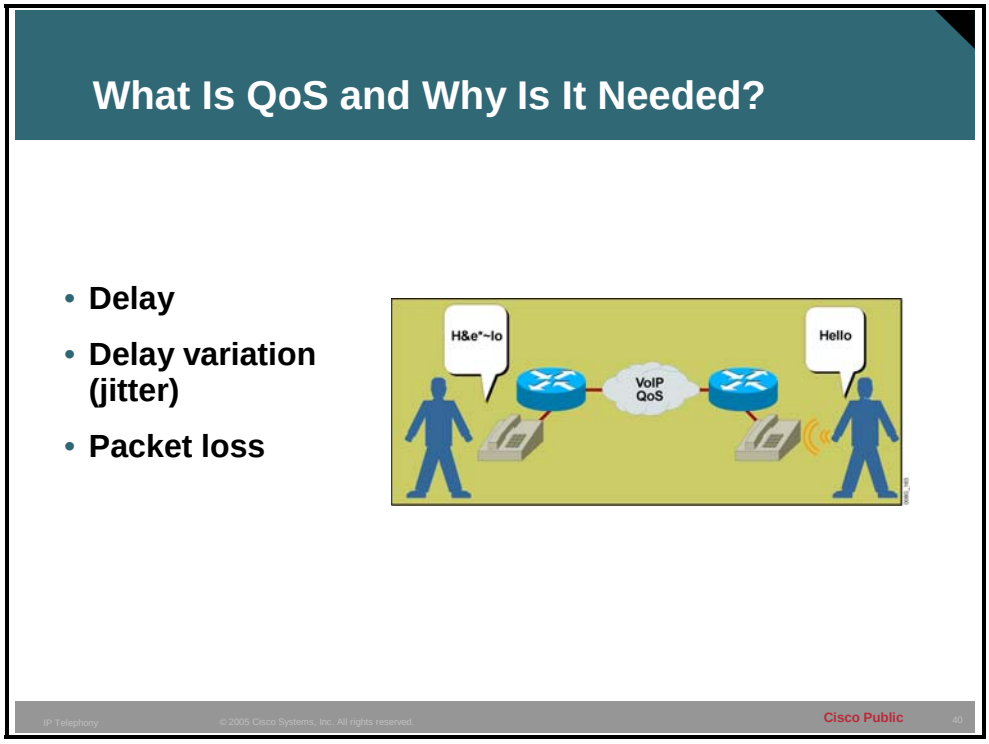
Calculating Delay Budget

Delay Type	Fixed (ms)	Variable (ms)
Coder delay	18	
Packetization delay	30	
Queuing and buffering		8
Serialization (64 kbps)	5	
Network delay (public frame)	40	25
Dejitter buffer	45	
Totals	138	33

QoS and Good Design

Need for QoS Mechanisms

This topic describes problems associated with transmitting voice over a data network and the need for QoS in such a network.

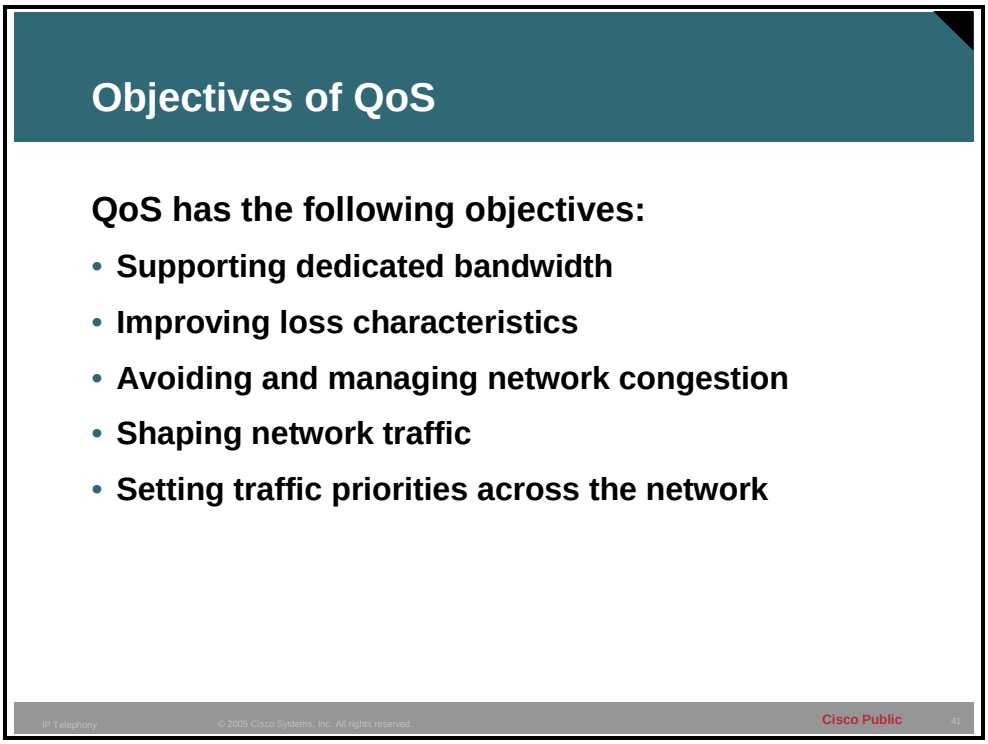


Real-time applications, such as voice applications, have different characteristics and requirements than traditional data applications. Voice applications tolerate little variation in the amount of delay. This delay variation affects delivery of voice packets. Packet loss and jitter degrade the quality of the voice transmission that is delivered to the recipient. The figure shows how these problems can affect a voice message.

 Copyright © 2005, Cisco Systems, Inc.

Objectives of QoS

To ensure that VoIP is a realistic replacement for standard PSTN telephony services, customers must receive the same consistently high quality of voice transmission that they receive with basic telephone services. This topic discusses how QoS can help you achieve this objective.



Like other real-time applications, VoIP is extremely sensitive to issues related to bandwidth and delay. To ensure that VoIP transmissions are intelligible to the receiver, voice packets cannot be dropped, excessively delayed, or subject to variations in delay, or jitter.

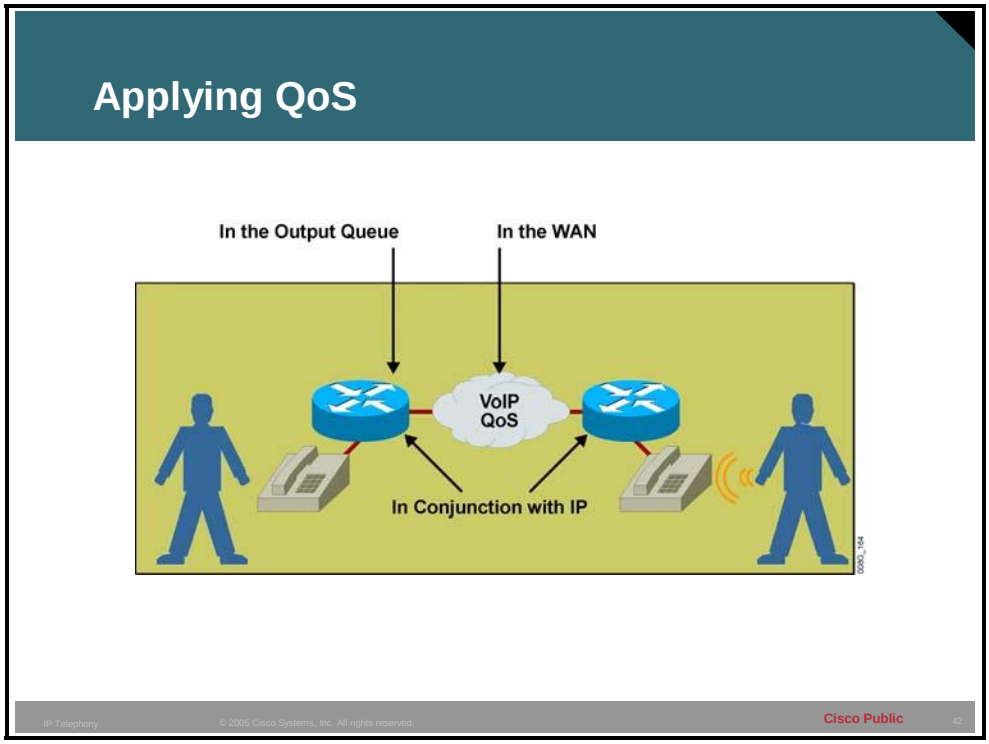
Example: QoS Objectives

VoIP guarantees high-quality voice transmission only if the signaling and audio channel packets have priority over other kinds of network traffic. To deploy VoIP, you must provide an acceptable level of voice quality by meeting VoIP traffic requirements for issues related to bandwidth, latency, and jitter. QoS provides better, more predictable network service by performing the following:

- **Supporting dedicated bandwidth:** Designing the network such that speeds and feeds can support the desired voice and data traffic
- **Improving loss characteristics:** Designing the Frame Relay network such that discard eligibility is not a factor, keeping voice below committed information rate (CIR)
- **Avoiding and managing network congestion:** Ensuring that the LAN and WAN infrastructure can support the volume of data traffic and voice calls
- **Shaping network traffic:** Using Cisco traffic-shaping tools to ensure smooth and consistent delivery of frames to the WAN
- **Setting traffic priorities across the network:** Marking the voice traffic as priority and queuing it first

Applying QoS for End-to-End Improvement of Voice Quality

Voice features for Cisco IOS QoS are deployed at different points in the network and designed for use with other QoS features to achieve specific goals, such as control over jitter and delay. This topic lists the network areas in which Cisco IOS QoS is implemented.



Cisco IOS software includes a complete set of features for delivering QoS throughout the network. Following are Cisco IOS features that address the voice packet delivery requirements of end-to-end QoS and service differentiation:

- In the output queue of the router:
  - **Class-based weighted fair queuing (CBWFQ):** Extends the standard weighted fair queuing (WFQ) functionality by providing support for user-defined traffic classes. You can create a specific class for voice traffic by using CBWFQ.
  - **Low Latency Queuing (LLQ):** Provides strict priority queuing on ATM VCs and serial interfaces. LLQ configures the priority status for a class within CBWFQ and is not limited to UDP port numbers (as in IP RTP priority). LLQ is considered a “best practice” by the Cisco Enterprise Solutions Engineering (ESE) group for delivering voice QoS services over a WAN.
  - **WFQ and distributed weighted fair queuing (DWFQ):** Segregates traffic into flows and then schedules traffic onto the outputs to meet specified bandwidth allocation or delay bounds.
  - **Weighted random early detection (WRED) and distributed weighted random early detection (DWRED):** Provides differentiated performance characteristics for different classes of service. This classification allows preferential handling of voice traffic under congestion conditions without worsening the congestion.

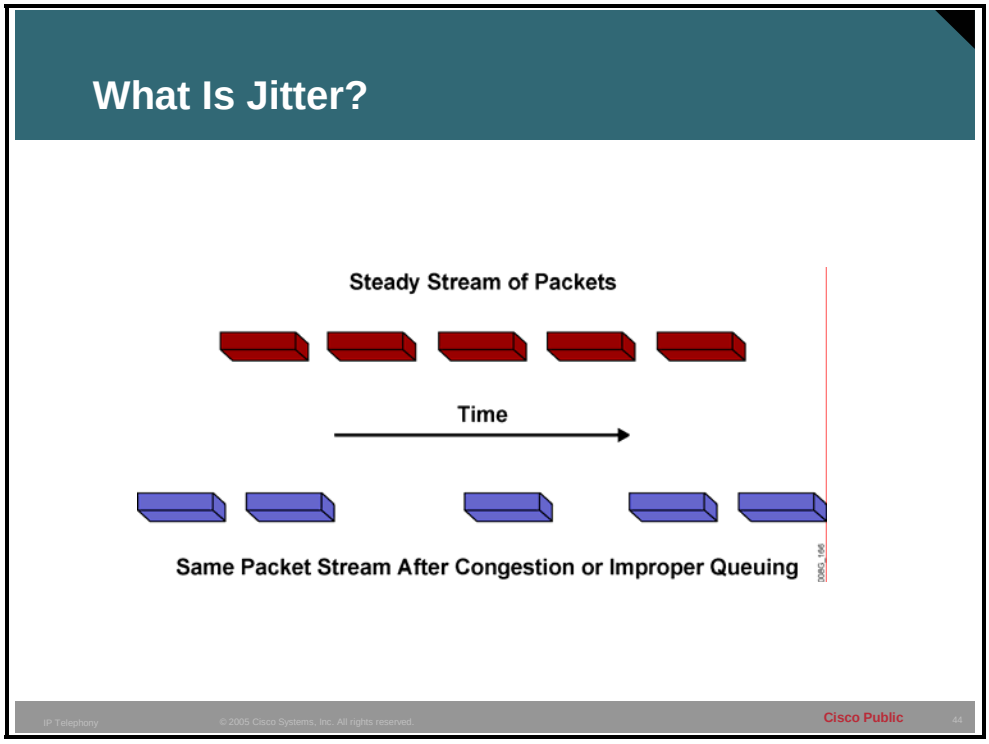
 Copyright © 2005, Cisco Systems, Inc.

- In the WAN or WAN protocol:
  - **Committed access rate (CAR):** Provides a rate-limiting feature for allocating bandwidth commitments and bandwidth limitations to traffic sources and destinations. At the same time, it specifies policies for handling the traffic that may exceed bandwidth allocation.
  - **Frame Relay traffic shaping (FRTS):** Delays excess traffic by using a buffer or queuing mechanism to hold packets and shape the flow when the data rate of the source is higher than expected.
  - **Frame Relay Forum Standard 12 (FRF.12):** Ensures predictability for voice traffic by providing better throughput on low-speed Frame Relay links. FRF.12 interleaves delay-sensitive voice traffic on one VC with fragments of a long frame on another VC that is using the same interface.
  - **IP to ATM class of service (CoS):** Includes a feature suite that maps CoS characteristics between the IP and ATM. It also offers differential service classes across the entire WAN—not just the routed portion—and gives mission-critical applications exceptional service during periods of high network usage and congestion.
  - **Multilink PPP (MLP) with link fragmentation and interleaving (LFI):** Allows large packets to be multilink-encapsulated and fragmented so that they are small enough to satisfy the delay requirements of real-time traffic. LFI also provides a special transmit queue for smaller, delay-sensitive packets, enabling them to be sent earlier than other flows.
- In conjunction with the IP operation:
  - **Compressed Real-Time Transport Protocol (CRTP):** Compresses the extensive RTP header when used in conjunction with RTP. The result is decreased consumption of available bandwidth for voice traffic and a corresponding reduction in delay.
  - **Resource Reservation Protocol (RSVP):** Supports the reservation of resources across an IP network, allowing end systems to request QoS guarantees from the network. For networks that support VoIP, RSVP—in conjunction with features that provide queuing, traffic shaping, and voice call signaling—provides Call Admission Control (CAC) for voice traffic.
  - **QoS policy propagation on Border Gateway Protocol (BGP):** Steadies BGP to distribute QoS policy to remote routers in a network. It allows classification of packets and then uses other QoS features, such as CAR and WRED, to specify and enforce business policies to fit a business model.

Jitter

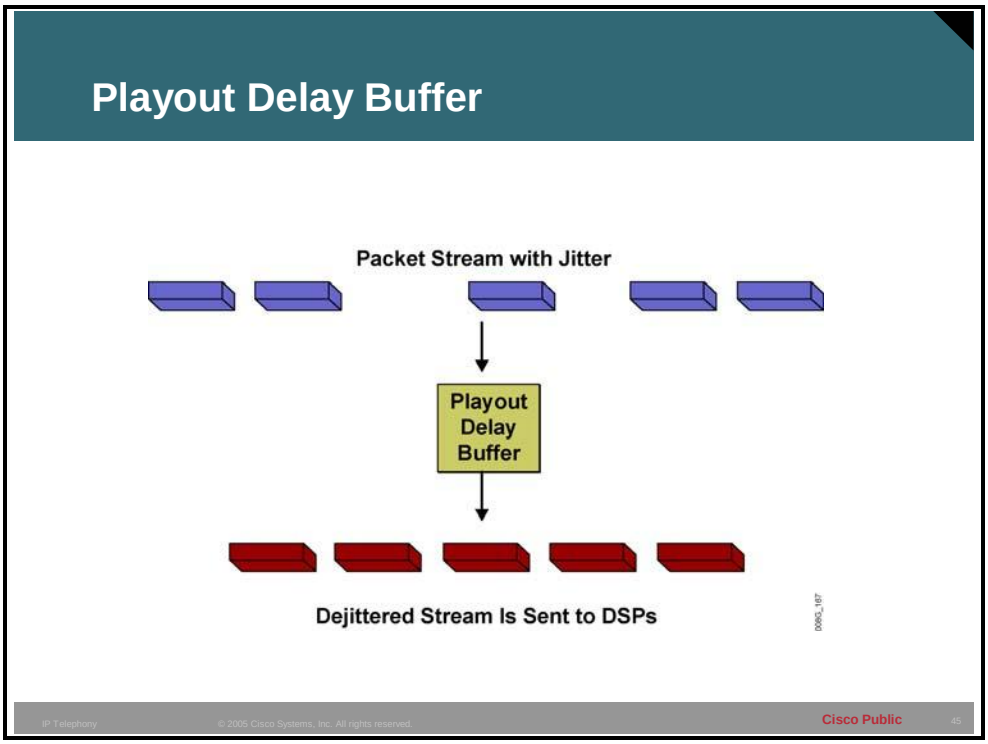
Understanding Jitter

Jitter is an undesirable effect caused by the inherent tendencies of TCP/IP networks and components. This topic describes the cause and effect of jitter.

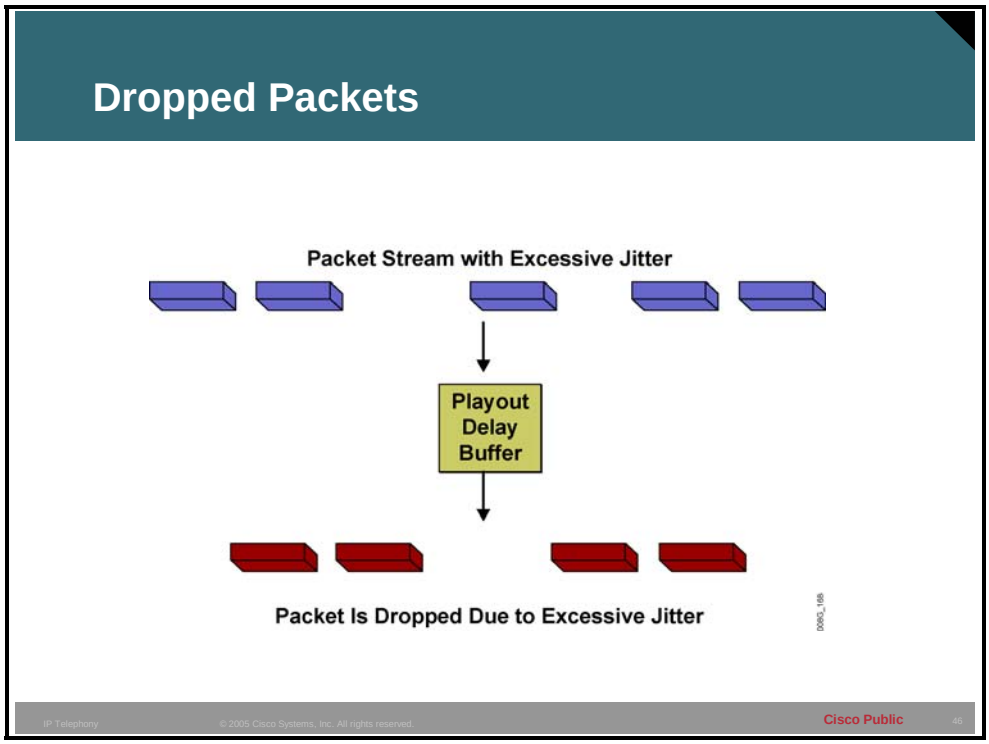


Jitter is defined as a variation in the delay of received packets. The sending side transmits packets in a continuous stream and spaces them evenly apart. Because of network congestion, improper queuing, or configuration errors, the delay between packets can vary instead of remaining constant, as shown in the figure. This variation causes problems for audio playback at the receiving end. Playback may experience gaps while waiting for the arrival of variable delayed packets.

 Copyright © 2005, Cisco Systems, Inc.



When a router receives an audio stream for VoIP, it must compensate for any jitter that it detects. The playout delay buffer mechanism handles this function. Playout delay is the amount of time that elapses between the time a voice packet is received at the jitter buffer on the DSP and the time a voice packet is played out to the codec. The playout delay buffer must buffer these packets and then play them out in a steady stream to the DSPs. The DSPs then convert the packets back into an analog audio stream. The playout delay buffer is also referred to as the dejitter buffer.

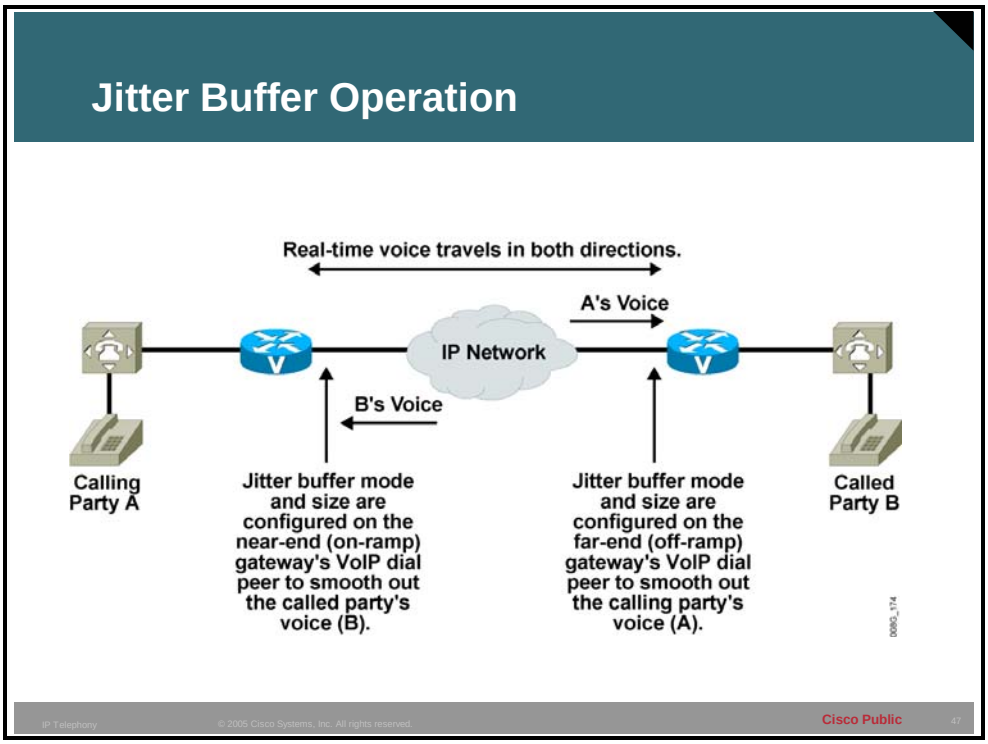


If the magnitude of jitter is so great that packets are received out of range of the playout delay buffer, the out-of-range packets are discarded and dropouts appear in the audio. For losses as small as one packet, the DSP interpolates what it calculates the audio should be, making the problem inaudible through the Cisco IOS Packet Loss Concealment (PLC) service.

 Copyright © 2005, Cisco Systems, Inc.

Overcoming Jitter

Cisco voice networks compensate for jitter by setting up a buffer, called the “jitter buffer,” on the gateway router at the receiving end of the voice transmission. This topic explains how to overcome jitter.



The jitter buffer receives voice packets from the IP network at irregular intervals. Occasionally, the voice packets are out of sequence. The jitter buffer holds the packets briefly, reorders them if necessary, and then plays them out at evenly spaced intervals to the decoder in the DSP on the gateway. Algorithms in the DSP determine the size and behavior of the jitter buffer based on user configuration and current network jitter conditions. The DSP uses this information to maximize the number of correctly delivered packets and minimize the amount of delay.

The size of the jitter buffer and the amount of delay is configurable by the user with the **playout-delay** command. Proper configuration is critical. If voice packets are held for too short a time, variations in delay may cause the buffer to underrun (become empty) and cause gaps in speech. However, packets that arrive at a full buffer are dropped, also causing gaps in speech.

To improve voice quality, the speech gaps are hidden by several different techniques that synthesize packets to replace those that were lost or not received in time. Depending on the contiguous duration of the gaps, the missing voice frames are replaced by prediction from the past frames (usually the last frame), followed by silence if the condition persists (for more than 30 to 50 ms, for example). The **show call active voice** command output gives buffer overflow and concealment statistics, which are a good indication of the network effect on audio quality.

Example: Overcoming Jitter

In an example that demonstrates how packets can be lost, a jitter buffer is configured with a maximum playout delay of 40 ms. On the network, packets are delayed from their source; perhaps a media server stops sending packets for 60 ms, or there is severe network congestion.

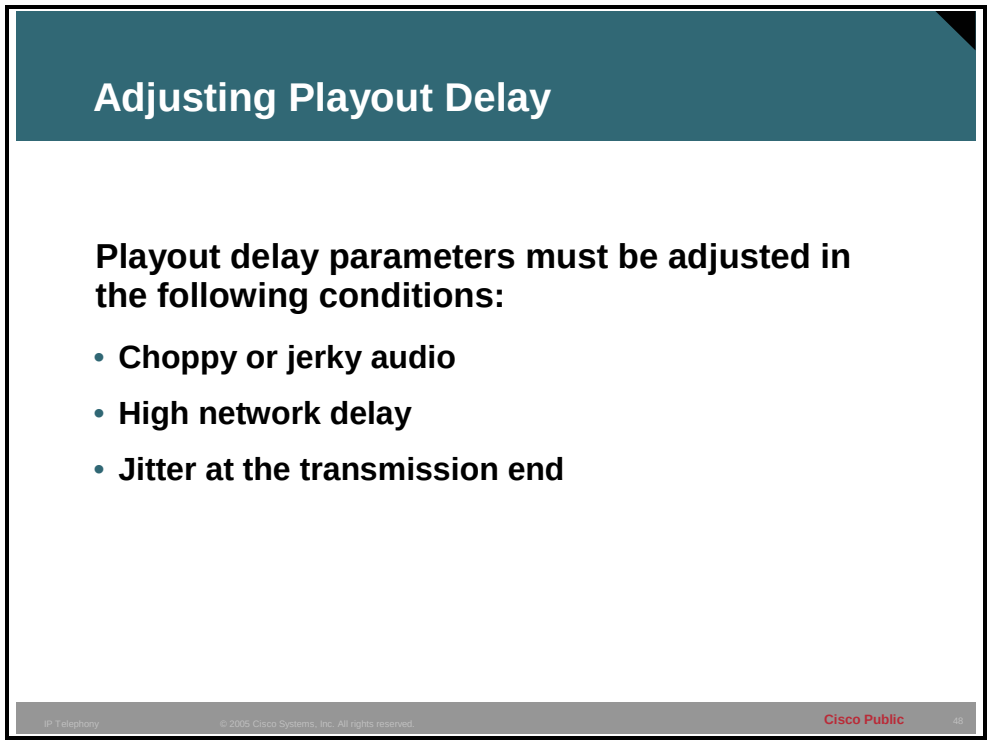
The jitter buffer empties while waiting for input from the network. Input does not arrive until *after* the maximum playout delay time is reached and there is a noticeable break in voice transmission. Now, the media server sends packets *to* the jitter buffer at a faster rate than the packets *leave* the jitter buffer; this makes the jitter buffer fill up. The jitter buffer discards subsequent packets, resulting in a choppy voice signal.

Even though the size of the jitter buffer is configurable, it is important to note that if the buffer size is too large, the overall delay on the connection may rise to unacceptable levels. You must weigh the benefit of improving jitter conditions against the disadvantage of increasing total end-to-end delay, which can also cause voice quality problems.

 Copyright © 2005, Cisco Systems, Inc.

Adjusting Playout Delay Parameters

This topic lists the symptoms that lead to adjusting playout delay parameters.



The conditions that require you to adjust playout delay parameters are as follows:

- **Choppy or jerky audio:** Gaps in speech patterns that produce choppy or jerky audio suggest that you should increase the minimum playout delay, increase the maximum playout delay, or both, if you are using adaptive mode. For fixed mode, you must increase the nominal value.
- **High network delay:** High overall network delay suggests that you should reduce the maximum playout delay in adaptive mode, or reduce the nominal delay in fixed mode. You must watch for loss of voice quality. The maximum delay value sets an upper limit on adaptive playout delay, which in many cases is the major contributor to end-to-end delay. In many applications, it may be preferable to have the system or the user terminate the call, rather than allow an arbitrarily large delay. The data received with jitter outside this limit will show up in the late packet count in the **show call active voice** playout statistics.
- **Jitter at the transmission end:** A noisy but well-understood network or interworking with an application that has lots of jitter at the transmission end, from a source such as a unified messaging server or interactive voice response (IVR) application, suggests selection of fixed mode.

Symptoms of Jitter on a Network

This topic provides examples of output for the **show call active voice** command, which can be used to determine the size of jitter problems.

Symptoms of Jitter

```
Router# show call active voice

<output omitted>

VOIP:
 ConnectionId[0xECDE2E7B 0xF46A003F 0x0 0x47070A4]
 IncomingConnectionId[0xECDE2E7B 0xF46A003F 0x0 0x47070A4]
 RemoteIPAddress=192.168.100.101
 RemoteUDPPort=18834
 RoundTripDelay=11 ms
 SelectedQoS=best-effort
 tx_DtmfRelay=inband-voice
 FastConnect=TRUE

 Separate H245 Connection=FALSE

 H245 Tunneling=FALSE
```

IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 49

Symptoms of Jitter (Cont.)

```
SessionProtocol=cisco
 SessionTarget=
 OnTimeRvPlayout=417000
 GapFillWithSilence=850 ms

 GapFillWithPrediction=2590 ms

 GapFillWithInterpolation=0 ms
 GapFillWithRedundancy=0 ms
 HiWaterPlayoutDelay=70 ms
 LoWaterPlayoutDelay=29 ms
 ReceiveDelay=39 ms

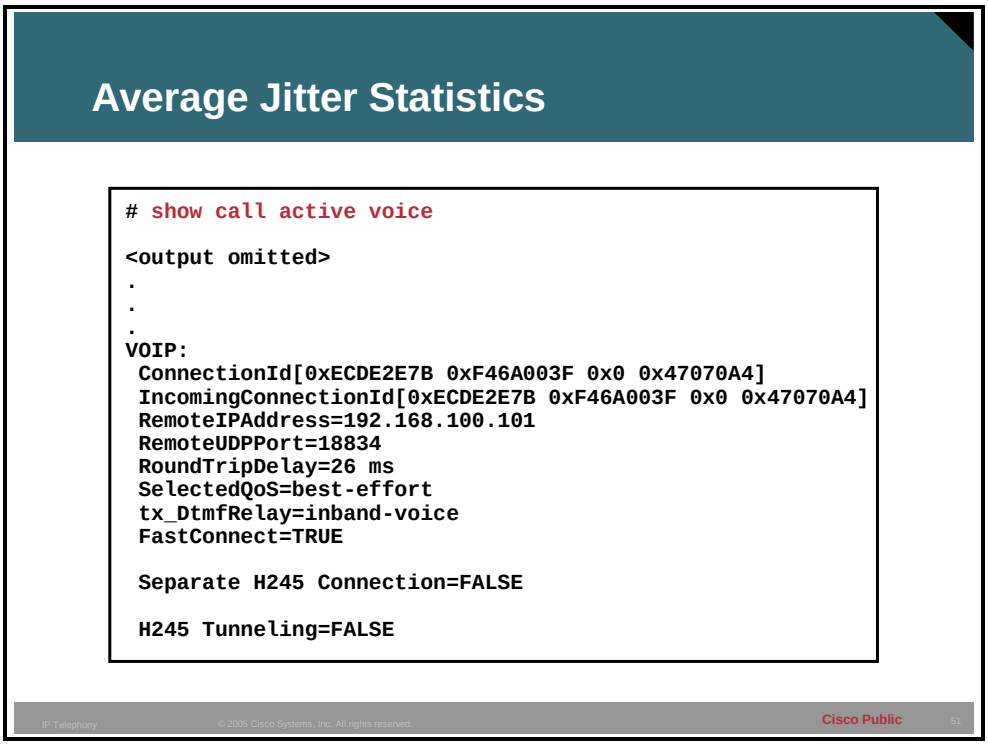
 LostPackets=0
 EarlyPackets=0
 LatePackets=86
```

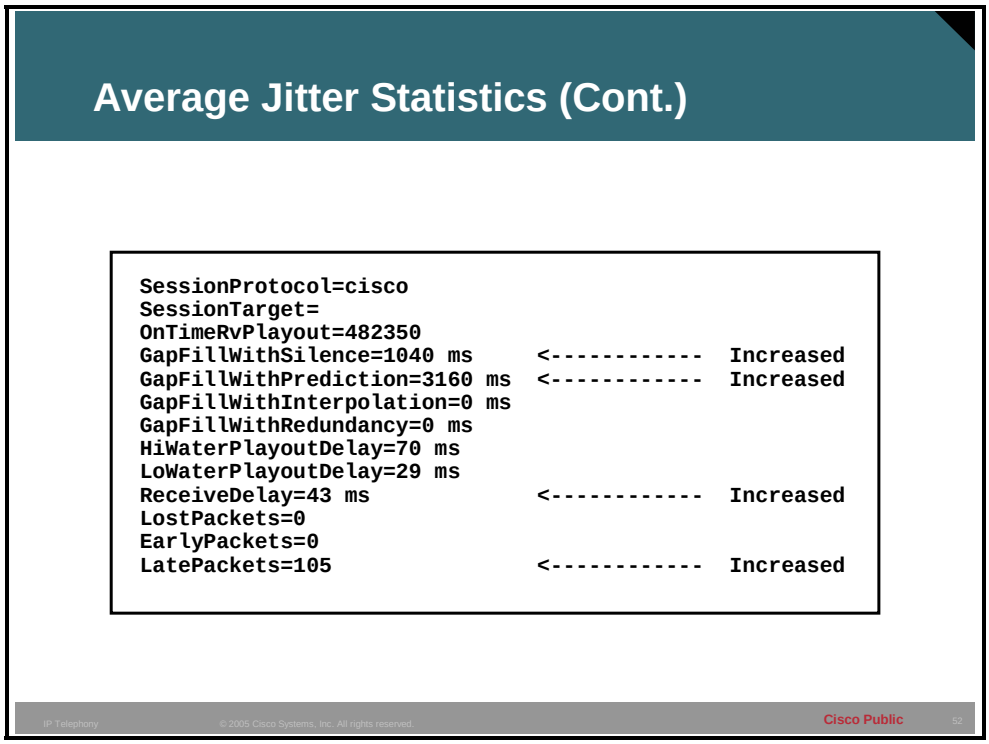
IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 50

 Copyright © 2005, Cisco Systems, Inc.

The figure shows sample output for the **show call active voice** command. Several fields in the **show call active voice** command output that can help you to determine the actual size of the jitter problems are as follows:

- **ReceiveDelay:** The playout delay for jitter compensation plus the average expected delay after the frame is available for playout to the decoder. The current low-water mark and high-water mark statistics for the receive delay are available in the output.
- **GapFillWith:** These fields refer to the amount of *concealment*—or packet synthesizing—that took place in this call, to replace the voice packets that were lost or not received in time.
- **LostPackets:** The actual number of packets that were lost; that is, the packets *not* received at the egress gateway. This is detected using the **sequence number** field in the RTP packets.
- **EarlyPackets:** The actual number of packets that arrived *earlier* than the current minimum delay packet. They cause the dejitter algorithm to readjust the minimum delay packet used in jitter estimation.
- **LatePackets:** The actual number of packets that arrived later than the current playout delay setting. The information in these packets is discarded.



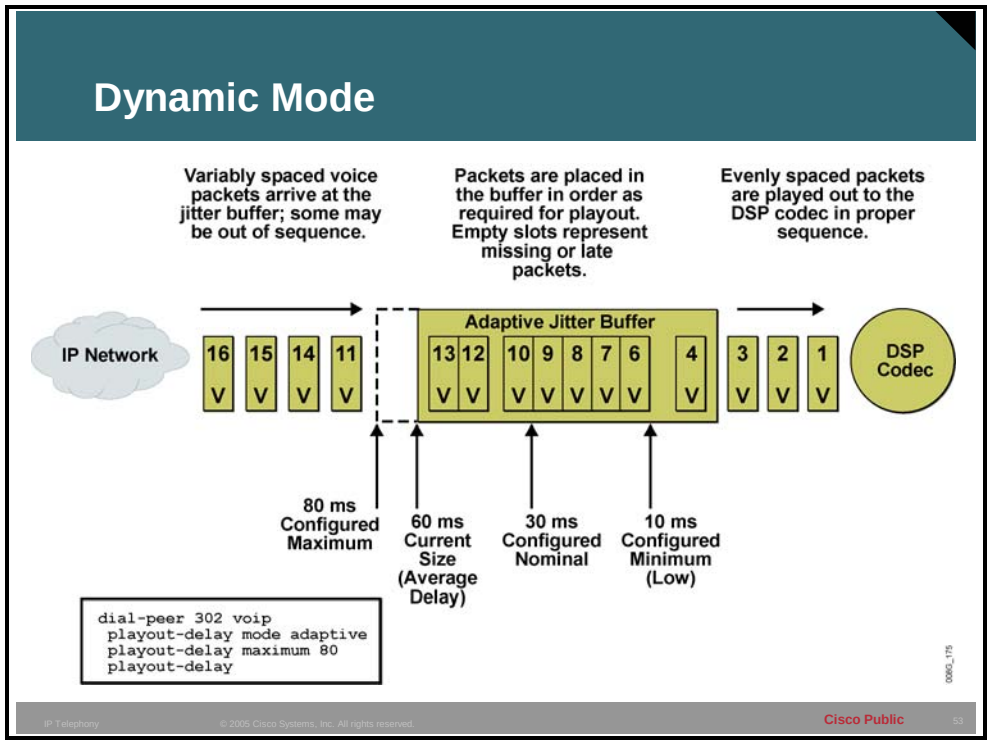


The sample output in this figure displays average jitter statistics when poor voice quality was perceived on the network. The GapFillWithSilence line indicates that too many consecutive packets were lost or late, and the DSP could not predict and fill in the gaps. The GapFillWithPrediction line indicates that packets were late or lost, and the DSP filled in the lost audio with prediction. The ReceiveDelay line indicates the average one-way delay the packets are experiencing as per the time stamps in the RTP header. The LatePackets line indicates the number of packets that were too late to be processed by the DSP. As these fields increase, the playout delay buffer should be increased in size.

 Copyright © 2005, Cisco Systems, Inc.

Dynamic Jitter Buffer

This topic describes the dynamic jitter buffer mode.



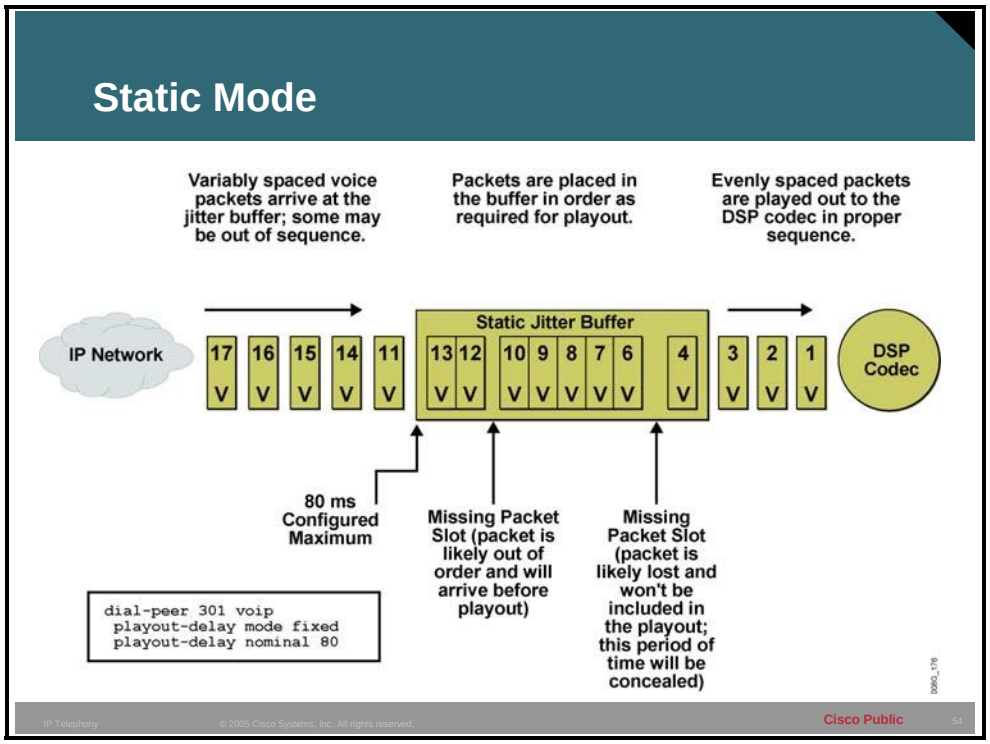
The **playout-delay** command allows you to select a jitter buffer mode (**static** or **dynamic**) and specify certain values that are used by the DSP algorithms to adjust the size of the jitter buffer. During a voice call, the algorithms read time stamps in the RTP headers of sample packets to determine the amount of delay that the jitter buffer will apply to an average packet; that is, as if there is no jitter at all in the network. This is called the average delay.

Example: Dynamic Jitter Buffer

When you configure the **playout-delay mode adaptive** option, the DSP algorithms in the codec take samples throughout the voice call and adjust the value of the average delay as network jitter conditions change. The size of the jitter buffer and the amount of delay applied are adjusted upward or downward, as needed. This adjustment ensures the smooth transmission of voice frames to the codec within the minimum and maximum limits that you configure. The algorithms are designed to *slowly* reduce the amount of delay and *quickly* increase the amount of delay during adjustment. As a result, voice quality is achieved at the risk of longer delay times.

Static Jitter Buffer

This topic describes the static mode buffer.



When you configure the **playout-delay mode fixed** option, you can specify the nominal delay value, which is the amount of playout delay applied at the beginning of a call by the jitter buffer. This is also the maximum size of the jitter buffer throughout the call.

Example: Static Jitter Buffer

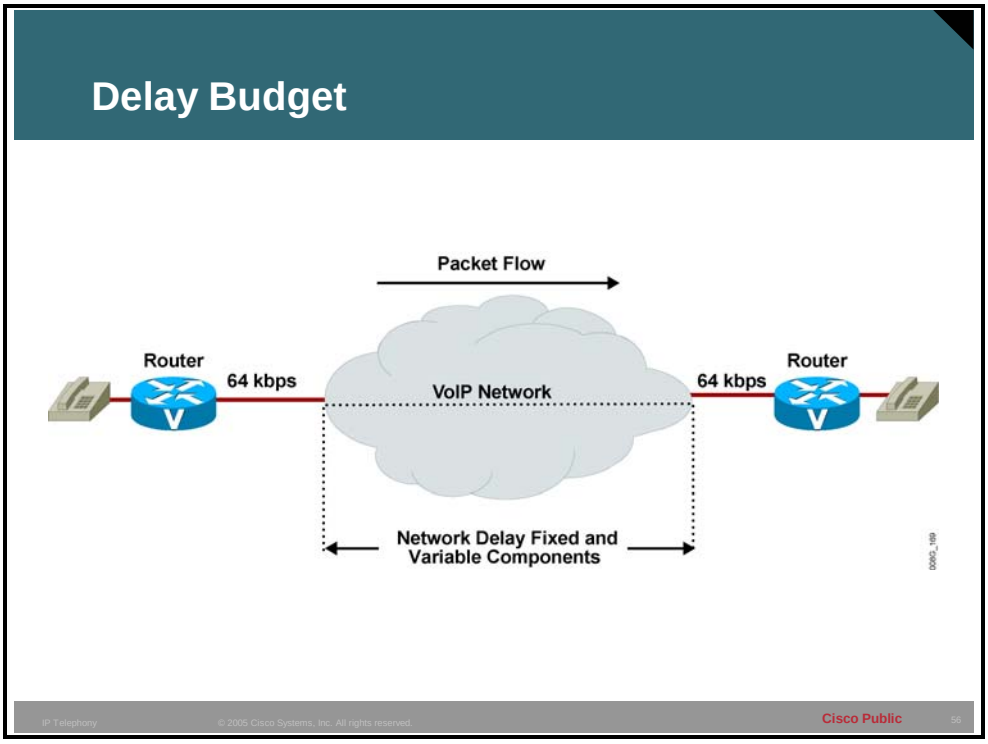
Configuring static or “fixed” playout delay limits the size of the buffer. The figure shows an example of adjusting the nominal size of the buffer to 80 ms. Care should be taken when using the jitter buffer in static mode. Variations in arrival times of voice packets may be put at risk when network conditions change. In addition, if the static jitter buffer is configured to be too large, overall one-way delay is increased, exacerbating delay and echo problems.

 Copyright © 2005, Cisco Systems, Inc.

Delay

Need for a Delay Budget

The end-to-end delay in a VoIP network is known as the delay budget. Network administrators must design a network to operate within an acceptable delay budget. This topic explains the concept of delay budget and how to measure it.



Delay is the accumulated latency of end-to-end voice traffic in a VoIP network. The purpose of a delay budget is to ensure that the voice network does not exceed accepted limits of delay for voice telephony conversation. The delay budget is the sum of all the delays, fixed and variable, that are found in the network along the audio path. You can measure the delay budget by adding up all of the individual contributing components, as shown in the figure. The delay budget is measured in each direction individually, not round-trip.

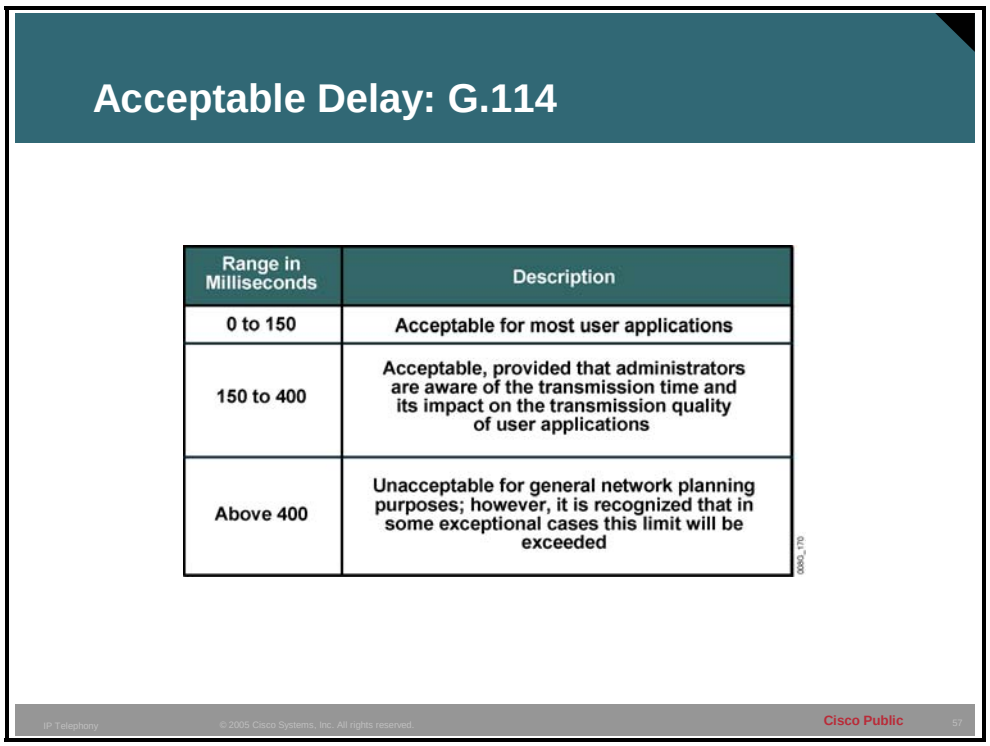
Network administrators must be aware that delay exists, and then design their network to bring end-to-end delay within acceptable limits.

Example: Need For a Delay Budget

As delay increases, talkers and listeners become unsynchronized and often find themselves speaking at the same time or both waiting for the other to speak. This condition is commonly called *talker overlap*. While the overall voice quality may be acceptable, users may find the stilted nature of the conversation unacceptably annoying. Talker overlap may be observed on international telephone calls that travel over satellite connections. Satellite delay is about 500 ms: 250 ms up and 250 ms down.

Guidelines for Acceptable Delay

International telephony communications must adhere to a delay standard. This topic defines the standard and its limits.



The ITU addresses network delay for voice applications in Recommendation G.114. This recommendation is oriented to national telecommunications administrations and is more stringent than what is normally applied in private voice networks. When the location and business needs of end users are well known to the network designer, more delay may prove acceptable.

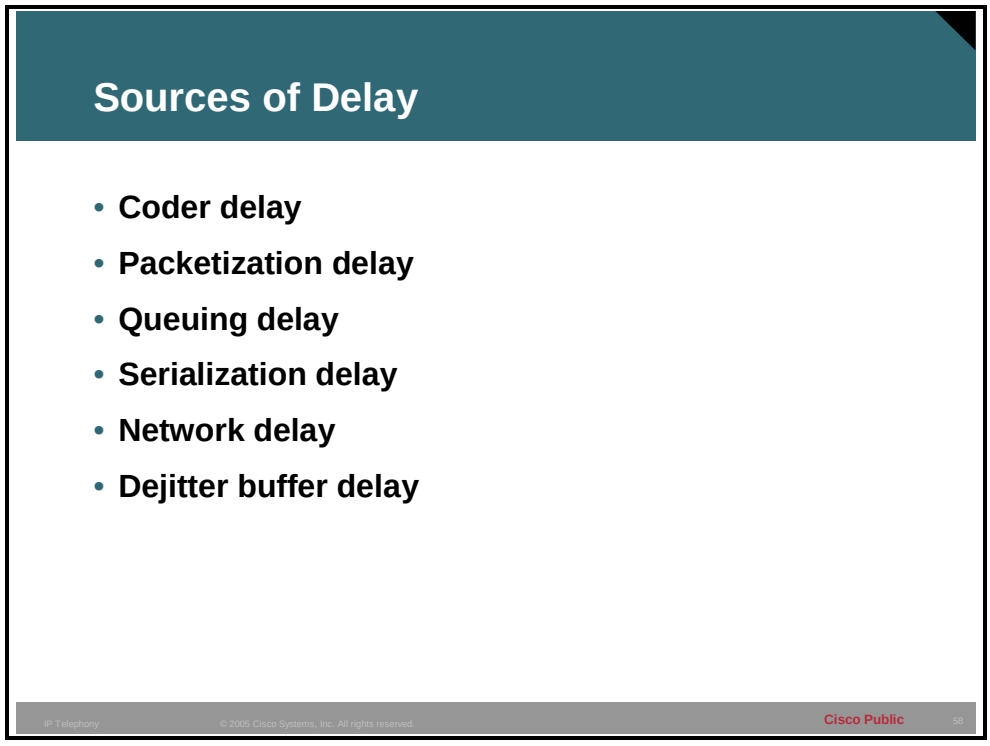
Example: Acceptable Delay

As shown in the figure, acceptable delay time is from 0 to 400 ms for private networks. Delay times that exceed 400 ms are unacceptable for general network planning. However, all networks should be engineered to recognize and minimize the voice-connection delay. For example, suppose an enterprise is doing the planning for a new IP telephony roll-out. They plan and design to meet the 150-ms one-way delay, but have some locations in which 250-ms one-way delay is the best they can do. Since most of these calls will be on-net calls, the organization has to decide if the lower quality of the calls is acceptable for these locations.

 Copyright © 2005, Cisco Systems, Inc.

Sources of Delay

Many factors add to overall delay. This topic lists six factors that are sources of delay.



Following is an explanation of six major factors that contribute to overall fixed and variable delay:

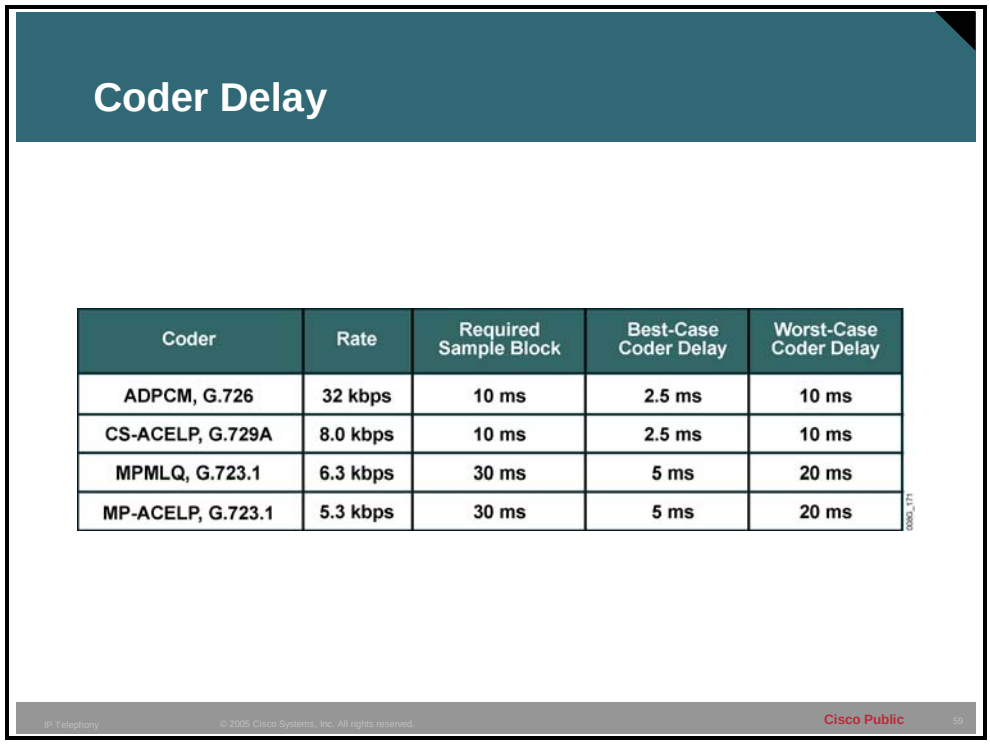
- **Coder delay:** Also called processing delay, coder delay is the time taken by the DSP to compress a block of pulse code modulation (PCM) samples. Because different coders work in different ways, this delay varies with the voice coder that is used and the processor speed.
- **Packetization delay:** Packetization delay is the time it takes to fill a packet payload with encoded or compressed speech. This delay is a function of the sample block size that is required by the vocoder and the number of blocks placed in a single frame. Packetization delay is also called accumulation delay because the voice samples accumulate in a buffer before being released. With typical payload sizes used on Cisco routers, packetization delay for G.711, G.726, and G.729 does not exceed 30 ms.
- **Queuing delay:** After the network builds a compressed voice payload, it adds a header and queues for transmission on the network connection. Because voice should have absolute priority in the router or gateway, a voice frame must wait only for a data frame already playing out or for other voice frames ahead of it. Essentially, the voice frame waits for the serialization delay of any preceding frames that are in the output queue. Queuing delay is a variable delay and is dependent on the trunk speed and the state of the queue.
- **Serialization delay:** Serialization delay is the fixed delay that is required to clock a voice or data frame onto the network interface; it is directly related to the clock rate on the trunk.

- **Network delay:** The public Frame Relay or ATM network that interconnects the endpoint locations is the source of the longest voice-connection delays. These delays are also the most difficult to quantify. If a private enterprise builds its own internal Frame Relay network for the purpose of wide-area connectivity, it is possible to identify the individual components of delay. In general, the fixed components are from propagation delays on the trunks within the network; variable delays are the result of queuing delays that clock frames into and out of intermediate switches. To estimate propagation delay, a popular estimate of 10 microseconds/mile or 6 microseconds/km (G.114) is widely used, although intermediate multiplexing equipment, backhauling, microwave links, and other features of carrier networks create many exceptions. Typical carrier delays for U.S. Frame Relay connections are 40 ms fixed, and 25 ms variable, for a total worst-case delay of 65 ms.
- **Dejitter buffer delay:** Because speech is a constant bit-rate service, the jitter from all the variable delays must be removed before the signal leaves the network. In Cisco routers and gateways, this is accomplished with a dejitter buffer at the far-end (receiving) router or gateway. The dejitter buffer transforms the variable delay into a fixed delay by holding the first sample that is received for a period of time *before* playing it out. This holding period is known as the initial playout delay. The actual contribution of the dejitter buffer to delay is the initial playout delay of the dejitter buffer *plus* the actual amount of delay of the first packet that was buffered in the network. The worst case would be twice the dejitter buffer initial delay (assuming the first packet through the network experienced only minimal buffering delay).

 Copyright © 2005, Cisco Systems, Inc.

Effects of Coders and Voice Sampling on Delay

The process of encoding an analog voice sample into a compressed digitized bit stream contributes to delay. This topic describes the effect of coder delay. Best-case and worst-case coder delays are shown in the figure.



Coder	Rate	Required Sample Block	Best-Case Coder Delay	Worst-Case Coder Delay
ADPCM, G.726	32 kbps	10 ms	2.5 ms	10 ms
CS-ACELP, G.729A	8.0 kbps	10 ms	2.5 ms	10 ms
MPMLQ, G.723.1	6.3 kbps	30 ms	5 ms	20 ms
MP-ACELP, G.723.1	5.3 kbps	30 ms	5 ms	20 ms

0060_171

The compression time for a Conjugate Structure Algebraic Code Excited Linear Prediction (CS-ACELP) process ranges from 2.5 to 10 ms, depending on the loading of the DSP. If the DSP is fully loaded with four voice channels, the coder delay will be 10 ms. If the DSP is loaded with one voice channel only, the coder delay will be 2.5 ms. For design purposes, use the worst-case time of 10 ms.

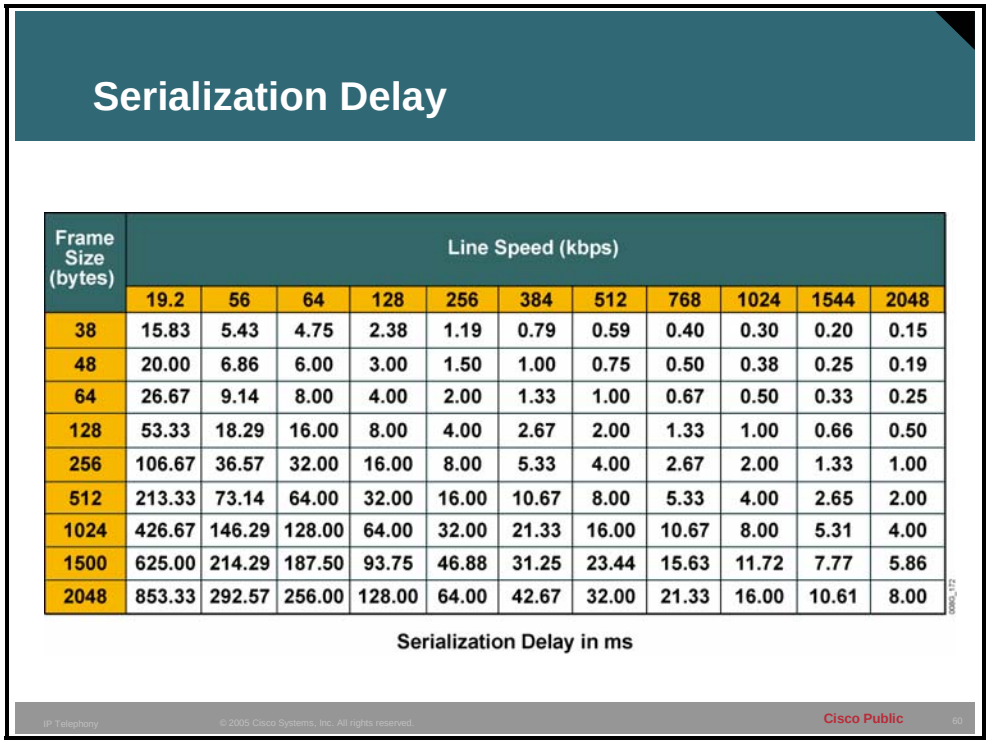
Decompression time is roughly 10 percent of the compression time for each block. However, because there may be multiple samples in each frame, the decompression time is proportional to the number of samples per frame. Consequently, the worst-case decompression time for a frame with three samples is 3 x 1 ms, or 3 ms. Generally, two or three blocks of compressed G.729 output are put in one frame, while only one sample of compressed G.723.1 output is sent in each frame.

Example: Coder Delay

The figure shows examples of some coder delays. CS-ACELP, for example, lists a best-case delay of 2.5 ms with a worst-case delay of 10 ms. In all calculations, the worst-case number should be used.

Managing Serialization Delay

An important part of delay is the serialization delay on the interface. This topic describes serialization delay and its management.



The figure shows the serialization delay required for different frame sizes at various line speeds. This table uses total frame size, not payload size, for computation. As an example, reading from the graphic, on a 64-kbps line, a CS-ACELP voice frame with a length of 38 bytes (37 bytes + 1-byte flag) has a serialization delay of 4.75 ms. If the line speed is increased to 1.544 Mbps, the serialization delay goes down to 0.2 ms. Cisco recommends a 10-ms serialization delay, not to exceed 20 ms.

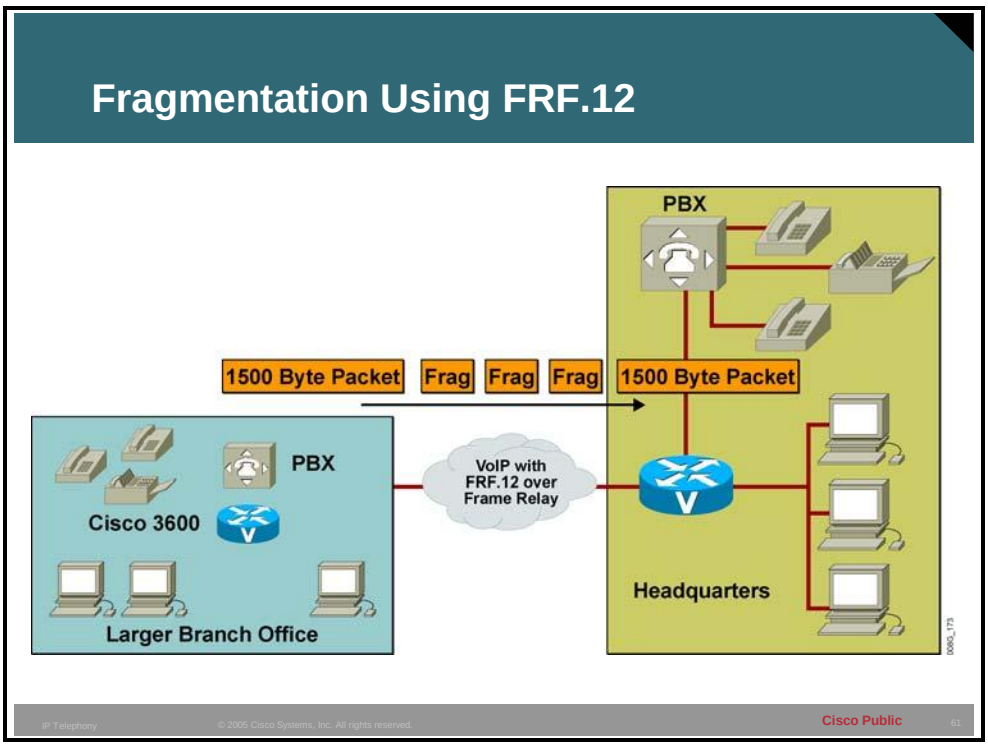
You can effectively change the serialization delay of a voice packet by performing the following:

- **Increasing the link speed:** Solves the problem, but is expensive
- **Decreasing the packet size:** May not be possible for all codec types, and also increases bandwidth overhead

 Copyright © 2005, Cisco Systems, Inc.

Managing Queuing Delay

Queuing delay contributes to overall delay. This topic explains queuing delay and offers a standard solution.



Queuing delay occurs when other elements in the outbound queue (voice or data packets) cause voice packets to be delayed. For example, the serialization delay for a 1500-byte packet is 214 ms to leave the router over a 56-kbps link. If a 1500-byte data packet that is not real-time is being sent, real-time (voice) packets are queued until the large data packet is transmitted. This delay is unacceptable for voice traffic. If data packets that are not real-time packets are fragmented into smaller frames, they are interleaved with real-time (voice) frames. In this way, both voice and data frames can be carried together on low-speed links without causing excessive delay to the real-time voice traffic. One way to implement this fragmentation is to use FRF.12 on VoIP over Frame Relay networks. FRF.12 serves to fragment Frame Relay frames into smaller frames, even from different permanent virtual circuits (PVCs).

Example: Fragment Size Configuration

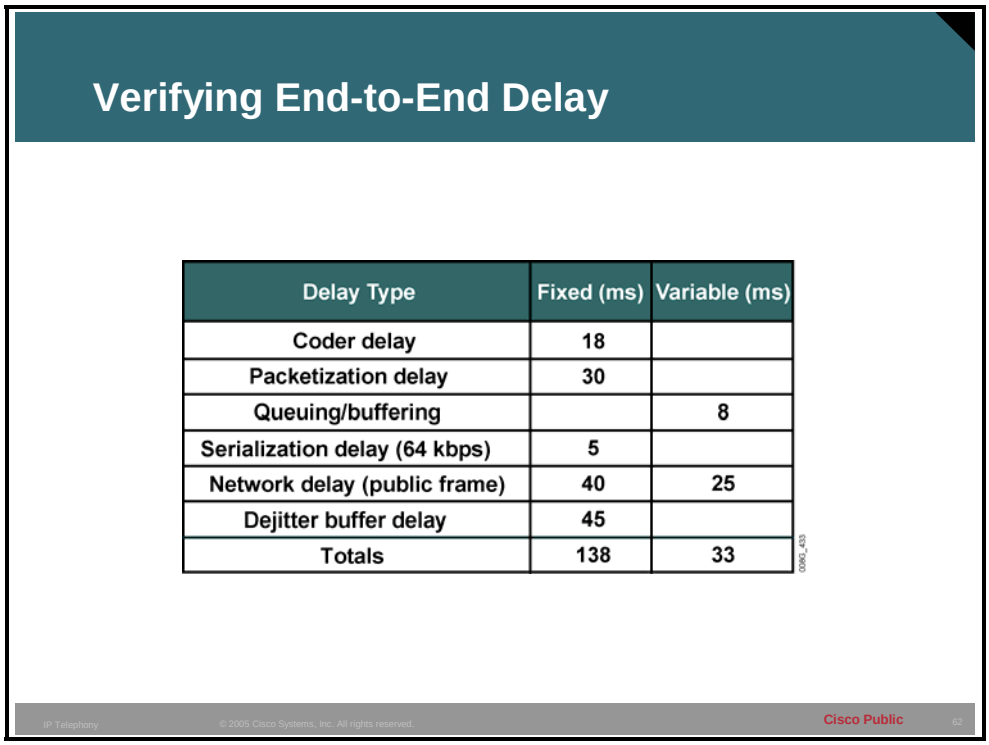
You can configure fragment size using the **frame-relay fragment** *fragment_size* command in a Frame Relay map class. The *fragment_size* argument defines the payload size of a fragment and excludes the Frame Relay headers and any Frame Relay fragmentation header. The valid range is from 16 bytes to 1600 bytes; the default is 53 bytes.

The *fragment_size* argument should be set so that the serialization delay is close to 10 ms; for example, if using a 384-kbps link, the fragmentation size should be set at 512 kbps.

Set the fragmentation size so that the largest data packet is not larger than the voice packets.

Verifying End-to-End Delay

End-to-end delay is calculated and compared to the G.114 recommendation. This topic illustrates the process.



A typical one-hop connection over a public Frame Relay connection may have the delay budget that is shown in the figure. To calculate one-way delay, simply add all of the contributing components together. The goal is to allow a one-way delay as recommended by G.114.

Example: Verifying End-To-End Delay

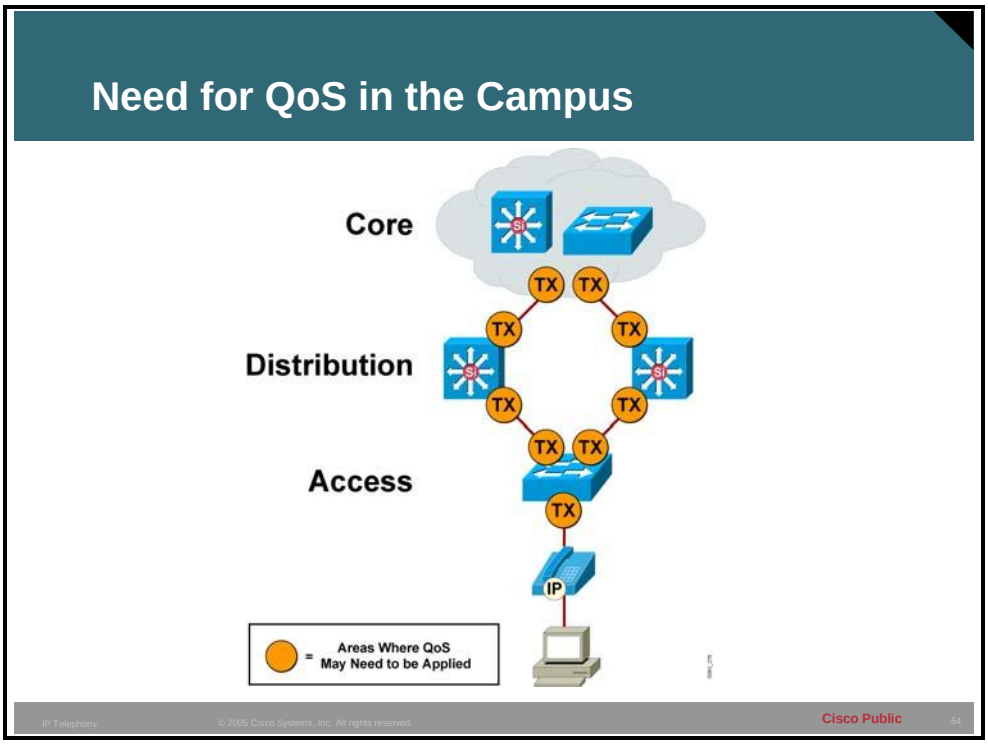
The figure shows an acceptable one-way delay of 138 ms, plus 33 ms, for a total of 171 ms.

 Copyright © 2005, Cisco Systems, Inc.

Applying QoS in the Campus

Need for QoS in the Campus

This topic describes the need for QoS measures in a campus network.



The bursty nature of data networks, combined with the high volume of smaller TCP packets, causes transmit buffers to fill to capacity in high-speed campus networks. If an output buffer fills, ingress interfaces are unable to place new flow traffic into the output buffer. When the ingress buffer is filled, which can happen quickly, packet drops occur. Typically, these drops are more than a single packet in any given flow. TCP packet loss causes retransmissions to occur, further aggravating the problem. Voice packet loss results in voice clipping and skips.

The figure illustrates the areas of a campus network where QoS is a concern. These areas are as follows:

- **Access ports:** Access-level ports that connect to IP Phones or gateways and the distribution switches
- **Distribution ports:** Uplink ports that connect to access switches and core switches
- **Core ports:** Uplink ports that connect the distribution switches to the core campus switches

VoIP traffic is sensitive to both delayed packets and dropped packets. Even though a campus may be using gigabit Ethernet trunks, which have extremely fast serialization times, delay and dropped packets may still be an issue because of the type of packets, type of applications, and number of packets. However, drops *always* adversely affect voice quality in the campus. Using

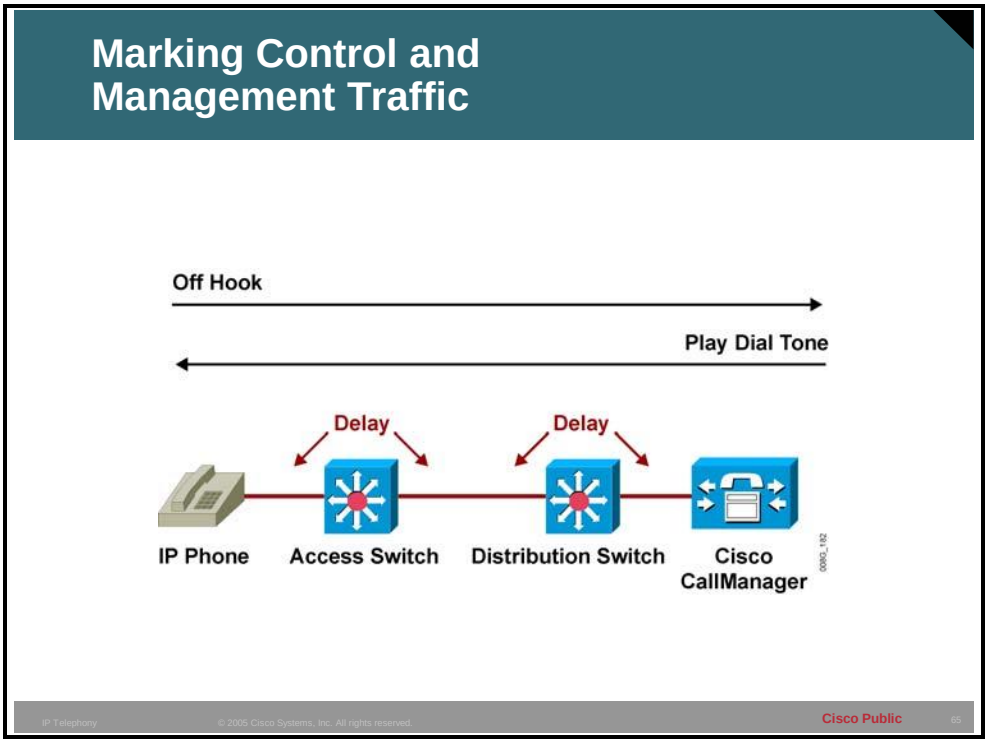
multiple queues on transmit interfaces is the only way to eliminate the potential for dropped traffic caused by buffers operating at 100 percent capacity. By separating voice (which is sensitive to delays and drops) into its own queue, you can prevent flows from being dropped at the ingress interface even if data flows fill up the data transmit buffer. If video is present, it should also have its own queue because it has similar delay characteristics.

Caution It is critical that you verify that flow control is disabled when enabling QoS (multiple queues) on Catalyst switches. Flow control interferes with the configured queuing behavior by acting on the ports before activation of queuing. Flow control is disabled by default.

 Copyright © 2005, Cisco Systems, Inc.

Marking Control and Management Traffic

Marking control and management traffic is critical to VoIP network performance. Control and management traffic should be marked for preferential dispatching throughout the campus. This topic describes marking control and management traffic as an approach to the management of QoS in a campus network.



In networks with high traffic loads, managing the delivery of control traffic is critical to ensuring a positive user experience with VoIP. Delay to Dial-Tone (DTT) time is an example of this type of delivery management. When a Cisco IP Phone goes off hook, it “asks” Cisco CallManager for instructions. Cisco CallManager then instructs the Cisco IP Phone to play a dial tone. If this management and control traffic is dropped or delayed within the network, the user experience is adversely affected. The same logic applies to all signaling traffic for gateways and telephones.

.

Configuring a Voice VLAN

```
Router# configure terminal
Router(config)# interface fastethernet 5/1
Router(config-if)# switchport voice vlan 101
Router(config-if)# exit
```

IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 66

The figure shows how to configure Fast Ethernet port 5/1 to send Cisco Discovery Protocol (CDP) packets that tell the Cisco IP Phone to use VLAN 101 as the voice VLAN.

Verifying the Configuration

```
Router# show interfaces fastethernet 5/1 switchport
Name: Fa5/1
Switchport: Enabled
Administrative Mode: access
Operational Mode: access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: off
Access Mode VLAN: 100
Voice VLAN: 101
Trunking Native Mode VLAN: 1 (default)
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 900 ((Inactive)) 901
((Inactive))
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

IP Telephony © 2005 Cisco Systems, Inc. All rights reserved. Cisco Public 67

This example shows how to verify the configuration of Fast Ethernet port 5/1.

 Copyright © 2005, Cisco Systems, Inc.

Switchwide Queuing

Configuration for switchwide queuing depends upon the type of interface used. The two types of interfaces used are:

- **Receive interface:** The recommended configuration for the receive interface is one standard FIFO queue.
- **Transmit interface:** The recommended configuration for the transmit interface is two standard queues with a single threshold (2Q1T). This method is preferred over other methods because it places traffic with specific CoS in one queue (as configured) and all other traffic in the second queue, thus simplifying configuration. The threshold indicates that traffic is dropped when the buffer capacity reaches 100 percent. Scheduling is done on a WRR basis. Admission to the queues is based on the 802.1p CoS value and is user-configurable in pairs. If you enable QoS, but do not modify the CoS-to-transmit queue mappings, switch performance could be affected because all traffic goes to queue 1.

Note 802.1p is a Layer 2 mechanism for classifying traffic using 3 bits. 802.1p adds 16 bits to the Layer 2 header.

IP Phone Port Queuing

In Cisco Catalyst software Release 5.5.1, the Catalyst 4000 line does not offer any advanced IP Phone-queuing features. Because of this, the Catalyst 4000 depends on the default CoS marking and enforcement of the Cisco IP Phone. Other access switches, such as the Catalyst 3500, offer more advanced IP port phone-queuing options.

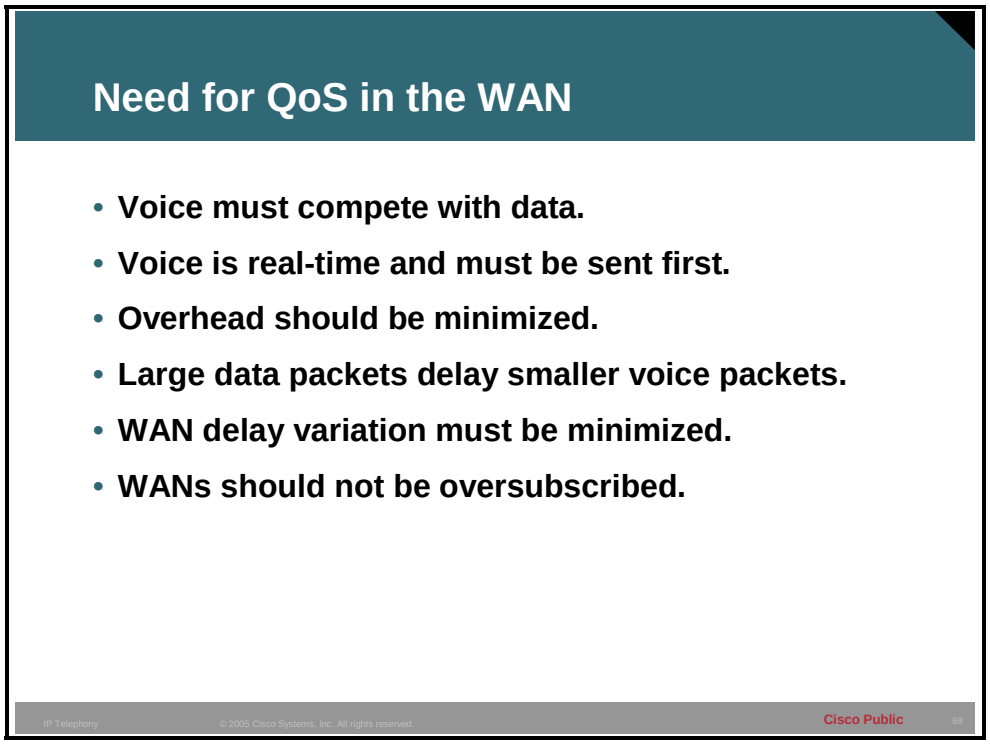
Uplink Interface to the Distribution Switch

You do not need to configure special queuing or scheduling commands on the Catalyst 4000 side of the link (from the access layer Catalyst 4000 to the distribution layer Catalyst 6000). Queuing is automatically enabled after QoS has been enabled and the classification and queue admission have been configured.

QoS Tools in the WAN

Need for QoS on WAN Links

This topic defines the need for QoS in a WAN.



You must consider and implement certain QoS measures before voice can be placed on a WAN to ensure the proper performance of voice and data applications. The following factors explain the need for QoS:

- **Voice must compete with data:** Voice traffic demand on the WAN is typically smooth; each voice call consumes a relatively fixed amount of bandwidth for the duration of the call. On the other hand, data traffic is bursty, peaking and leveling off based on user access and application type. The amount of total bandwidth that you provision must have the capacity to carry all of the expected traffic.
- **Voice is real-time and must be sent first:** Because voice is a real-time application and delayed packets have a severe impact on performance, you must prioritize voice ahead of data traffic that is not real-time traffic.
- **Overhead should be minimized:** Voice is sent using UDP. Unfortunately, this requirement adds significant overhead to the overall packet size. You must identify a means for numbering the packets that are needed, because minimizing the overhead with compression allows for smaller, more efficient packets.
- **Large data packets delay smaller voice packets:** With certain applications such as file transfers and web browsing, data packets that compete with voice can be relatively large. Voice packets are forced to wait until the larger data packets are sent. By fragmenting the

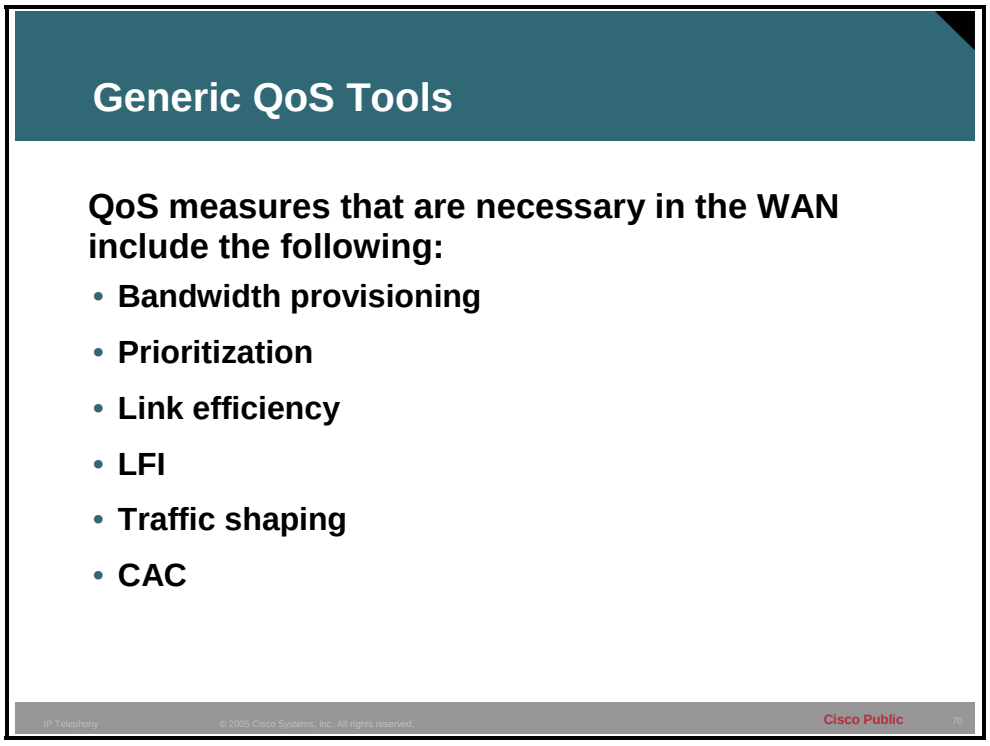
 Copyright © 2005, Cisco Systems, Inc.

data packets into smaller, more manageable sizes, you can reduce the delay that is experienced by voice packets.

- **WAN delay variation must be minimized:** The natural behavior of certain WAN technologies, such as Frame Relay, ATM, and PPP can exacerbate delay variation and result in poor voice performance. By using tools to reduce the delay variation on WAN technologies, you can add significant performance to voice applications.
- **WANs should not be oversubscribed:** If you place too many voice calls on a WAN, the necessary bandwidth that is required by data applications will be choked. You must take care to ensure that data still gets its deserved bandwidth. Excess voice calls can severely impact all calls on the network.

Recommendations for Generic QoS in the WAN

This topic lists generic QoS tools.



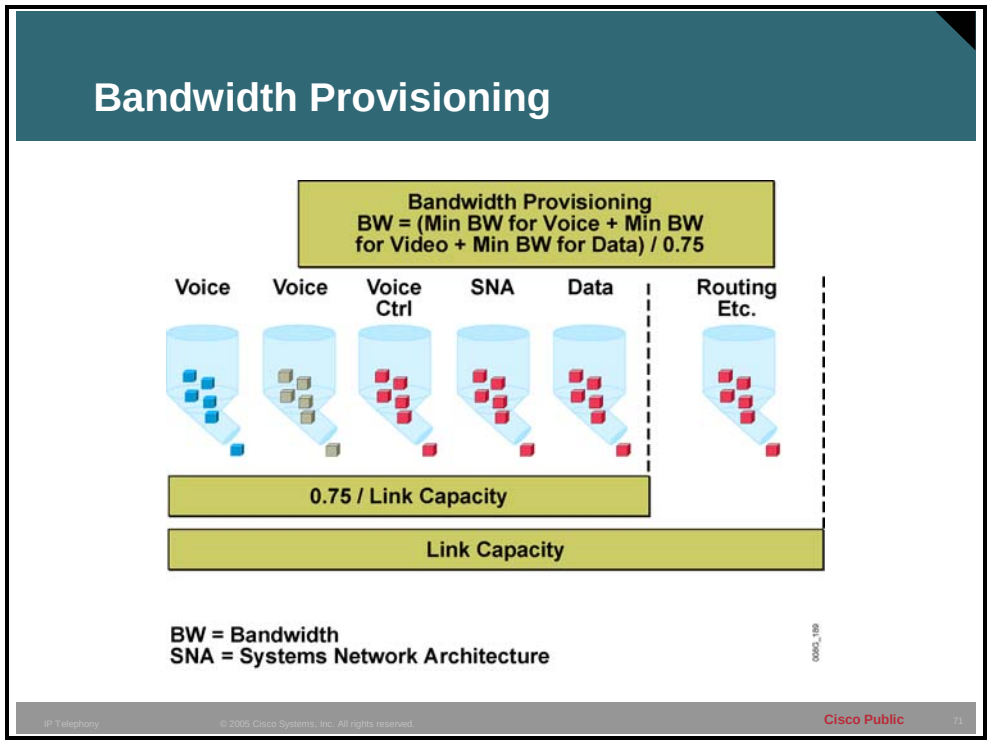
Depending on the Layer 2 technology that you use, the following QoS measures may be necessary in the WAN. Each of these QoS tools will be covered in this lesson:

- Bandwidth provisioning
- Prioritization
- Link efficiency
- LFI
- Traffic shaping
- CAC

 Copyright © 2005, Cisco Systems, Inc.

Bandwidth Provisioning

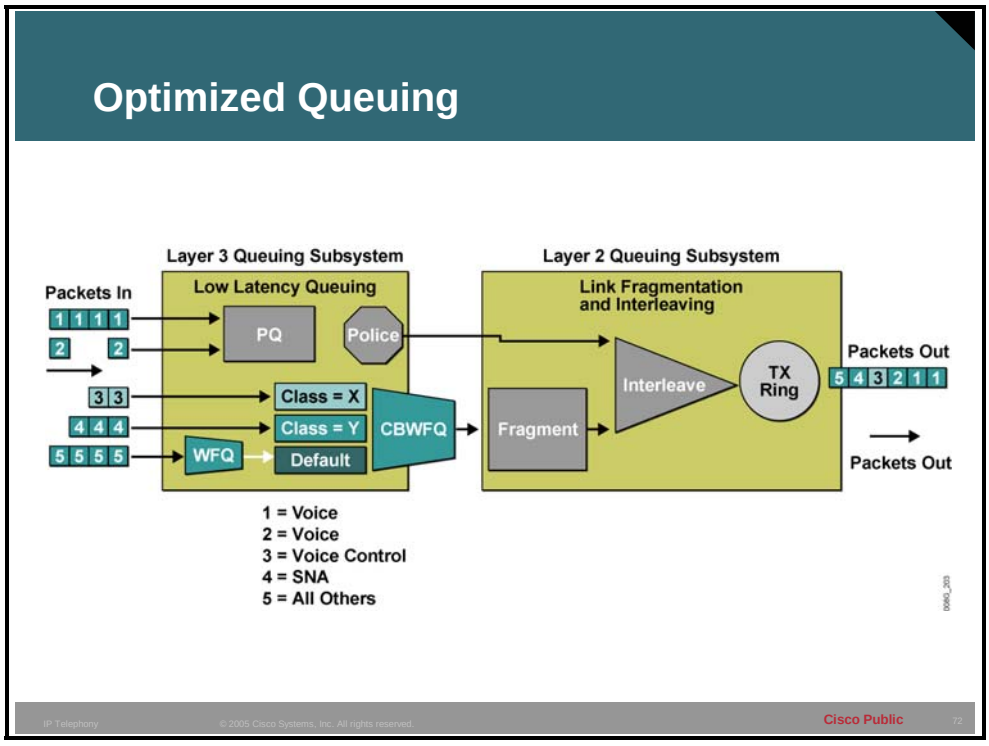
This topic describes bandwidth provisioning as a tool for implementing QoS in the WAN.



The figure represents a typical network. This network has a number of delay-sensitive traffic types: voice, video, and Systems Network Architecture (SNA). Before you place voice and video on a network, you must ensure that adequate bandwidth exists for all required applications; for example, SNA is also delay-sensitive but should not be queued *ahead* of voice and video. To begin, the minimum bandwidth requirements for each major application (for example, voice media streams, video streams, voice control protocols, and all data traffic) should be summed. This sum represents the minimum bandwidth requirement for any given link, and it should consume no more than 75 percent of the total bandwidth that is available on that link. This 75 percent rule assumes that some bandwidth is required for overhead traffic, such as routing and Layer 2 keepalives, as well as for additional applications such as e-mail, HTTP traffic, and other data traffic that is not easily measured.

Optimized Queuing

This topic describes optimized queuing as a tool for implementing QoS in the WAN.



When you are choosing from among the many available prioritization schemes, the major factors that you must consider include the type of traffic on the network and the wide-area media that is being traversed.

For multiservice traffic over an IP WAN, Cisco recommends LLQ for low-speed links. This approach allows up to 64 traffic classes with the ability to specify, for example, PQ behavior for voice and interactive video, a minimum bandwidth for SNA data and market data feeds, and, as illustrated in the figure, WFQ to other traffic types.

Example: Optimized Queuing

The figure illustrates LLQ, which works as follows:

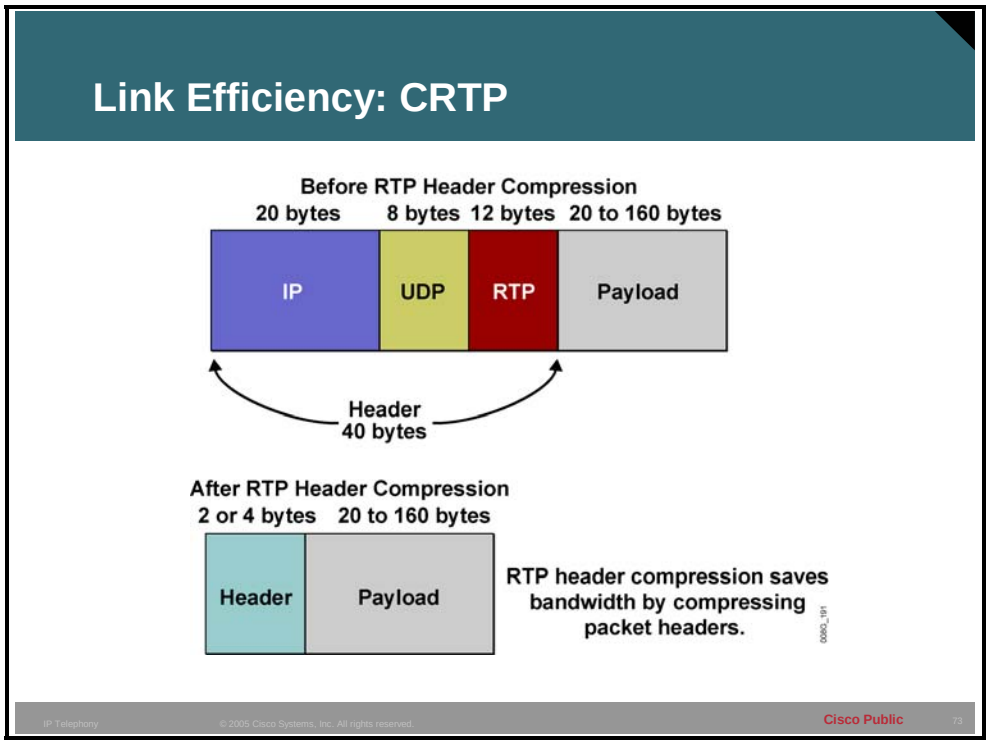
- Voice is placed into a queue with PQ capabilities and allocated a bandwidth of 48 kbps, for example. This bandwidth is based on the total number of expected calls. The entrance criterion to this queue should be the DSCP value of Express Forwarding (EF), or IP precedence value of 5. Traffic in excess of 48 kbps is dropped if the interface becomes congested. Therefore, you must use an admission control mechanism to ensure that you do not exceed this value.
- As the WAN links become congested, it is possible to completely starve the voice control signaling protocols and therefore eliminate the capacity of the IP Phones to complete calls across the IP WAN. Voice control protocol traffic, such as H.323 and SCCP, requires its own CBWFQ with a minimum configurable bandwidth equal to a DSCP value of AF31, which correlates to an IP precedence value of 3.

 Copyright © 2005, Cisco Systems, Inc.

- SNA traffic is placed into a queue that has a specified bandwidth of 56 kbps, for example. This bandwidth represents the expected SNA demand on the network. Queuing operation within this class is FIFO with a minimum allocated bandwidth of 56 kbps. Traffic in this class that exceeds 56 kbps is placed in the default queue. The entrance criterion to this queue could be TCP port numbers, a Layer 3 address, IP precedence, or a DSCP.
- You can place all remaining traffic in a default queue. If a bandwidth is specified, the queuing operation is FIFO. Alternatively, specifying the keyword **fair** assigns WFQ to the operation.

Link Efficiency

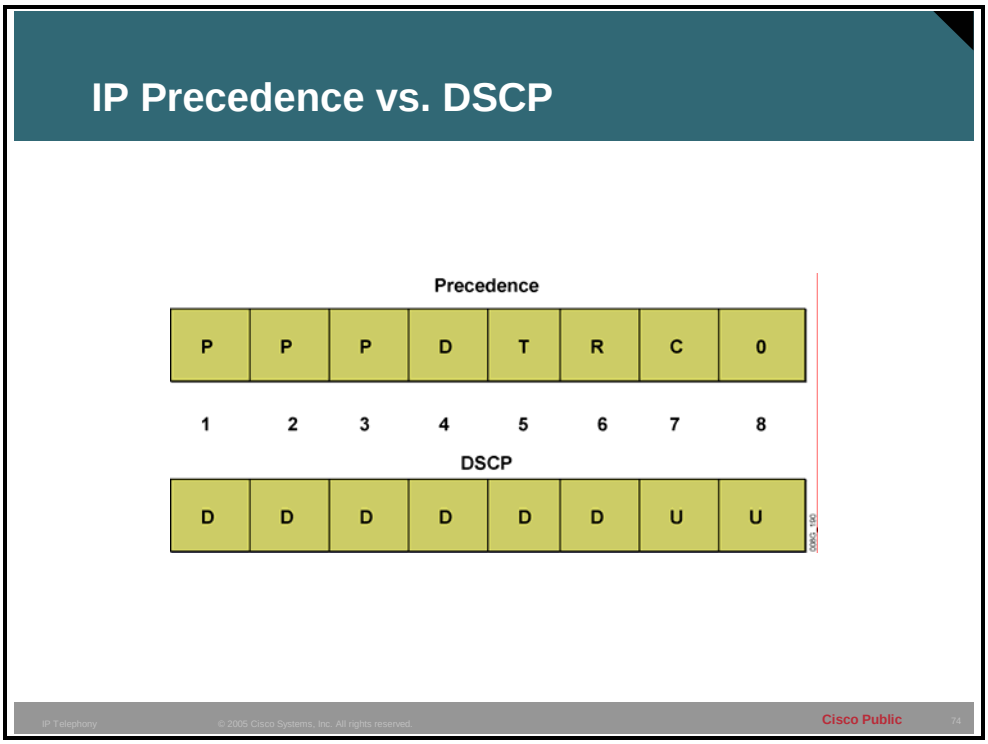
This topic describes link efficiency as a tool for implementing QoS in the WAN.



Because wide-area bandwidth is often prohibitively expensive, only low-speed circuits may be available or cost-effective when you are interconnecting remote sites. In this scenario, it is important to achieve the maximum savings by transmitting as many voice calls as possible over the low-speed link. Many compression schemes, such as G.729, can squeeze a 64-kbps call down to an 8-kbps payload. Cisco gateways and IP Phones support a range of codecs that enhance efficiency on these low-speed links.

The link efficiency is further increased by using CRTP, which compresses a 40-byte IP + UDP + RTP header to approximately 2 to 4 bytes. In addition, VAD takes advantage of the fact that in most conversations, only one party is talking at a time. VAD recovers this empty time and allows data to use the bandwidth.

 Copyright © 2005, Cisco Systems, Inc.



IP Precedence

The 8-bit CoS field in an IP packet header was originally defined in RFC 791 (superseded by RFC 1122). It defined the most significant bits as shown in the table.

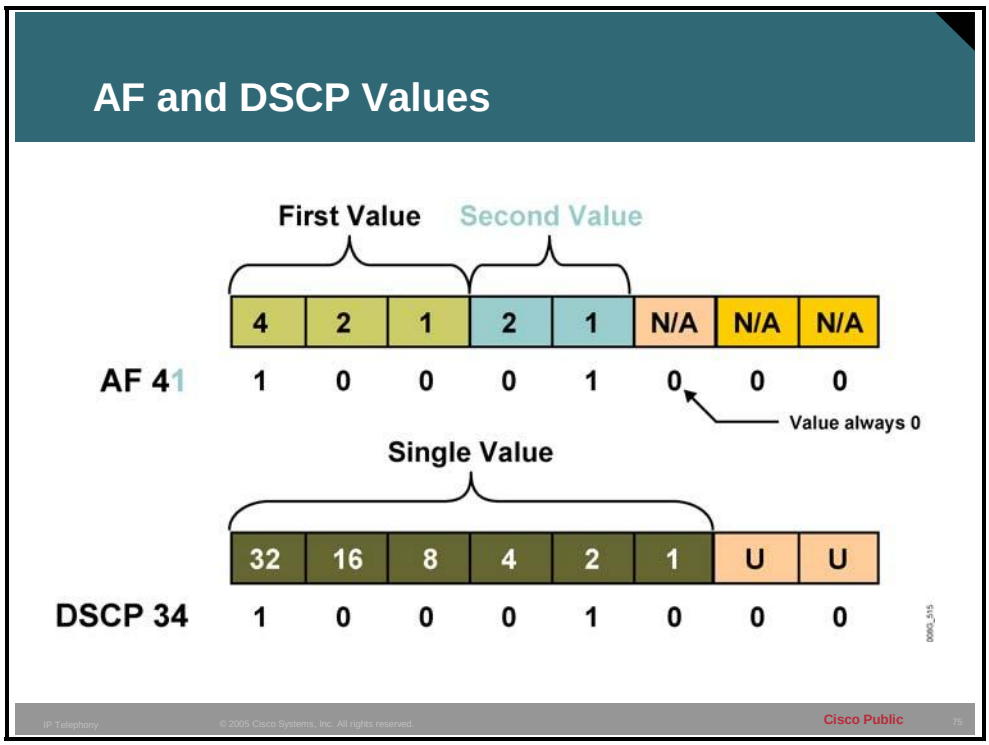
IP Precedence

Binary Value	Precedence Value	Description
111	7	Network Control
110	6	Internetwork Control
101	5	Critical
100	4	Flash Override
011	3	Flash
010	2	Immediate
001	1	Priority
000	0	Routine

In addition, the next 4 bits, when turned on, refer to the following:

- **Bit 4, D:** Instructs the network to minimize delay
- **Bit 5, T:** Instructs the network to maximize throughput
- **Bit 6, R:** Instructs the network to maximize reliability
- **Bit 7, C:** Instructs the network to minimize costs
- **Bit 8:** Reserved for future use

DSCP



The newest use of the eight CoS bits is commonly called the DiffServ standard. It uses the same precedence bits (the most significant bits: 1, 2, and 3) for priority setting, but further clarifies their functions and definitions and offers finer priority granularity through use of the next three bits in the CoS field. DiffServ reorganizes and renames the precedence levels (still defined by the three most significant bits of the CoS field) into the categories shown in the table.

DiffServ Standard

Precedence Bits	Description
Precedence 7	Stays the same (link layer and routing protocol keepalive)
Precedence 6	Stays the same (used for IP routing protocols)
Precedence 5	EF
Precedence 4	Class 4
Precedence 3	Class 3
Precedence 2	Class 2
Precedence 1	Class 1
Precedence 0	Best effort

Bits 3 and 4 of the CoS field (now called the DSCP in the DiffServ standard) allow further priority granularity through the specification of packet-drop probability for any of the defined classes. Collectively, classes 1 through 4 are referred to as Assured Forwarding (AF). The table illustrates the DSCP coding for specifying the priority level (class) plus the drop percentage.

 Copyright © 2005, Cisco Systems, Inc.

(Bits 1, 2, and 3 define the class; bits 4 and 5 specify the drop percentage; bit 6 is always 0.) As an example, AF41 is expressed as 100010, where the first three bits represent class 4, the next two bits specify a low drop percentage, and the last bit is always 0. AF41 has a higher priority than any class 3, 2, or 1, and enjoys the lowest drop percentage. AF41 is also referred to as DSCP 34, as shown in the figure.

DSCP Coding

Drop Percentage	DSCP Coding			
	Class 1	Class 2	Class 3	Class 4
Low drop percentage	001010	010010	011010	100010
Medium drop percentage	001100	010100	011100	100100
High drop percentage	001110	010110	011110	100110

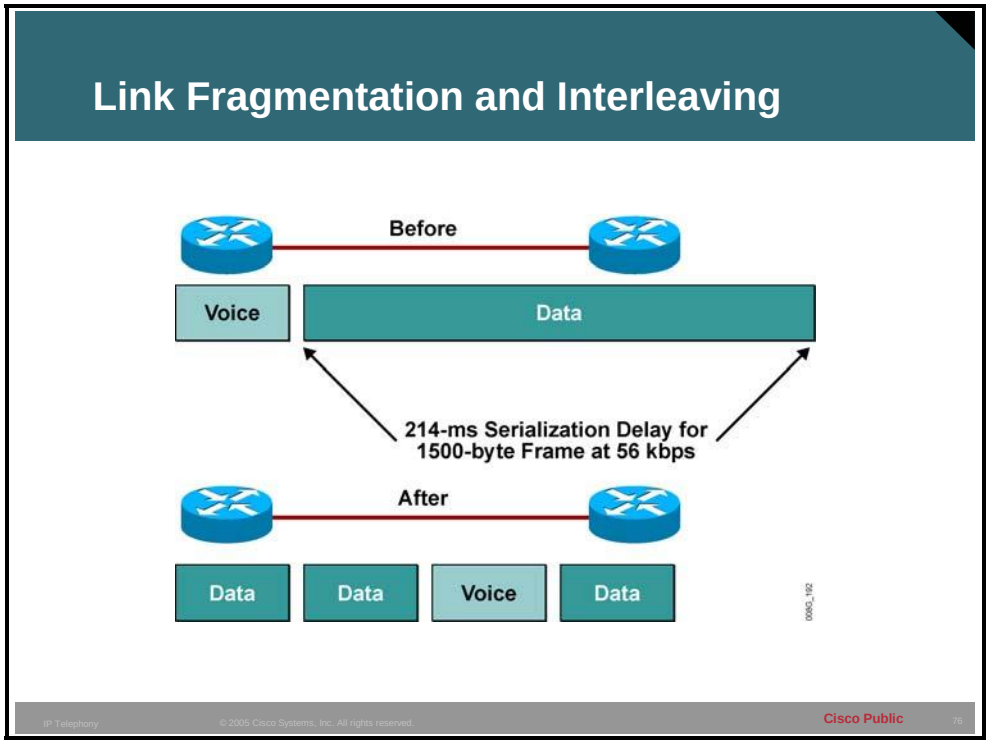
Using this system, a device first prioritizes traffic by class, then differentiates and prioritizes traffic that is in the same class by considering the drop percentage. It is important to note that this standard does not offer a precise definition of low, medium, and high drop percentages. Additionally, not all devices recognize the DiffServ bit 4 and 5 settings. In fact, even when the settings are recognized, they do not necessarily trigger the same forwarding action from each device on the network.

Each device implements its own response in relation to the packet priorities that it detects. The DiffServ proposal is meant to allow a finer granularity of priority setting for the applications and devices that can use it, but it does not specify interpretation (that is, action to be taken). In this application, bits 7 and 8 are unused.

The figure shows the relationship between AF values and DSCP values. AF41 can also be referred to as DSCP 34.

Link Fragmentation and Interleaving

This topic describes link fragmentation and interleaving (LFI) as a tool for implementing QoS in the WAN.



For low-speed links (less than 768 kbps), it is necessary to use techniques that provide LFI. This approach places bounds on jitter by preventing the delay of voice traffic behind large data frames. The following three techniques exist for this purpose:

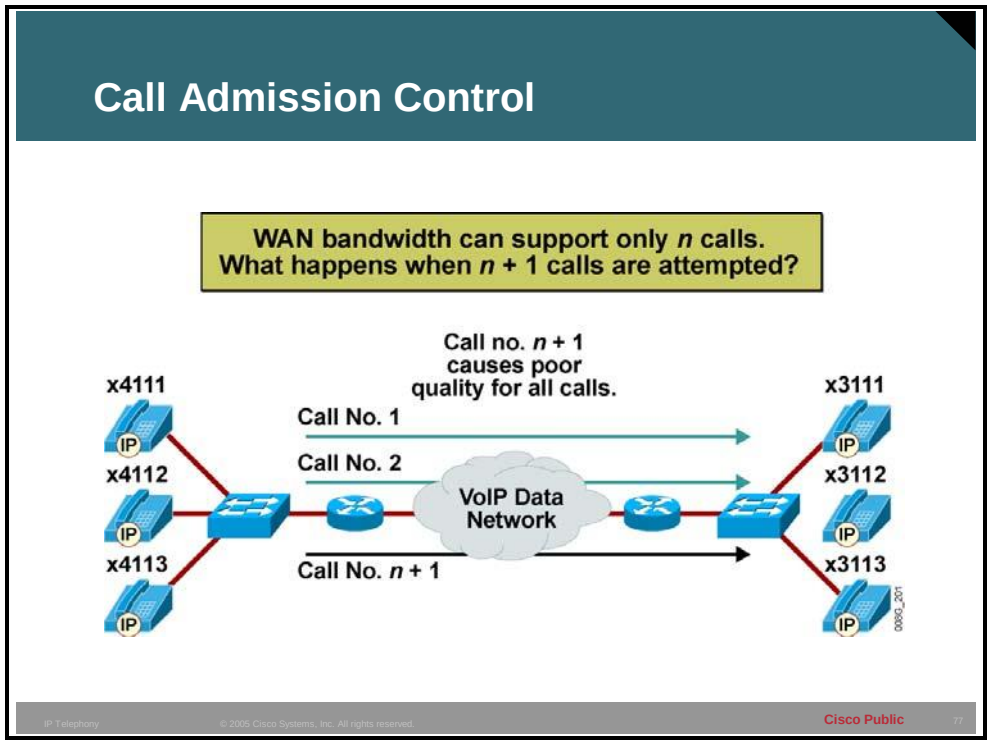
- MLP for point-to-point serial links
- FRF.12 for Frame Relay
- MLP over ATM for ATM connections

The figure shows the necessity of fragmenting the large data packet into smaller segments. Data packets should be fragmented to the same size as voice packets. If the data packets are fragmented to a size smaller than voice packets, voice packets will also be fragmented. Determining the size of the voice packet will depend on the codec type selected. Also, remember that using CRTP can reduce the size of a voice packet significantly.

 Copyright © 2005, Cisco Systems, Inc.

CAC

This topic describes CAC as a tool for implementing QoS in the WAN.



CAC is required to ensure that network resources are not oversubscribed. CAC could be described as a way to protect voice from voice. Calls that exceed the specified bandwidth are either rerouted using an alternative route such as the PSTN, or a fast busy tone is returned to the calling party. This way the next voice call does not degrade the quality of all the calls on the link. You can implement CAC on a gatekeeper or by using Cisco CallManager.

Reference For more information on VoIP CAC, see the following topic on the Cisco.com website: http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/cac.htm

Example: CAC

The figure illustrates the need for CAC. If the network segment was designed to carry two VoIP calls, then when the third call arrives at either the gatekeeper or the CallManager, the call is either rerouted to the PSTN or the caller is sent a fast busy tone. This way, the third call does not impact the quality of the two existing calls.

Cisco Systems
Networking Academy

Course Glossary

Cisco Networking Academy Program

IP Telephone v1.0

NOTE: The Course Glossary for *IP Telephony* v1.0 highlights and defines key terms and acronyms used throughout this course. Many of these terms are also described in the Cisco Internetworking Terms and Acronyms resource, available via http://www.cisco.com.

Acronym or Term	Definition
3DES	Triple Data Encryption Standard. A stronger form of the Data Encryption Standard (DES), 3DES follows a pattern of encryption/decryption/encryption. 3DES has many different variations.
AAL1	ATM adaptation layer 1. One of four AALs recommended by the ITU-T. AAL1 is used for connection-oriented, delay-sensitive services requiring constant bit rates, such as uncompressed video and other isochronous traffic.
ABR	available bit rate. QoS class defined by the ATM Forum for ATM networks. ABR is used for connections that do not require timing relationships between source and destination. ABR provides no guarantees in terms of cell loss or delay, providing only best-effort service. Traffic sources adjust their transmission rate in response to information they receive describing the status of the network and its capability to successfully deliver data.
access rate	*See* AR.
adaptive differential pulse code modulation	*See* ADPCM.
adaptive predictive coding	*See* APC.
Ad-Hoc conference	A conference call feature where a conference is started by an initiator and only the initiator of the conference can add people into the conference.
admission request	*See* ARQ.
ADPCM	adaptive differential pulse code modulation. A waveform process by which analog voice samples are encoded into digital signals.
advanced integration module	*See* AIM.
Advanced Research Projects Agency	*See* ARPA.
AF	Assured Forwarding. A means of providing different levels of forwarding assurances for IP packets. This method is used by providers who offer differentiated services to their customers.
AIM	advanced integration module. A module in some Cisco routers that provides enhanced processing capabilities to the routers.
alternate mark inversion	*See* AMI.
American National Standards Institute	*See* ANSI.
AMI	alternate mark inversion. Line-code modulation type used on T1 and E1 circuits. In AMI, marks (or ones) cause a pulse in alternating positive and negative directions, while zeros never pulse. Two pulses of the same polarity are not allowed. AMI requires that the sending device maintain ones density. Ones density is not maintained independently of the data stream. Sometimes called *binary coded alternate mark inversion*.
ANI	automatic number identification. SS7 feature in which a series of digits, either analog or digital, are included in the call, identifying the telephone number of the calling device. In other words, ANI identifies the number of the calling party. *See also* CLID.
ANSI	American National Standards Institute. A voluntary organization composed of corporate, government, and other members that coordinates standards-related activities, approves U.S. national standards, and develops positions for the United States in international standards organizations. ANSI helps develop international and U.S. standards relating to, among other things, communications and networking. ANSI is a member of the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO).

 Copyright © 2005, Cisco Systems, Inc.

Acronym or Term	Definition
APC	adaptive predictive coding. A narrowband analog-to-digital conversion technique employing a one-level or multilevel sampling system in which the value of the signal at each sample time is adaptively predicted to be a linear function of the past values of the quantized signals. APC is related to LPC in that both use adaptive predictors. However, APC uses fewer prediction coefficients, thus requiring a higher bit-rate than LPC.
API	application programming interface. The means by which an application program talks to communications software. Standardized APIs allow application programs to be developed independently of the underlying method of communication. A set of standard software interrupts, calls, and data formats that computer application programs use to initiate contact with other devices (for example, network services, mainframe communications programs, or other program-to-program communications). Typically, APIs make it easier for software developers to create the links that an application needs to communicate with the operating system or with the network.
application programming interface	*See* API.
AR	access rate. (1) The maximum data rate of the access channel, typically referring to access to broadband networks and network services. (2) A Frame Relay term that addresses the maximum transmission rate supported by the access link into the network, and the port speed of the device (switch or router) at the edge of the carrier network. The AR defines the maximum rate for data transmission or receipt. *See also* CIR.
ARPA	Advanced Research Projects Agency. Research and development organization that is part of Department of Defense (DoD). ARPA is responsible for numerous technological advances in communications and networking. ARPA evolved into Defense Advanced Research Projects Agency (DARPA), and then back into ARPA again (in 1994).
ARQ	admission request. An RAS admission message defined as an attempt by an endpoint to initiate a call.
AS5300	A series of Cisco gateways that provide reliable, scalable, and feature-rich data and voice gateway functionality. The Cisco AS5300 Series Universal Gateways include the Cisco AS5300 Access Server/Voice Gateway and the Cisco AS5350 Universal Gateway.
Assured Forwarding	*See* AF.
Asynchronous Transfer Mode	*See* ATM.
ATM	Asynchronous Transfer Mode. The international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53-byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM is designed to take advantage of high-speed transmission media, such as E3, SONET, and T3.
ATM adaptation layer 1	*See* AAL1.
automatic number identification	*See* ANI.
available bit rate	*See* ABR.
B8ZS	binary 8-zero substitution. Line-code modulation type used on T1 circuits. In B8ZS, marks (or ones) cause a pulse in alternating positive and negative directions, while zeros never pulse. Two pulses of the same polarity are not allowed, except when inserting a code to represent eight zeros. B8ZS maintains ones density by inserting a special code in place of eight consecutive zeros. The special code contains intentional violations of the bipolar pattern.
bandwidth change request	*See* BRQ.
basic call	*See* BC.
BC	basic call. A call between two users that does not require Advanced Intelligent Network Release 1 features (e.g., a POTS call).

Acronym or Term	Definition
Bc	committed burst. Negotiated tariff metric in Frame Relay internetworks. The maximum amount of data (in bits) that a Frame Relay internetwork is committed to accept and transmit above the CIR. *See also* Be *and* CIR.
Be	excess burst. Negotiated tariff metric in Frame Relay internetworks. The number of bits that a Frame Relay internetwork attempts to transmit after Bc is accommodated. Be data, in general, is delivered with a lower probability than Bc data because Be data can be marked as DE by the network. *See also* Bc.
Bell operating company	*See* BOC.
BHCA	busy hour call attempts. A traffic engineering term that refers to the number of call attempts made during the busiest hour of the day.
binary 8-zero substitution	*See* B8ZS.
BLF	busy lampfield. A visual display of the status of all or some of your phones. Your BLF tells you if a phone is busy or on hold. Your BLF is typically attached to or part of your operator phone.
BOC	Bell operating company. BOC is a term for any of the 22 original companies (or their successors) that were created when AT&T was broken up in 1983 and given the right to provide local telephone service in a given geographic area. The companies had previously existed as subsidiaries of AT&T and were called the ”Bell System.” The purpose of the breakup was to create competition at both the local and long-distance service levels. BOCs compete with other, independent companies to sell local phone service. In certain areas, long-distance companies, including AT&T, can now compete for local service. Collectively, companies offering local phone service are referred to legally as local exchange carriers (LECs). BOCs are not allowed to manufacture equipment and were initially not allowed to provide long-distance service. The Telecommunications Act of 1996 now permits them to engage in long-distance business under certain circumstances. As of 1996, the BOCs consisted of original and successor companies to: Bell Telephone Company of Nevada, Illinois Bell, Indiana Bell, Michigan Bell, New England Telephone and Telegraph Company, New Jersey Bell, New York Telephone Company, U S West Communications Company, South Central Bell, Southern Bell, Southwestern Bell, Bell Telephone of Pennsylvania, The Chesapeake and Potomac Telephone Company, The Chesapeake and Potomac Telephone Company of Maryland, The Chesapeake and Potomac Telephone Company of Virginia, The Diamond State Telephone Company, The Ohio Bell Telephone Company, The Pacific Telephone and Telegraph Company, and the Wisconsin Telephone Company.
BRI voice module	*See* BVM.
BRQ	bandwidth change request. RAS bandwidth control message sent by endpoint to gatekeeper requesting an increase/decrease in call bandwidth.
busy hour call attempts	*See* BHCA.
busy lampfield	*See* BLF.
BVM	BRI voice module. An optional device for Cisco modular routers providing four ISDN BRI ports for connection to ISDN PBXs or PINXs. The BVM has four ISDN BRI ports for voice traffic. Each BRI port supports two voice channels (ISDN B channels) and one signaling channel (ISDN D channel).
calling line ID	*See* CLID.
CAS	channel associated signaling. The transmission of signaling information in association with the voice channel. In T1 networks, CAS signaling often is referred to as “robbed-bit” signaling because the network is robbing user bandwidth for other purposes.
CBR	constant bit rate. QoS class defined by the ATM Forum for ATM networks. CBR is used for connections that depend on precise clocking to ensure undistorted delivery.

 Copyright © 2005, Cisco Systems, Inc.

Acronym or Term	Definition
CBWFQ	class-based weighted fair queuing. Congestion management mechanism that extends the standard WFQ functionality to provide support for user-defined traffic classes.
CCIS	common channel interoffice signaling. A technology that uses a common link to carry signaling information for a number of trunks. CCIS is similar to ITU-T SS6 protocol that operated at low bit rates (2.4, 4.8, and 9.6 kbps) and transmitted messages that were only 28 bits in length.
CCITT	Consultative Committee for International Telegraph and Telephone. Former name for the International organization responsible for the development of communications standards. Now called the ITU-T. *See also* ITU-T.
CCS	common channel signaling. Signaling system used in telephone networks that utilizes a statistical multiplexing protocol for signaling. A specified channel is exclusively designated to carry signaling information for all channels in the system. An example is ISDN or SS7. *See also* SS7.
CDVT	cell delay variation tolerance. In ATM, a QoS parameter for managing traffic that is specified when a connection is set up. In CBR transmissions, CDVT determines the level of jitter that is tolerable for the data samples taken by the PCR. *See also* CRB.
cell delay variation tolerance	*See* CDVT.
CELP	code excited linear prediction. Compression algorithm used in low bit-rate voice encoding. Used in ITU-T Recommendations G.728, G.729, G.723.1.
central office	*See* CO.
centum call seconds	Units used to measure traffic load. A CCS is 1/36th of an erlang. The formula for a centum call second is the number of calls per hour multiplied by their average duration in seconds, all divided by 100.
CES	circuit emulation service. Enables users to multiplex or to concentrate multiple circuit emulation streams for voice and video with packet data on a single high-speed ATM link without a separate ATM access multiplexer.
channel associated signaling	*See* CAS.
channel ID	*See* CID.
CID	channel ID. Designates the Frame Relay subchannel ID for Voice over Frame Relay.
CIR	committed information rate. The rate at which a Frame Relay network agrees to transfer information under normal conditions, averaged over a minimum increment of time. CIR, measured in bits per second, is one of the key negotiated tariff metrics. *See also* Bc.
circuit emulation service	*See* CES.
Cisco Architecture for Voice, Video and Integrated Data	*See* Cisco AVVID.
Cisco AVVID	Cisco Architecture for Voice, Video and Integrated Data. Cisco AVVID is the architecture for Voice, Video and Integrated Data. Cisco AVVID includes three components: infrastructure, such as switches and routers; clients, such as IP Phones, H.323 videoconferencing equipment, and PCs; and applications, such as call control, that use a common IP network.
Cisco CallManager	Software-based call-processing agent. It is a component of the Cisco IP telephony solution, part of Cisco AVVID. The software extends enterprise telephony features and functions to packet telephony network devices such as IP Phones, media processing devices, VoIP gateways, and multimedia applications.
Cisco.com	The name of the Cisco Systems external website.

Acronym or Term	Definition
Cisco ICM software	Cisco Intelligent Call Management software. Software, which delivers an integrated suite of contact center capabilities. Cisco ICM software provides intelligent queue management in a contact center environment. It enables improved queue management across a variety of ACDs from different vendors as well as integrating IVRs, database and desktop applications, and CTI solutions
Cisco Intelligent Call Management software	*See* Cisco ICM software.
Cisco IOS	Cisco Systems software that provides common functionality, scalability, and security for all products under the CiscoFusion architecture. Cisco IOS software allows centralized, integrated, and automated installation and management of internetworks while ensuring support for a wide variety of protocols, media, services, and platforms.
Cisco IPCC	Cisco IP Contact Center. An integrated suite of products that enables contact center agents using Cisco IP Phones to receive both TDM and VoIP calls. IPCC provides ACD and IVR capabilities in a single-vender IP suite. The IPCC can be implemented in a single-site environment or integrated into an enterprise-wide multisite contact center.
Cisco IP Contact Center	*See* Cisco IPCC.
Cisco IP Phone	The Cisco family of IP Phones provides a complete range of intelligent communication systems that use the data network while providing the convenience and ease of use of a business telephone.
Cisco IP SoftPhone	A Windows-based application for the PC. Used as a standalone end station or in conjunction with the Cisco IP Phone, it provides mobility, directory integration, user interface, and a virtual conference room.
class-based weighted fair queuing	*See* CBWFQ.
CLEC	competitive local exchange carrier. A company that builds and operates communication networks in metropolitan areas and provides its customers with an alternative to the local telephone company. In the United States, a CLEC is a company that competes with the already established local telephone business by providing its own network and switching. The term distinguishes new or potential competitors from established local exchange carriers (LECs) and arises from the Telecommunications Act of 1996, which was intended to promote competition among both long-distance and local phone service providers. North American Telecom and Winstar Communications are examples of CLECs, which are generally listed as simply “local exchange carriers.”
CLI	command-line interface. An interface that allows the user to interact with the operating system by entering commands and optional arguments. The UNIX operating system and Microsoft MS-DOS provide CLIs.
CLID	calling line ID. Information about the billing telephone number from which a call originated. The CLID value might be the entire telephone number, the area code, or the area code plus the local exchange. Also known as Caller ID.
CNG	comfort noise generation. While using VAD, the DSP at the destination emulates background noise from the source side, preventing the perception that a call is disconnected.
CO	central office. The local telephone company office to which all local loops in a given area connect and in which circuit switching of subscriber lines occurs.
“Codebook” excitation index	Used by the receiver to look up a set of excitation values. A codebook is a set of rules that helps to determine what conditions indicate a Cisco device fault.
code excited linear prediction	*See* CELP.
comfort noise generation	*See* CNG.

 Copyright © 2005, Cisco Systems, Inc.

Acronym or Term	Definition
command-line interface	*See* CLI.
committed burst	*See* Bc.
committed information rate	*See* CIR.
common channel interoffice signaling	*See* CCIS.
common channel signaling	*See* CCS.
competitive local exchange carrier	*See* CLEC.
Compressed Real-Time Transport Protocol	*See* CRTP.
computer telephony integration	*See* CTI.
Conjugate Structure Algebraic Code Excited Linear Prediction	*See* CS-ACELP.
constant bit rate	*See* CBR.
Consultative Committee for International Telegraph and Telephone	*See* CCITT.
CPE	customer premises equipment. (1) Terminating equipment, such as terminals, telephones, and modems, installed at customer sites, and connected to the telephone company network. (2) Any telephone equipment residing on the customer site.
CRC	cyclic redundancy check. Error-checking technique in which the frame recipient calculates a remainder by dividing frame contents by a prime binary divisor and compares the calculated remainder to a value stored in the frame by the sending node.
cross-connect (adj.) cross connect (n, v)	Cross connect is a connection scheme between cabling runs, subsystems, and equipment, using patch cords or jumpers that attach to connecting hardware on each end. Cross-connection is the attachment of one wire to another, usually by anchoring each wire to a connecting block and then placing a third wire between them so that an electrical connection is made. The TIA/EIA-568-A standard specifies that cross-connect cables (also called patch cords) are to be made out of stranded cable.
CRTP	Compressed Real-Time Transport Protocol. A type of header compression designed to reduce the IP/UDP/RTP headers to two bytes for most packets in the case where no UDP checksums are being sent, or four bytes with checksums.
CS-ACELP	Conjugate Structure Algebraic Code Excited Linear Prediction. CELP voice compression algorithm providing 8 kbps, or 8:1 compression, standardized in ITU-T Recommendation G.729 or G.729A.
CTI	computer telephony integration. The name given to the merger of traditional telecommunications (PBX) equipment with computers and computer applications. The use of caller ID to retrieve customer information automatically from a database is an example of a CTI application.
customer premises equipment	*See* CPE.
cyclic redundancy check	*See* CRC.
DACS	digital access and crossconnect system. A digital cross-connect system that provides grooming, switching, and aggregation.

Acronym or Term	Definition
data carrier detect	*See* DCD.
data circuit-terminating equipment (ITU-T expansion)	*See* DCE.
data communications equipment (EIA expansion)	*See* DCE.
data-link connection identifier	*See* DLCI.
data terminal equipment	*See* DTE.
data terminal ready	*See* DTR.
dB	decibel. Unit for measuring relative power ratios in terms of gain or loss. The rule of thumb to remember is that 10 dB indicates an increase (or a loss) by a factor of 10; 20 dB indicates an increase (or a loss) by a factor of 100; 30 dB indicates an increase (or a loss) by a factor of 1000.
DCD	data carrier detect. Signal from the DCE (modem or printer) to the DTE (typically your PC), indicating that the modem is receiving a carrier signal from the DCE (modem) at the other end of the telephone circuit.
DCE	data communications equipment (EIA expansion). data circuit-terminating equipment (ITU-T expansion). Devices and connections of a communications network that comprise the network end of the user-to-network interface. The DCE provides a physical connection to the network, forwards traffic, and typically provides a clocking signal used to synchronize data transmission between DCE and DTE devices. Modems and interface cards are examples of DCE.
DDS	digital data service. A class of service that is offered by telecommunications companies to transport data rather than voice. Originally called Dataphone Digital Service by AT&T in the late 1970s.
DE bits	discard eligible bits. Bits that are used to tag Frame Relay frames that are eligible to be discarded if the network gets congested.
decibel	*See* dB.
delay budget	The maximum amount of delay in data, voice, and video applications. The total end-to-end delay when engineering a VoIP implementation should not exceed the 150- to 200-ms delay budget.
Delay Dial	A signaling method in which the terminating side remains off hook until it is ready to receive address information. The off-hook interval is the delay dial signal.
DHCP	Dynamic Host Configuration Protocol. Provides a mechanism for allocating IP addresses dynamically so that addresses can be reused when hosts no longer need them.
Dialed Number Identification Service	*See* DNIS.
dial plan mapper	Provides the mapping of IP addresses to telephone numbers. After enough digits are accumulated to match a configured destination pattern, the dial plan mapper maps the IP host to a telephone number.
dial pulse	*See* DP.

 Copyright © 2005, Cisco Systems, Inc.

Acronym or Term	Definition
dialup (adj, n) dial up (v)	Modem access to a data network. The use of a dial or push-button telephone to create a telephone or data call. Dialup calls are usually billed by time of day, duration of call, and distance traveled. It is a connection to the Internet, or any network, where a modem and a standard telephone are used to make a connection between computers.
dialup remote access server	A remote access server is computer hardware that resides on a corporate LAN and into which employees dial on the PSTN to get access to their e-mail and to software and data on the corporate LAN (for example, status on customer orders). Remote access servers are also used by commercial service providers, such as ISPs, to allow their customers access into their networks. Remote access servers are typically measured by how many simultaneous dial-in users (on analog or digital lines) they can handle and whether they can work with cheaper digital circuits, such as T 1 and E 1 connections.
digital access and crossconnect system	*See* DACS.
digital data service	*See* DDS.
Digital Private Network Signaling System	*See* DPNSS.
digital service level zero	*See* DS0.
digital signal processor	*See* DSP.
digital speech interpolation	*See* DSI.
digital subscriber line	*See* DSL.
Digital T1/E1 Packet Voice Trunk Network Module	A flexible and scalable T1/E1 voice solution for Cisco 2600 and 3600 series Modular Access routers that supports up to 60 voice channels in a single network module.
Digital T1/E1 voice port adapter	A single-width port adapter, which incorporates one or two universal ports configurable for either T1 or E1 connection with high-performance DSP support for up to 24 to120 channels of compressed voice.
discard eligible bits	*See* DE bits.
disengage request	*See* DRQ.
DLCI	data-link connection identifier. Value that specifies a PVC or an SVC in a Frame Relay network. In the basic Frame Relay specification, DLCIs are locally significant (connected devices might use different values to specify the same connection at different ends of the network).
DNIS	Dialed Number Identification Service. Feature of trunk lines where the called number is identified; this called number information is used to route the call to the appropriate service. DNIS is a service used with toll-free dedicated services whereby calls placed to specific toll-free numbers are routed to the appropriate area within the company.
DP	dial pulse. A means of signaling that consists of regular momentary interruptions of a direct or alternating current at the sending end in which the number of interruptions corresponds to the value of the digit or character. In short, the old style of rotary dialing. Dial the number "5" and you will hear five "clicks."
DPNSS	Digital Private Network Signaling System. A common-channel, message-oriented signaling protocol commonly used by PBXs.

Acronym or Term	Definition
drop and insert	Allows DS-0 channels from one T1 or E1 facility to be cross-connected digitally to DS-0 channels on another T1 or E1. By using this method, channel traffic is sent between a PBX and a CO PSTN switch or other telephony device, so that some PBX channels are directed for long-distance service through the PSTN while the router compresses others for interoffice VoIP calls. In addition, drop and insert can cross connect a telephony switch (from the CO or PSTN) to a channel bank for external analog connectivity. Also called TDM Cross-Connect. *See* DACS.
DRQ	disengage request. RAS message sent by the gateway to the gatekeeper during the process of a call. The gateway waits for the DCF message before it sends the setup message to the new destination gatekeeper.
DS0	digital service level zero. Single timeslot on a DS1 (also known as T1) digital interface—that is, a 64-kbps, synchronous, full-duplex data channel, typically used for a single voice connection on a PBX. Also, a single timeslot on an E1.
DSI	digital speech interpolation. An algorithm that analyzes voice channels for silence. It suppresses the voice bits to conserve packet-line bandwidth and inserts a code to indicate to the far end that these bits have been removed. Also referred to as VAD.
DSL	digital subscriber line. Public network technology that delivers high bandwidth over conventional copper wiring at limited distances. There are four types of DSL: ADSL, HDSL, SDSL, and VDSL. All are provisioned via modem pairs, with one modem located at a central office and the other at the customer site. Because most DSL technologies do not use the whole bandwidth of the twisted pair, there is room remaining for a voice channel.
DSP	digital signal processor. An electronic circuit that compresses voice signals, generates tones, and decodes received compressions. DSPs can also emulate modems for purposes of fax relay.
DTE	data terminal equipment. Device at the user end of a user-network interface that serves as a data source, destination, or both. DTE connects to a data network through a DCE device (for example, a modem) and typically uses clocking signals generated by the DCE. DTE includes such devices as computers, protocol translators, and multiplexers.
DTMF	dual tone multifrequency. Tones generated when a button is pressed on a telephone to convey address signaling.
DTR	data terminal ready. EIA/TIA-232 circuit that is activated to let the DCE know when the DTE is powered up and not in test mode.
dual tone multifrequency	*See* DTMF.
Dynamic Host Configuration Protocol	*See* DHCP.
E&M	ear and mouth. Earth and Magneto. recEive and transMit. (1) Trunking arrangement generally used for two-way switch-to-switch or switch-to-network connections. Cisco analog E&M interface is an 8-pin modular connector that allows connections to PBX trunk lines (tie-lines). E&M also is emulated on E1 and T1 digital interfaces. (2) A type of signaling traditionally used in the telecommunications industry. Indicates the use of a handset that corresponds to the ear (receiving) and mouth (transmitting) component of a telephone.
ear and mouth	*See* E&M.
Earth and Magneto	*See* E&M.
ECMA	European Computer Manufacturers Association. Group of European computer vendors who have done substantial OSI standardization work.
E-lead	The wiring arrangement on an E&M circuit in which the signal side sends its signaling information.

 Copyright © 2005, Cisco Systems, Inc.

Acronym or Term	Definition
ESF	Extended Superframe. Framing type used on T1 circuits that consists of 24 frames of 193 bits each, with the 193rd bit providing framing information and other functions. ESF is an enhanced version of SF. *See also* SF.
ETSI	European Telecommunication Standards Institute. ETSI is a nonprofit organization producing voluntary telecommunications standards used throughout Europe.
European Computer Manufacturers Association	*See* ECMA.
European Telecommunication Standards Institute	*See* ETSI.
excess burst	*See* Be.
Extended Superframe	*See* ESF.
FDM	frequency-division multiplexing. Technique whereby information from multiple channels can be allocated bandwidth on a single wire based on frequency. An example is DSL.
FIFO	first-in/first-out. Refers to a buffering scheme where the first byte of data entering the buffer is the first byte retrieved by the CPU. In telephony, FIFO refers to a queuing scheme where the first calls received are the first calls processed.
first-in/first-out	*See* FIFO.
flash memory	A special type of electrically erasable programmable read-only memory (EEPROM) that can be erased and reprogrammed in blocks instead of one byte at a time. Many modern PCs have their basic input/output system (BIOS) stored on a flash memory chip so that it can be updated easily if necessary. Such a BIOS is sometimes called a flash BIOS. Flash memory is also popular in modems because it enables the modem manufacturer to support new protocols as they become standardized.
Foreign Exchange Office	*See* FXO.
Foreign Exchange Station	*See* FXS.
four-wire	One of two distinct types of audio interfaces (two-wire or four-wire). The four-wire implementation provides separate paths for receiving and sending audio signals, consisting of T, R, and T1, R1 leads.
frame forwarding	Mechanism by which frame-based traffic, such as HDLC and SDLC, traverses an ATM network.
Frame Relay traffic shaping	*See* FRTS.
frequency-division multiplexing	*See* FDM.
FRTS	Frame Relay traffic shaping. Queuing method that uses queues on a Frame Relay network to limit surges that can cause congestion. Data is buffered and sent into the network in regulated amounts to ensure that the traffic can fit within the promised traffic envelope for the particular connection.
FXO	Foreign Exchange Office. An FXO interface connects to the PSTN central office. Cisco FXO interface is an RJ-11 connector that allows an analog connection at the PSTN's central office or to a station interface on a PBX.
FXS	Foreign Exchange Station. An FXS interface connects directly to a standard telephone and supplies ring, voltage, and dial tone. Cisco FXS interface is an RJ-11 connector that allows connections to basic telephone service equipment, key sets, and PBXs.

Acronym or Term	Definition
gatekeeper	(1) The component of an H.323 telephony system that performs call address resolution, admission control, and subnet bandwidth management. (2) Telecommunications: H.323 entity on a LAN that provides address translation and control access to the LAN for H.323 terminals and gateways. The gatekeeper can provide other services to the H.323 terminals and gateways, such as bandwidth management and locating gateways. A gatekeeper maintains a registry of devices in the multimedia network. The devices register with the gatekeeper at startup and request admission to a call from the gatekeeper.
gatekeeper discovery request	*See* GRQ.
gateway	An H.323 term that describes the component of a H.323 telephony network that translates between one technology and another, typically between traditional telephony and TCP/IP.
generic traffic shaping	Shapes traffic by reducing outbound traffic flow to avoid congestion by constraining traffic to a particular bit rate using the token bucket mechanism.
GRQ	gatekeeper discovery request. RAS gatekeeper discovery message sent by endpoint to gatekeeper.
HDB3	high density binary 3. A line coding method used to maintain synchronization by ensuring a sufficient number of binary ones. HDB3 is used on E1 circuits.
HDLC	High-Level Data Link Control. Bit-oriented synchronous data-link-layer protocol developed by International Organization for Standardization (ISO). *See also* SDLC.
high density binary 3	*See* HDB3.
High-Level Data Link Control	*See* HDLC.
Hoot and Holler	A broadcast audio network used extensively by the brokerage industry for market updates and trading. Similar networks are used in publishing, transportation, power plants, and manufacturing.
Hot Standby Router Protocol	*See* HSRP.
HSRP	Hot Standby Router Protocol. Provides high network availability and transparent network topology changes. HSRP creates a hot standby router group with a lead router that services all packets sent to the hot standby address. Other routers in the group monitor the lead router, and if it fails, one of these standby routers inherits the lead position and the hot standby group address.
HTTP	Hypertext Transfer Protocol. The protocol used by web browsers and web servers to transfer files, such as text and graphic files.
Hyperterm software	Terminal emulation software.
Hypertext Transfer Protocol	*See* HTTP.
IC	*See* IXC.
IETF	Internet Engineering Task Force. Task force consisting of over 80 working groups responsible for developing Internet standards

 Copyright © 2005, Cisco Systems, Inc.

Acronym or Term	Definition
ILEC	incumbent local exchange carrier. An ILEC is a telephone company in the United States that was providing local service when the Telecommunications Act of 1996 was enacted. ILECs include the former Bell operating companies (BOCs), which were grouped into holding companies known collectively as the regional Bell operating companies (RBOCs) when the Bell System was broken up by a 1983 consent decree. ILECs are in contradistinction to competitive local exchange carriers (CLECs). A “local exchange” is the local “central office” of an LEC. Lines from homes and businesses terminate at a local exchange. Local exchanges connect to other local exchanges within a local access and transport area (LATA) or to inter-exchange carriers (IXCs), such as long-distance carriers AT&T, MCI, and Sprint.
IMAP	Internet Message Access Protocol. Method of accessing e-mail or bulletin board messages kept on a mail server that can be shared. IMAP permits client e-mail applications to access remote message stores as if they were local without actually transferring the message.
IMT	Inter-Machine Trunk. A means to give service providers access to more favorable tariffs and rates. In SS7 environments, IMTs terminate bearer traffic on the voice gateways.
IN	Intelligent Network. A network that provides IP routing, QoS, network access and control, and network management services.
incumbent local exchange carrier	*See* ILEC.
Integrated Services Digital Network	*See* ISDN.
Intelligent Network	*See* IN.
interactive voice response	*See* IVR.
inter-exchange carrier	*See* IXC.
Inter-Machine Trunk	*See* IMT.
International Telecommunication Union	*See* ITU.
International Telecommunication Union Telecommunication Standardization Sector	*See* ITU-T.
Internet Engineering Task Force	*See* IETF.
Internet Message Access Protocol	*See* IMAP.
Internet Protocol	*See* IP.
IP	Internet Protocol. Network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. Defined in RFC 791.
IP cloud	The area in which data travels through an IP network. Illustrated in diagrams as a cloud.
IP precedence	A 3-bit value in the ToS byte used for assigning precedence to IP packets.
IP RTP priority	A Frame Relay feature that provides a strict priority queuing scheme on a Frame Relay PVC for delay-sensitive data, such as voice.
ISDN	Integrated Services Digital Network. Communication architecture offered by telephone companies that permits customers to access digital networks to carry data, voice, and other source traffic.

Acronym or Term	Definition
ISDN User Part	*See* ISUP.
ISUP	ISDN User Part. SS7 protocol layer that defines the protocol used to prepare, manage, and release trunks that carry voice and data between calling and called parties under the auspice of ISDN.
ITU	International Telecommunication Union. An organization established by the United Nations to set international telecommunications standards and to allocate frequencies for specific uses.
ITU-T	International Telecommunication Union Telecommunication Standardization Sector. International body that develops worldwide standards for telecommunications technologies. The ITU-T carries out the functions of the former CCITT. *See also* CCITT.
IVR	interactive voice response. Term used to describe systems that provide information in the form of recorded messages over telephone lines in response to user input in the form of spoken words, or, more commonly, DTMF signaling. Examples include banks that allow you to check your balance from any telephone, and automated stock quote systems.
IXC	inter-exchange carrier. Common carrier providing long-distance connectivity between local access and transport areas (LATAs). The three major IXCs are AT&T, MCI, and Sprint, but several hundred IXCs offer long-distance service in the United States.
Java Telephony Application Programming Interface	*See* JTAPI.
JTAPI	Java Telephony Application Programming Interface. A Java API for call control developed by Sun Microsystems.
LCC	Lost Calls Cleared
LCD	Lost Calls Delayed
LCH	Lost Calls Held
LDAP	Lightweight Directory Access Protocol. Protocol that provides read/write interactive access to X.500 Directories for uniform application security and access levels.
LDCELP	low-delay CELP. CELP voice compression algorithm providing 16-kbps, or 4:1, compression. Standardized in ITU-T Recommendation G.728.
least significant bit	*See* LSB.
LEC	local exchange carrier. LEC is the term for a public telephone company in the U.S. that provides local service. Some of the largest LECs are the Bell operating companies (BOCs), which were grouped into holding companies known collectively as the regional Bell operating companies (RBOCs) when the Bell System was broken up by a 1983 consent decree. In addition to the Bell companies, there are a number of independent LECs, such as GTE. LEC companies are also sometimes referred to as “telcos.” A “local exchange” is the local “central office” of an LEC. Lines from homes and businesses terminate at a local exchange. Local exchanges connect to other local exchanges within a local access and transport area (LATA) or to interexchange carriers (IXCs) such as long-distance carriers AT&T, MCI, and Sprint.
LFI	link fragmentation and interleaving. A Cisco IOS feature that reduces delay on slower-speed links by breaking up large datagrams and interleaving low-delay traffic packets with the smaller packets resulting from the fragmented datagram.
Lightweight Directory Access Protocol	*See* LDAP.
linear predictive coding	*See* LPC.
line code	Electrical modulation scheme used by digital carrier systems. In North America, T1 uses AMI or B8ZS line coding. In other countries, E1 uses AMI or HDB3 line coding.

 Copyright © 2005, Cisco Systems, Inc.

Acronym or Term	Definition
link fragmentation and interleaving	*See* LFI.
LLQ	Low Latency Queuing. Enables use of a single priority queue in conjunction with CBWFQ. Typically, the priority queue only carries VoIP traffic. All other traffic is carried in the user-defined queues of CBWFQ.
local exchange carrier	*See* LEC.
location request	*See* LRQ.
low-delay CELP	*See* LDCELP.
Low Latency Queuing	*See* LLQ.
LPC	linear predictive coding. Voice coding that uses a special algorithm that models the way human speech works. Because LPC can take advantage of an understanding of the speech process, it can be efficient without sacrificing voice quality.
LRQ	location request. RAS location request message sent to request the gatekeeper contact information for one or more E.164 addresses.
LSB	least significant bit. The bit of a binary expression having the least value; or, representing the number of ones.
Main Distribution Frame	*See* MDF.
MC	multipoint controller. A required part of an MCU. The MC is the conference controller. The MC handles negotiation between all terminals to determine common capabilities and controls conference resources such as multicasting. The MC does not deal directly with any of the media streams.
MCSs	media convergence servers. An integral component of the Cisco IP Communications system. A high availability server platform for Cisco AVVID.
MCU	multipoint control unit. A component that manages videoconferences of three or more participants.
MDF	Main Distribution Frame. The point where all network-related external services, IP equipment, and wiring converge within a building.
mean opinion score	*See* MOS.
media convergence servers	*See* MCSs.
Media Gateway Control Protocol	*See* MGCP.
media termination point	*See* MTP.
Meet-Me conference	A conference feature where everyone who dials the same Meet-Me number will join the conference together.
MEL CAS	Mercury Exchange Limited Channel Associated Signaling. A voice signaling protocol used primarily in the United Kingdom.
Mercury Exchange Limited Channel Associated Signaling	*See* MEL CAS.
MGCP	Media Gateway Control Protocol. Protocol that helps bridge the gap between circuit-switched and IP networks. A combination of IPDC and SGCP, MGCP allows external control and management of data communications devices, or "media gateways" at the edge of multiservice packet networks by software programs.

Acronym or Term	Definition
MICA	Modem ISDN Channel Aggregation. Modem module and card used in the Cisco AS5300 universal access servers. A MICA modem provides an interface between an incoming or outgoing digital call and an ISDN telephone line; the call does not have to be converted to analog as it does with a conventional modem and an analog telephone line. Each line can accommodate, or aggregate, up to 24 (T1) or 30 (E1) calls.
Microsoft NetMeeting	Complete H.323 desktop Internet multimedia solution for all Windows users with multipoint data conferencing, text chat, whiteboard, and file transfer, as well as point-to-point audio and video.
M-lead	The wiring arrangement on an E&M circuit in which the trunking side sends its signaling information.
MLP	Multilink Point-to-Point Protocol. Method of splitting, recombining, and sequencing datagrams across multiple logical data links under the PPP protocol.
Modem ISDN Channel Aggregation	*See* MICA.
MOS	mean opinion score. A common benchmark used to determine the perceived quality of sound produced by specific codecs.
MP	multipoint processor. Part of an MCU. The MP processes the media streams. It receives audio, video, or data bits from the endpoints for which it does the required mixing, switching, and other processing before distributing the stream to the videoconference participants.
MTP	media termination point. A Cisco software application. An MTP software device allows the Cisco CallManager to extend supplementary services, such as hold and transfer, to calls routed through an H.323 endpoint or an H.323 gateway.
multicast backbone	Multicast backbone of the Internet. It is a virtual multicast network composed of multicast LANs and the point-to-point tunnels that interconnect them.
Multilink Point-to-Point Protocol	*See* MLP.
multipoint controller	*See* MC.
multipoint control unit	*See* MCU.
multipoint processor	*See* MP.
network service access point	*See* NSAP.
NSAP	network service access point. Network address, as specified by ISO. An NSAP is the point at which OSI network service is made available to a transport layer (Layer 4) entity.
ODBC	Open Database Connectivity. Abstracts data USING applications from database management systems. Standard API for accessing data in both relational and nonrelational database management systems. Using this API, common database applications can be written to access data stored in a variety of database management systems on a variety of computers regardless of DBMS or programming interface.
off hook	Call condition in which transmission facilities are already in use. Also known as *busy*.
Off-Premises eXtension	*See* OPX.
OMAP	operations, maintenance, administration, and provisioning. Telephony operations functions include monitoring and discovery of problems before they negatively impact service. Administration deals with billing, department cross-charges, accounting, and capacity management. The telephony maintenance function is quite similar to the data networking processes of fault isolation and correction. The final element, provisioning, is used to define services for individual subscribers.

 Copyright © 2005, Cisco Systems, Inc.

Acronym or Term	Definition
on hook	(1) Condition that exists when a receiver or a handset is resting on the switch hook, or is not in use. (2) Idle state (open loop) of a single telephone or PBX line loop.
OOS	Out-of-Service. State of the call or trunk.
Open Database Connectivity	*See* ODBC.
Open System Interconnection	*See* OSI.
operations, maintenance, administration, and provisioning	*See* OMAP.
OPX	Off-Premises eXtension. A telephone line from a telephone system that is terminated in a different building than the one in which the telephone system resides.
OSI	Open System Interconnection. International standardization program created by ISO and ITU-T to develop standards for data networking that facilitate multivendor equipment interoperability.
Out-of-Service	*See* OOS.
packet voice digital signal processor module	*See* PVDM.
PAM	pulse amplitude modulation. Modulation scheme where the modulating wave is caused to modulate the amplitude of a pulse stream.
PBX	private branch exchange. Digital or analog telephone switches located on the customer premises and used to connect private and public telephone networks.
PCI	protocol control information. Control information added to user data to compose an OSI packet. The OSI equivalent of the term “header.”
PCM	pulse code modulation. Technique of encoding analog voice into a 64-kbps data stream by sampling with 8-bit resolution at a rate of 8000 times per second.
PCMCIA	Personal Computer Memory Card Industry Association. A standard interface that connects any type of device to a portable computer. Developed by PCMCIA in the early 1990s.
Perceptual Speech Quality Measurement	*See* PSQM.
permanent virtual circuit	*See* PVC.
Personal Computer Memory Card Industry Association	*See* PCMCIA.
phase-lock loop	*See* PLL.
PINX	private integrated services network exchange. A PBX or key system, which in a BRI voice application uses QSIG signaling.
plain old telephone service	*See* POTS.
PLAR	private line, automatic ringdown. Voice circuit that connects two single endpoints together. When either telephone handset is taken off hook, the remote telephone automatically rings.
PLAR Off-Premises eXtension	*See* PLAR-OPX.

Acronym or Term	Definition
PLAR-OPX	PLAR Off-Premises eXtension. Specifies a PLAR Off-Premises eXtension connection. Using this option, the local voice port provides a local response before the remote voice port receives an answer. On FXO interfaces, the voice port will not answer until the remote side answers.
PLL	phase-lock loop. A circuit on a T1 or E1 module that provides clocking information.
point of presence	*See* POP.
POP	point of presence. In OSS, a physical location where an inter-exchange carrier installed equipment to interconnect with an LEC.
Post, Telephone, and Telegraph	*See* PTT.
POTS	plain old telephone service. Basic telephone service supplying standard single-line telephones, telephone lines, and access to the PSTN. *See also* PSTN.
PQ	priority queuing. PQ ensures that important traffic gets the fastest handling at each point where it is used. It was designed to give strict priority to important traffic.
priority queuing	*See* PQ.
private branch exchange	*See* PBX.
private integrated services network exchange	*See* PINX.
private line, automatic ringdown	*See* PLAR.
protocol control information	*See* PCI.
PSQM	Perceptual Speech Quality Measurement. A technique used for measuring voice quality. It compares the received audio with the transmitted audio.
PSTN	public switched telephone network. General term referring to the variety of telephone networks and services in place worldwide. Sometimes called POTS.
PTT	Post, Telephone, and Telegraph. Government agency that provides telephone services. PTTs exist in most areas outside North America and provide both local and long-distance telephone services.
public switched telephone network	*See* PSTN.
pulse amplitude modulation	*See* PAM.
pulse code modulation	*See* PCM.
PVC	permanent virtual circuit. Connections that are assigned but not connected until data is sent, thereby not using bandwidth when idle. A virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and teardown in situations where certain virtual circuits must exist all the time. In ATM terminology, called a permanent virtual connection.
PVDM	packet voice digital signal processor module. Provides the ability to increase the voice processing capabilities within a single network module.
QoS	quality of service. (1) Measure of performance for a transmission system that reflects its transmission quality and service availability. (2) A set of tools used in networking devices to ensure best-of-class transmission quality and service availability.
QSIG	Q Signaling. An inter-PBX signaling protocol for networking PBX supplementary services in a multi- or single-vendor environment.

 Copyright © 2005, Cisco Systems, Inc.

Acronym or Term	Definition
Q Signaling	*See* QSIG.
quality of service	*See* QoS.
RAS	registration, admission, and status. Protocol that is used between endpoints and the gatekeeper to perform management functions. RAS signaling function performs registration, admissions, bandwidth changes, status, and disengage procedures between the VoIP gateway and the gatekeeper.
RBOCs	regional Bell operating companies. Seven regional telephone companies formed by the breakup of AT&T. RBOCs differ from regional Bell holding companies (RBHCs) in that RBOCs do not cross boundaries that were set out by the consent decree. Regional Bell operating company (RBOC) is a term describing one of the U.S. regional telephone companies (or their successors) that were created as a result of the breakup of American Telephone and Telegraph Company (AT&T, known also as the Bell System or “Ma Bell”) by a U.S. Federal Court consent decree on December 31, 1983. The seven original regional Bell operating companies were Ameritech, Bell Atlantic, BellSouth, NYNEX, Pacific Bell, Southwestern Bell, and US WEST. Each of these companies owned at least two Bell operating companies (BOCs). The BOCs were given the right to provide local phone service while AT&T was allowed to retain its long-distance service. The RBOCs and their constituent BOCs are part of the class of local exchange carriers (LECs). In addition to the RBOCs, there are more than 100 other franchised local telephone companies classed as local exchange carriers. Competitive local exchange carriers (CLECs) are additional companies allowed to compete with the LECs. These include AT&T, in some localities, and power companies. An interexchange carrier (IXC) is a long-distance carrier that carries traffic between LECs. Under the Telecommunications Act of 1996, RBOCs and LECs are allowed to compete for long-distance telephone traffic under certain circumstances. RBOCs are generally in competition for digital data and Internet traffic with wireless service providers and cable TV companies. RBOCs are gradually making available new telephone carrier technologies such as ISDN and DSL.
RBS	robbed-bit signaling. A technique by which a single bit in every DS0 bearer channel is "stolen" from every sixth frame. The stolen bit is then used to carry signaling information.
Real Time Streaming Protocol	*See* RTSP.
Real-Time Transport Protocol	*See* RTP.
recEive and transmit	*See* E&M.
redirect server	A server that accepts a SIP request, maps the address into zero or more new addresses, and returns these addresses to the client. It does not initiate its own SIP request nor does it accept calls.
reduced instruction set computing	*See* RISC.
regional Bell operating companies	*See* RBOCs.
registration, admission, and status	*See* RAS.
registration request	*See* RRQ.
Request For Comments	*See* RFC.
request notification	*See* RQNT.
Resource Reservation Protocol	*See* RSVP.

Acronym or Term	Definition
RFC	Request For Comments. Document series generated by the IETF and used as the primary means for communicating information about the Internet. Some RFCs are designated by the Internet Architecture Board (IAB) as Internet standards. Most RFCs document protocol specifications, such as Telnet and FTP, but some are humorous or historical. RFCs are available online from numerous sources.
RISC	reduced instruction set computing. A microprocessor design that provides fewer and simpler instructions burned into the silicon. Fewer instructions let the processor perform at a higher speed. The difference is made up by requiring more work to be done by compilers and greater memory usage.
robbed-bit signaling	*See* RBS.
round robin (n) round-robin (adj)	An algorithm used to schedule processes in a fixed cyclic order. Simply put, it means to "take turns."
RQNT	request notification. RAS message that instructs the gateway to watch for specific events.
RRQ	registration request. RAS message sent as a registration request.
RSVP	Resource Reservation Protocol. Protocol that supports the reservation of resources across an IP network. Applications running on IP end systems can use RSVP to indicate to other nodes the nature (bandwidth, jitter, maximum burst, and so on) of the packet streams they want to receive. Also known as Resource Reservation Setup Protocol.
RTCP	Real-Time Transport Control Protocol. Protocol that monitors the QoS of an IP RTP connection and conveys information about the ongoing session.
RTP	Real-Time Transport Protocol. Commonly used with IP networks. RTP is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP provides such services as payload type identification, sequence numbering, time stamping, and delivery monitoring to real-time applications.
Real-Time Transport Control Protocol	*See* RTCP.
RTSP	Real Time Streaming Protocol. Enables the controlled delivery of real-time data, such as audio and video. Sources of data can include both live data feeds, such as live audio and video, and stored content, such as pre-recorded events. RTSP is designed to work with established protocols, such as RTP and HTTP.
SAP	Session Announcement Protocol. A protocol used to assist in the advertisement of multicast multimedia conferences and other multicast sessions, and to communicate the relevant session setup information to prospective participants.
SCCP	(1) signaling connection control part. Software that provides an OSI network layer service to its users. It does not support intermediate routing. (2) Skinny Client Control Protocol. The Cisco standard for real-time calls and conferencing over IP.
SCP	service control point. An element of an SS7-based Intelligent Network that performs various service functions, such as number translation, call setup and teardown, and so on.
SDLC	Synchronous Data Link Control. IBM Systems Network Architecture (SNA) data-link-layer communications protocol. SDLC is a bit-oriented, full-duplex serial protocol that has spawned numerous similar protocols, including HDLC. *See also* HDLC.
SDP	Session Description Protocol. A protocol used to describe multimedia sessions in order to enable session announcement, session invitation, and other forms of multimedia session initiation.
serial tunnel	*See* STUN.
service control point	*See* SCP.

 Copyright © 2005, Cisco Systems, Inc.

Acronym or Term	Definition
service level agreement	*See* SLA.
service switching point	*See* SSP.
Session Announcement Protocol	*See* SAP.
Session Description Protocol	*See* SDP.
session initiation protocol	*See* SIP.
SF	Super Frame. Common framing type used on T1 circuits. SF consists of 12 frames of 193 bits each, with the 193rd bit providing framing synchronization. SF is superseded by ESF but is still widely used. Also called D4 framing. *See also* ESF.
signal ground	Refers to the common electrical reference point of a circuit.
signaling connection control part	*See* SCCP.
Signaling System 7	*See* SS7.
signal/noise ratio	*See* SNR.
signal transfer point	*See* STP.
SIMMs	single in-line memory modules. A small circuit board that holds a number of memory chips.
Simple Mail Transfer Protocol	*See* SMTP.
single in-line memory modules	*See* SIMMs.
SIP	session initiation protocol. Protocol developed by the IETF MMUSIC Working Group as an alternative to H.323. SIP features are compliant with IETF RFC 2543, published in March 1999. SIP equips platforms to signal the setup of voice and multimedia calls over IP networks.
Skinny Client Control Protocol	*See* SCCP.
SLA	service level agreement. An agreement between the ISP and the client that guarantees a certain level of data transmission over the network.
small office/home office	*See* SOHO.
SMDS	Switched Multimegabit Data Service. High-speed, packet-switched, datagram-based WAN networking technology offered by the telephone companies.
SMTP	Simple Mail Transfer Protocol. The standard Internet protocol providing e-mail services.
SNR	signal/noise ratio. A measure of transmission quality. The ratio of good or usable data (signal) to bad or undesired (noise) on a line, expressed in decibels (dB).
SOHO	small office/home office. Networking solutions and access technologies for offices that are not directly connected to large corporate networks.
spanning tree (n) spanning-tree (adj)	Loop-free subset of a network topology.
SQL	Structured Query Language. International standard language for defining and accessing relational databases.

Acronym or Term	Definition
SRST	Survivable Remote Site Telephony. 1. A feature of any VoIP network that provides backup in case of network component failures. 2. A feature on some Cisco routers that uses the Skinny protocol to provide call-handling support for the local IP Phones if the WAN connection to the Cisco CallManager fails.
SS7	Signaling System 7. Standard CCS system used with BISDN and ISDN. Developed by Bellcore. *See also* CCS.
SSP	service switching point. Element of an SS7-based Intelligent Network that performs call origination, termination, or tandem switching.
STP	signal transfer point. Element of an SS7-based Intelligent Network that performs routing of the SS7 signaling.
Structured Query Language	*See* SQL.
STUN	serial tunnel. Router feature allowing two SDLC- or HDLC-compliant devices to connect to one another through an arbitrary multiprotocol topology (using Cisco routers) rather than through a direct serial link.
Super Frame	*See* SF.
Survivable Remote Site Telephony	*See* SRST.
SVC	switched virtual circuit. Virtual circuit that is dynamically established on demand and is torn down when transmission is complete. SVCs are used in situations where data transmission is sporadic.
Switched Multimegabit Data Service	*See* SMDS.
switched virtual circuit	*See* SVC.
Synchronous Data Link Control	*See* SDLC.
T1/E1	T1: The standard digital multiplexed 24-channel voice/data digital span line. Used predominantly in North America. Operates at a data rate of 1.544 Mbps. Digital WAN carrier facility. T1 transmits DS-1 formatted data through the telephone-switching network, using AMI or B8ZS coding. *See also* AMI and B8ZS. E1: Wide-area digital transmission scheme used throughout the world that carries data at a rate of 2.048 Mbps. E1 lines can be leased for private use from common carriers.
tabletop	A conference telephone used on a conference room table.
TAPI	Telephony Application Programming Interface. A call control model developed by Microsoft and Intel.
TCAP	transaction capabilities application part. SS7 protocol layer that helps exchange noncircuit-related data between applications.
T-CCS	Transparent Common Channel Signaling. Feature that allows the connection of two PBXs with digital interfaces that use a proprietary or unsupported CCS protocol without the need for interpretation of CCS signaling for call processing. T1/E1 traffic is transported transparently through the data network, and the feature preserves proprietary signaling. From the PBX standpoint, this is accomplished through a point-to-point connection. Calls from the PBXs are not routed, but follow a preconfigured route to the destination.
TDM	time-division multiplexing. Technique in which information from multiple channels can be allocated bandwidth on a single wire based on preassigned timeslots. Bandwidth is allocated to each channel regardless of whether the station has data to transmit.
Telephony Application Programming Interface	*See* TAPI.

 Copyright © 2005, Cisco Systems, Inc.

Acronym or Term	Definition
time-division multiplexing	*See* TDM.
time stamp (n) time-stamp (v, adj)	A field in certain FastPacket formats that indicates the amount of time the packet has spent waiting in queues during the transmission between its source and destination nodes. Used to control the delay experienced by the packet.
transaction capabilities application part	*See* TCAP.
Transparent Common Channel Signaling	*See* T-CCS.
Triple Data Encryption Standard	*See* 3DES.
two-wire	One of two distinct types of audio interface (two-wire or four-wire). With the two-wire implementation, full-duplex audio signals are transmitted over a single pair, which consists of tip (T) and ring (R) leads.
UAC	user agent client. A client application that initiates the SIP request.
UAS	user agent server. A server application that contacts the user when a SIP request is received, and then returns a response on behalf of the user. The response accepts, rejects, or redirects the request.
UDP	User Datagram Protocol. Connectionless transport layer protocol in the TCP/IP protocol stack. UDP is a simple protocol that exchanges datagrams without acknowledgments or guaranteed delivery, requiring that error processing and retransmission be handled by other protocols. UDP is defined in RFC 768.
U interface	The ISDN interface between the telco and the user, also known as the local loop.
user agent client	*See* UAC.
user agent server	*See* UAS.
User Datagram Protocol	*See* UDP.
VAD	voice activity detection. Used to statistically save bandwidth by not sending packets in the absence of speech. When enabled on a voice port or a dial peer, silence is not transmitted over the network, only audible speech. When VAD is enabled, the sound quality is slightly degraded but the connection uses much less bandwidth.
variable bit rate	*See* VBR.
variable bit rate-nonreal time	*See* VBR-NRT.
variable bit rate real-time	*See* VBR-RT.
VBR	variable bit rate. QoS class defined by the ATM Forum for ATM networks. VBR is subdivided into an RT class and NRT class.
VBR-NRT	variable bit rate-nonreal time. Subclass of VBR. Used for connections in which there is no fixed timing relationship between samples but that still need a guaranteed QoS.
VBR-RT	variable bit rate-real time. Subclass of VBR. Used for connections in which there is a fixed timing relationship between samples.
V card	An electronic business card. V cards carry information such as name, telephone numbers, mail addresses, e-mail addresses, and URLs.
VIC	voice interface card. A Cisco interface card used to connect the system to either the PSTN or to a PBX. *See also* PBX *and* PSTN.

Acronym or Term	Definition
videoconference	A meeting between people in different locations, using audio and video. The simplest type of videoconference can involve transmission of static images between two locations; the most complex videoconferences can use full-motion video and high-quality audio between multiple locations.
video on demand	*See* VoD.
Virtual Private Network	*See* VPN.
VoATM	Voice over ATM. A technology that enables a router to carry voice traffic (for example, telephone calls and faxes) over an ATM network. When sending voice traffic over ATM, the voice traffic is encapsulated using a special AAL5 encapsulation for multiplexed voice.
VoD	video on demand. System using video compression to supply video programs to viewers when requested via ISDN or cable.
VoFR	Voice over Frame Relay. A technology that enables a router to carry voice traffic (for example, telephone calls and faxes) over a Frame Relay network. When sending voice traffic over Frame Relay, the voice traffic is segmented and encapsulated for transit across the Frame Relay network.
voice activity detection	*See* VAD.
voice interface card	*See* VIC.
Voice over ATM	*See* VoATM.
Voice over Frame Relay	*See* VoFR.
Voice over IP	*See* VoIP.
Voice over X	*See* VoX.
VoIP	Voice over IP. The capability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using a variety of signaling protocols.
VoIP over Frame Relay	*See* VoIPovFR.
VoIPovFR	VoIP over Frame Relay. Provides VoIP application interworking over an existing Frame Relay network. Can be used over point-to-point leased lines or a Frame Relay circuit; it does not require a full-fledged Frame Relay network or service.
VoX	Voice over X. Term that refers to nontraditional methods of carrying voice.
VPN	Virtual Private Network. Enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level.
WAN interface card	*See* WIC.
weighted fair queuing	*See* WFQ.
WFQ	weighted fair queuing. Congestion management algorithm that identifies conversations (in the form of traffic streams), separates packets that belong to each conversation, and ensures that capacity is shared fairly between these individual conversations. WFQ is an automatic way of stabilizing network behavior during congestion and results in increased performance and reduced retransmission.
WIC	WAN interface card. A Cisco interface card that connects the system to the WAN link service provider.

 Copyright © 2005, Cisco Systems, Inc.

Acronym or Term	Definition
Wink Start	A method of E&M signaling. When the signaling leads indicate a change to an off-hook state, the other side must send a momentary *wink* (on-hook to off-hook to on-hook transition) on the correct signaling lead before the call signaling information can be sent by the sending side. After the call signaling information is received, the side that sent the wink goes off hook again when the subscriber answers and stays that way for the duration of the call.

Cisco Systems
Networking Academy

Reference Lists

Cisco Networking Academy Program
IP Telephone v1.0

Table of Content

REFERENCE LISTS 1

General 3
Introduction to Packet Voice Technologies 3
Introduction to VoIP 4
Configuring Cisco CallManager Express (CME) 5
Voice Dial Plans, Configuring Voice Interfaces and Dial Peers 7
Configuring CME Additional Features 9
VoIP Signaling and Call Control 10
Improving and Maintaining Voice Quality 11

 Copyright © 2005, Cisco Systems, Inc.

General

For additional information on this module, refer to the resources listed below.

- *Cisco IP Communications Express: CallManager Express with Cisco Unity Express.* Indianapolis, Indiana: Cisco Press; ISBN: 158705180X; 2005.

Introduction to Packet Voice Technologies

For additional information on this module, refer to the resources listed below.

Traditional Telephony

- *Voice Network Signaling and Control*
  http://www.cisco.com/warp/public/788/signalling/net_signal_control.html

Packetized Telephony Networks

- *Extending Enterprise Productivity with Converged IP-Based Cisco Solutions*
  http://www.cisco.com/warp/public/cc/so/neso/vvda/avvid/avid_pl.htm

IP Telephony Applications

- *Design Guides*
  http://www.cisco.com/en/US/netsol/ns340/ns394/ns147/ns17/networking_solutions_design_guidances_list.html

Analog Voice Basics & Analog-to-Digital Voice Encoding

- McQuerry, S., McGrew, K., Foy, S. *Cisco Voice over Frame Relay, ATM, and IP.* Indianapolis, Indiana: Cisco Press; ISBN: 1578702275; 2001.

Signaling Systems

- *Voice Network Signaling and Control|*
  http://www.cisco.com/warp/public/788/signalling/net_signal_control.html

Copyright © 2005, Cisco Systems, Inc.

Introduction to VoIP

For additional information on this module, refer to the resources listed below.

Gateways and Their Roles

- *Cisco 1700 Series Modular Access Routers, Product Bulletin, No. 1596*
  http://www.cisco.com/en/US/products/hw/routers/ps221/prod_bulletin09186a00800920de.html

Encapsulating Voice in IP Packets

- *Request for Comments*
  http://www.faqs.org/rfcs/
- *Configuring Compressed Real-Time Protocol*
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos_c/qcpart6/qcrtphc.htm

Calculating Bandwidth Requirements

- *Voice over IP – Per Call Bandwidth Consumption*
  http://www.cisco.com/warp/public/788/pkt-voice-general/bwidth_consume.html
- *Voice over IP (VoIP)*
  http://www.cisco.com/en/US/tech/tk652/tk701/tsd_technology_support_protocol_home.html
- *Voice over Frame Relay (VoFR*)
  http://www.cisco.com/en/US/tech/tk652/tk692/tsd_technology_support_protocol_home.html
- *Voice over ATM (VoATM)*
  http://www.cisco.com/en/US/tech/tk652/tk690/tsd_technology_support_protocol_home.html

 Copyright © 2005, Cisco Systems, Inc.

Configuring Cisco CallManager Express (CME)

For additional information on this module, refer to the resources listed below.

Overview of Cisco CME

- *Cisco CallManager Express with Cisco Unity Express Solution White Paper*
  http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_white_paper09186a00801c637f.shtml

Challenges and Solutions in VoIP

- *Voice over IP – Per Call Bandwidth Consumption*
  http://www.cisco.com/warp/public/788/pkt-voice-general/bwidth_consume.html#related
- *Voice Quality*
  http://www.cisco.com/en/US/tech/tk652/tk698/tsd_technology_support_protocol_home.html
- *Quality of Service for Voice over IP*
  http://www.cisco.com/en/US/tech/tk652/tk698/technologies_white_paper09186a00800d6b73.shtml

Cisco CME Features and Functionality

- *CallManager Express 3.1 System Administrators Guide*
  http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_administration_guide_book09186a0080380ccc.html
- *Cisco CallManager Express Data Sheet*
  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns331/c643/cdccont_0900aecd8026b194.pdf

Cisco CME Network Parameters

- *Configuring DHCP*
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfdhcp.htm#xtocid0
- *Setting Time and Calendar Services*
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/ffun_c/fcfprt3/fcf012.htm#1001075
- *Cisco CallManager Express 3.1: Setting Up a Cisco CME System*
  http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_administration_guide_chapter09186a00801f12c1.html
- *The Network Time Protocol*
  http://ntp.org

Copyright © 2005, Cisco Systems, Inc.

IP Phone Registration

- *Cisco CallManager Express Data Sheet*
  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns331/c643/cdccont_0900aecd8026b194.pdf

Ephone-dn and Ephone

- *Cisco CallManager Express 3.1: Overview*
  http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_administration_guide_chapter09186a00801f12ab.html

Cisco CME Files

- *Cisco CallManager Express Data Sheet*
  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns331/c643/cdccont_0900aecd8026b194.pdf
- *Cisco CME software* (A user ID and password are required to access this site.)
  http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml

Initial Phone Setup

- *Cisco CallManager Express Data Sheet*
  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns331/c643/cdccont_0900aecd8026b194.pdf

 Copyright © 2005, Cisco Systems, Inc.

Voice Dial Plans, Configuring Voice Interfaces and Dial Peers

For additional information on this module, refer to the resources listed below.

Call Establishment Principles

- *Understanding Inbound and Outbound Dial Peers on Cisco IOS Platforms*
  http://www.cisco.com/warp/public/788/voip/in_out_dial_peers.html

Configuring Dial Peers

- *Dial Peer Overview*
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax_c/vvfpeers.htm#xtocid2
- *Case Study: Understanding Inbound Matching and Default Dial-Peer 0*
  http://www.cisco.com/warp/public/788/voip/in_dial_peer_match.html#topic13
- *Voice—Understanding Inbound and Outbound Dial Peers on Cisco IOS Platforms*
  http://www.cisco.com/warp/public/788/voip/in_out_dial_peers.html
- *Cisco IOS Voice, Video, and Fax Command Reference, Release 12.2*
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax_r/
- *Cisco IP Telephony*, Cisco Press; ISBN: 1587050501; 1st edition (December 17, 2001)

Specific-Purpose Connections

- *Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*
  (A user ID and password are required to access this site.)
  http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080080ada.html

Building a Scalable Numbering Plan

- *Designing a Static Dial Plan*
  http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/dp3_isd.htm
- *Understanding One Stage and Two Stage Voice Dialing*
  http://www.cisco.com/warp/public/788/voip/1stage2stage.html
- *Voice Design and Implementation Guide*
  http://www.cisco.com/warp/public/788/pkt-voice-general/8.html

Copyright © 2005, Cisco Systems, Inc.

Configuring Voice Ports

- *Configuring Voice Ports*
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/voice_c/vcprt1/vcports.htm
- *Configuring and Troubleshooting Transparent CCS*
  http://www.cisco.com/warp/public/788/voip/trans_channel_signal.html
- *Configuring Voice Ports*
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax_c/vvfport.htm

Adjusting Voice Quality

- *Voice Quality Tuning Commands*
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fvvfax_c/vvfport.htm#wp1161013

Dial Peer

- *Understanding Inbound and Outbound Dial Peers on Cisco IOS Platform*
  (A user ID and password are required to access this site.)
  http://cisco.com/en/US/partner/tech/tk652/tk90/technologies_tech_note09186a0080147524.shtml

Class of Restriction

- *Configuring Class of Restriction*
  http://cisco.com/en/US/partner/tech/tk652/tk90/technologies_configuration_example09186a008019d649.shtml

 Copyright © 2005, Cisco Systems, Inc.

Configuring CME Additional Features

For additional information on this module, refer to the resources listed below.

Cisco CME GUI Features & Configuring Phone Features

- *Cisco CallManager Express 3.1: Overview*
  http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_administration_guide_chapter09186a00801f12ab.html

VoIP Signaling and Call Control

For additional information on this module, refer to the resources listed below.

Need for Signaling and Call Control

- *ITU-T Recommendation H.323*
  http://www.itu.int/rec/recommendation.asp?type=folders&lang=e&parent=T-REC-H.323
- IETF RFC 3261, *SIP: Session Initiation Protocol*
  http://www.faqs.org/rfcs/rfc3261.html
- IETF RFC 2705: *Media Gateway Control Protocol (MGCP), version 1.0*
  http://www.faqs.org/rfcs/rfc2705.html

Configuring H.323

- *ITU-T Recommendation H.323 (Version 4)*
  http://www.itu.int/rec/recommendation.asp?type=items&lang=E&parent=T-REC-H.323-200011-S
- *Cisco IOS Voice, Video, and Fax Configuration Guide*
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080080ada.html
- *Cisco IOS Voice, Video, and Fax Command Reference*
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a0080080c8b.html

Configuring MGCP

- IETF RFC 2705: *Media Gateway Control Protocol (MGCP), version 1.0*
  http://www.faqs.org/rfcs/rfc2705.html
- IETF RFC 2805: *Media Gateway Control Protocol Architecture and Requirements*
  http://www.faqs.org/rfcs/rfc2805.html
- *Cisco IOS Voice, Video, and Fax Configuration Guide*
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_book09186a0080080ada.html
- *Cisco IOS Voice, Video, and Fax Command Reference*
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a0080080c8b.html
- *Configuring MGCP Gateway and FXO/FXS Ports on a Cisco CallManager Server*
  http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_tech_note09186a008017825e.shtml

 Copyright © 2005, Cisco Systems, Inc.

Improving and Maintaining Voice Quality

For additional information on this module, refer to the resources listed below.

IP QoS Mechanisms

- *Quality of Service (QoS)*
  http://www.cisco.com/en/US/tech/tk543/tsd_technology_support_category_home.html
- *Implementing Quality of Service Policies with DSCP*
  http://www.cisco.com/en/US/tech/tk543/tk757/technologies_tech_note09186a00800949f2.shtml

Implementing AutoQoS

- Cisco AutoQoS Whitepaper
  http://www.cisco.com/en/US/tech/tk543/tk759/technologies_white_paper09186a00801348bc.shtml
- Configuring Automatic QoS
  http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a0080121d11.html#1032637
- AutoQos – VoIP
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080153ece.html#73342

Comparing Voice Quality Measurement Standards

- PESQ information
  http://www.pesq.org
- Cisco PESQ article
  Robison, Helen M. *Designing Voice Quality in Hybrid TDM-IP Networks*
  http://www.cisco.com/en/US/about/ac123/ac114/ac173/ac225/about_cisco_packet_technology0900aecd800c9140.html

VoIP Challenges

- *Understanding Jitter in Packet Voice Networks (Cisco IOS Platforms)*
  http://www.cisco.com/warp/public/788/voice-qos/jitter_packet_voice.html
- *Understanding Delay in Packet Voice Networks*
  http://www.cisco.com/warp/public/788/voip/delay-details.html
- *Quality of Services (QoS)*
  http://www.cisco.com/en/US/tech/tk543/tsd_technology_support_category_home.html

Copyright © 2005, Cisco Systems, Inc.

QoS and Good Design

- *Voice Quality*
  http://www.cisco.com/en/US/tech/tk652/tk698/tsd_technology_support_protocol_home.html

Jitter

- *Playout Delay Enhancements for Voice Over IP*
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t5/dt_pod.htm
- *Understanding Jitter in Packet Voice Networks (Cisco IOS Platforms)*
  http://www.cisco.com/warp/public/788/voice-qos/jitter_packet_voice.html

Delay

- *Understanding Delay in Packet Voice Networks*
  http://www.cisco.com/warp/public/788/voip/delay-details.html#60

Apply QoS in the Campus

- *Cisco AVVID Network Infrastructure Enterprise Quality of Service Design*
  http://www.cisco.com/application/pdf/en/us/guest/netsol/ns17/c649/ccmigration_09186a00800d67ed.pdf

QoS Tools in the WAN

- *Voice over IP (VoIP) Frame Relay (VoFR) and ATM (VoATM)*
  http://www.cisco.com/en/US/tech/tk652/tsd_technology_support_category_home.html

Configuring QoS in the WAN

- *Voice Technologies*
  http://www.cisco.com/en/US/tech/tk652/tsd_technology_support_category_home.html

Configuring CAC

- *Resource-Based CAC Mechanisms*
  http://www.cisco.com/univercd/cc/td/doc/cisintwk/intsolns/voipsol/cac.htm#903253
- *Call Admission Control for H.323 Gateways*
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00800e0d4b.html#76206
- *Call Admission Control for MGCP*
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087d37.html#1048015
- *Measurement-Based Call Admission Control for SIP*
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00801541b2.html

 Copyright © 2005, Cisco Systems, Inc.