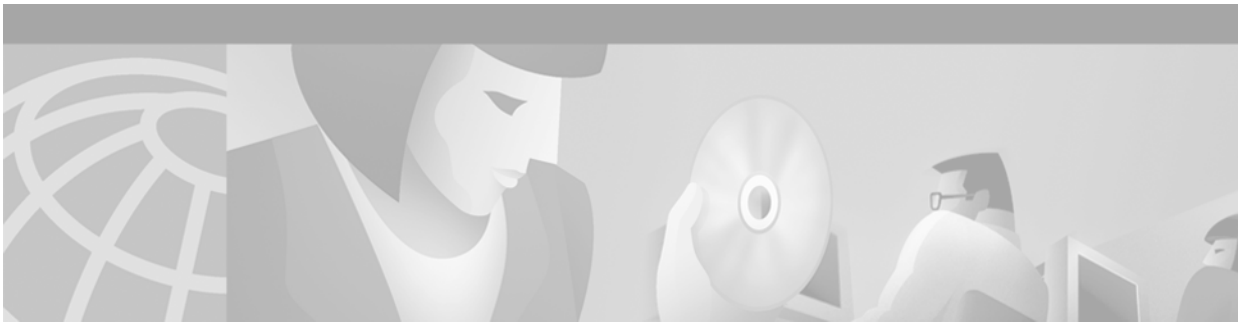

Voice, Video, and Fax Overview

The *Cisco IOS Voice, Video, and Fax Configuration Guide* shows you how to configure your Cisco router or access server to support voice, video, and fax applications. This chapter is an overview of some of the concepts and technologies described in the guide.

Configuration Guide Overview

The *Cisco IOS Voice, Video, and Fax Configuration Guide* is the result of reorganizing and renaming the *Cisco IOS Multiservice Applications Configuration Guide*. The reorganized publication is divided into the following parts:

- Basic Voice Configuration
- H.323 Support and Other VoIP Call Control Signaling Protocols
- Voice over Layer 2 Protocols
- Telephony Applications
- Trunk Management and Conditioning Features
- Fax, Video, and Modem Support

Each part contains one or more chapters that describe configuration procedures for each respective technology. The following sections describe some of the chapter contents for this configuration guide.

Dial Peers

Dial peers describe the entities to or from which a call is established and the key to understanding the Cisco voice implementation. All voice technologies use dial peers to define the characteristics associated with a call leg. A call leg is a discrete segment of a call connection that lies between two points in the connection. An end-to-end call comprises four call legs, two from the perspective of the source route, and two from the perspective of the destination route.

You use dial peers to apply specific attributes to call legs and to identify call origin and destination. Attributes applied to a call leg include specific quality of service (QoS) features (such as IP RTP Priority and IP Precedence), compression/decompression (codec), voice activity detection (VAD), and fax rate.

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

- Plain old telephone service (POTS)—Dial peer describing the characteristics of a traditional telephony network connection. POTS peers point to a particular voice port on a voice network device.

  When you configure POTS dial peers, the key commands that you must be configure are the **port** and **destination-pattern** commands. The **destination-pattern** command defines the telephone number associated with the POTS dial peer. The **port** command associates the POTS dial peer with a specific logical dial interface, normally the voice port connecting the Cisco device to the local POTS network.

  Specific applications, such as interactive voice response (IVR), are configured on the POTS dial peer as well.

- Voice network (VoIP, VoATM, and VoFR)—Dial peer describing the characteristics of a packet network connection; in the case of VoIP, for example, it is an IP network. Voice-network peers point to specific voice-network devices.

  When you configure voice-network dial peers, the key commands that you must configure are the **destination-pattern** and **session-target** commands. The **destination-pattern** command defines the telephone number associated with the voice-network dial peer. The **session-target** command specifies a destination address for the voice-network peer.

Other applications (such as store-and-forward fax, which uses the infrastructure of VoIP but is not strictly a voice technology) also use dial peers to assign attributes to call legs.

Voice Ports

Voice port commands define the characteristics associated with a particular voice-port signaling type. The Cisco implementation of voice supports both analog and digital telephony connections. The connection supported (and the associated signaling) depends on the type of voice network module (VNM) or voice feature card (VFC) installed in your Cisco router or access server.

Voice ports provide support for three basic analog voice signaling formats:

- FXO—Foreign Exchange Office interface. The FXO interface is an RJ-11 connector that allows a connection to be directed at the Public Switched Telephone Network (PSTN) central office (CO) (or to a standard PBX interface, if the local telecommunications authority permits). This interface is of value for off-premises extension applications.
- FXS—Foreign Exchange Station interface. The FXS interface is an RJ-11 connector that allows connection for basic telephone equipment, keysets, and PBXs; FXS connections supply ring, voltage, and dial tone.
- E&M—Ear and mouth (or recEive and transMit) interface. The E&M interface is an RJ-48 connector that allows connection for PBX trunk lines (tie lines). It is a signaling technique for 2-wire and 4-wire telephone and trunk interfaces.

  The Cisco MC3810 multiservice concentrator also supports E&M Mercury Exchange Limited channel-associated signaling (MEL CAS), which is used primarily in the United Kingdom.

Depending on the Cisco device you are configuring, the following digital signaling is supported:

- ISDN PRI
- ISDN BRI

- E1 R2
- T1 CAS

The voice port syntax depends on the hardware platform on which it is being configured.

Voice Technologies

Cisco IOS Release 12.2 offers the following voice and voice-related technologies:

- VoIP
- Voice over Frame Relay (VoFR)
- Voice over ATM (VoATM)
- H.323 gateways
- Media Gateway Control Protocol (MGCP) and related protocols
- Session Initiation Protocol (SIP)
- Tool Command Language (TCL) and interactive voice response (IVR)
- Multimedia Conference Manager
- Fax gateways
- Video

Voice over IP

Cisco offers VoIP that uses IP to carry voice traffic. Because voice traffic is being transported via IP, you need to configure signaling parameters as part of the voice-port configuration in addition to feature-specific elements such as dial peers. VoIP is compliant with International Telecommunications Union-Telecommunications (ITU-T) specifications H.323 and Cisco's H.323 Version 2.

VoIP can be used to provide the following:

- A central-site telephony termination facility for VoIP traffic from multiple voice-equipped remote office facilities.
- A PSTN gateway for Internet telephone traffic. VoIP used as a PSTN gateway leverages the standardized use of H.323-based Internet telephone client applications. In the case of a device with extensive capacity running VoIP (such as the Cisco AS5800 universal access server), it provides the functionality of a carrier class switch.

VoIP enables Cisco routers and access servers to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the digital signal processor (DSP) segments the voice signal into frames that are then coupled in groups of two and stored in voice packets. The voice packets are transported using IP in compliance with ITU-T specification H.323. Because VoIP is a delay-sensitive application, you must have a well-engineered network end-to-end to use VoIP successfully. Fine-tuning your network to adequately support VoIP involves a series of protocols and features geared toward QoS. Traffic shaping considerations must be taken into account to ensure the reliability of the voice connection.

Voice over Frame Relay

VoFR uses Frame Relay to transport voice traffic. Because VoFR is transporting signals over Layer 2, you must configure timing parameters in addition to feature-specific elements such as dial peers and voice ports. VoFR is compliant with FRF.11 and FRF.12 specifications.

VoFR enables a Cisco device to carry voice traffic (for example, telephone calls and faxes) over a Frame Relay network. When voice traffic is sent over Frame Relay, the voice traffic is segmented and encapsulated for transit across the Frame Relay network. The segmentation engine uses FRF.12 fragmentation. FRF.12 (also known as FRF.11 Annex C) allows long data frames to be fragmented into smaller pieces and interleaved with real-time frames. In this way, real-time voice and nonreal-time data frames can be carried together on lower speed links without causing excessive delay to the real-time traffic.

The segmentation size configured must match the line rate or port access rate. To ensure a stable voice connection, you must configure the same data segmentation size on both sides of the voice connection. When voice segmentation is configured, all priority queueing, custom queueing, and weighted fair queueing are disabled on the interface.

When you configure voice and data traffic over the same Frame Relay data-link connection identifier (DLCI), you must take traffic-shaping considerations into account to ensure the reliability of the voice connection.

Cisco VoFR implementation supports the following types of VoFR calls:

- Static FRF.11 trunks
- Switched VoFR calls:
  - Dynamic switched calls
  - Cisco trunk (private line) calls

Voice over ATM

VoATM uses ATM adaptation layer 5 (AAL5) to route voice traffic. Because VoATM is transporting signals over Layer 2, you must configure timing parameters in addition to feature-specific elements such as dial peers and voice ports.

VoATM enables a Cisco MC3810 multiservice concentrator to carry voice traffic (for example, telephone calls and faxes) over an ATM network. The Cisco MC3810 multiservice concentrator supports compressed VoATM on ATM port 0 only.

When voice traffic is sent over ATM, the voice traffic is encapsulated using a special AAL5 encapsulation for multiplexed voice. The ATM permanent virtual circuit (PVC) must be configured to support real-time voice traffic, and the AAL5 voice encapsulation must be assigned to the PVC. The PVC must also be configured to support variable bit rate (VBR) for real-time networks for traffic shaping between voice and data PVCs.

Traffic shaping is necessary so that the carrier does not discard the incoming calls from the Cisco MC3810 multiservice concentrator. To configure voice and data traffic shaping, you must configure the peak, average, and burst options for voice traffic. Configure the burst value if the PVC will be carrying bursty traffic. The peak, average, and burst values are needed so the PVC can effectively handle the bandwidth for the expected number of voice calls.

H.323 Gateways

The H.323 standard provides for sending audio, video, and data conferencing data on an IP-based internetwork. The Cisco functionality enables gateway H.323 terminals to communicate with terminals running other protocols. Gateways provide protocol conversion between terminals running different types of protocols. Gatekeepers are optional nodes that manage other nodes in an H.323 network. Gateways communicate with gatekeepers using the registration, admission, and status (RAS) protocol. The gatekeeper maintains resource computing information, which it uses to select the appropriate gateway during the admission of a call.

Cisco software complies with the mandatory requirements and several of the optional features of the H.323 Version 2 specification. Cisco H.323 Version 2 software enables gatekeepers, gateways, and proxies to send and receive all the required fields in H.323 Version 2 messages. Cisco H.323 Version 2 features include the following:

- Lightweight registration
- Improved gateway selection process
- Gateway resource availability reporting
- Support for single proxy configurations
- Tunneling of redirecting number information element
- H.245 tunneling
- Hookflash relay
- H.235 security
- Codec negotiation
- H.245 empty capabilities set

Media Gateway Control Protocol

Media Gateway Control Protocol (MGCP) defines the call control relationship between VoIP gateways that translate audio signals to and from the packet network and call agents (CAs). The CAs are responsible for processing the calls. The MGCP gateways interact with a CA, also called a Media Gateway Controller (MGC) that performs signal and call processing on gateway calls. In the MGCP configurations supported by Cisco, the gateway can be a Cisco router, access server, or cable modem, and the CA is a third-party server.

Session Initiation Protocol

Session Initiation Protocol (SIP) is an alternative protocol developed by the Internet Engineering Task Force (IETF) for multimedia conferencing over IP. SIP features are compliant with IETF RFC 2543, *SIP: Session Initiation Protocol*, published in March 1999.

The Cisco SIP functionality enables Cisco access platforms to signal the setup of voice and multimedia calls over IP networks. The SIP feature also provides nonproprietary advantages in the following areas:

- Protocol extensibility
- System scalability
- Personal mobility services
- Interoperability with different vendors

SIP is an ASCII-based, application-layer control protocol that can be used to establish, maintain, and terminate calls between two or more endpoints.

Like other VoIP protocols, SIP is designed to address the functions of signaling and session management within a packet telephony network. Signaling allows call information to be carried across network boundaries. Session management provides the ability to control the attributes of an end-to-end call.

SIP provides the following capabilities:

- Determining the location of the target endpoint—SIP supports address resolution, name mapping, and call redirection.
- Determining the media capabilities of the target endpoint—Through Session Description Protocol (SDP), SIP determines the lowest level of common services between the endpoints. Conferences are established using only the media capabilities that can be supported by all endpoints.
- Determining the availability of the target endpoint—If a call cannot be completed because the target endpoint is unavailable, SIP determines whether the called party is connected to a call already or did not answer in the allotted number of rings. SIP then returns a message indicating why the target endpoint was unavailable.
- Establishing a session between the originating and target endpoints—If the call can be completed, SIP establishes a session between the endpoints. SIP also supports midcall changes, such as the addition of another endpoint to the conference or the changing of a media characteristic or codec.
- Handling the transfer and termination of calls—SIP supports the transfer of calls from one endpoint to another. During a call transfer, SIP simply establishes a session between the transferee and a new endpoint (specified by the transferring party) and terminates the session between the transferee and the transferring party. At the end of a call, SIP terminates the sessions among all parties.

Interactive Voice Response

IVR consists of simple voice prompting and digit collection to gather caller information for authenticating the user and identifying the destination. IVR applications can be assigned to specific ports or invoked on the basis of Dialed Number Identification Service (DNIS). An IP public switched telephone network gateway can have several IVR applications to accommodate many different gateway services, and you can customize the IVR applications to present different interfaces to the various callers.

IVR systems 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 dual tone multifrequency (DTMF) signaling. For example, when a user makes a call with a debit card, an IVR application is used to prompt the caller to enter a specific type of information, such as an account number. After playing the voice prompt, the IVR application collects the predetermined number of touch tones and then places the call to the destination phone or system.

IVR uses TCL scripts to gather information and to process accounting and billing. For example, a TCL IVR script plays when a caller receives a voice-prompt instruction to enter a specific type of information, such as a personal identification number (PIN). After playing the voice prompt, the TCL IVR application collects the predetermined number of touch tones and sends the collected information to an external server for user authentication and authorization.

Since the introduction of the Cisco IVR technology, the software has undergone several enhancements. Cisco TCL IVR Version 2.0 is made up of separate components that are described individually in the sections that follow. The enhancements are as follows:

- MGCP scripting package implementation
- Real Time Streaming Protocol (RTSP) client implementation

- TCL IVR prompt playout and digit collection on IP call legs
- New TCL verbs to use RTSP and MGCP scripting features

The enhancements add scalability and enable the TCL IVR scripting functionality on VoIP legs. In addition, support for RTSP enables VoIP gateways to play messages from RTSP-compliant announcement servers. The addition of these enhancements also reduces the CPU load and saves memory on the gateway because no packetization is involved. Larger prompts can be played, and the use of an external audio server is allowed.

Multimedia Conference Manager

The Multimedia Conference Manager provides both gatekeeper and proxy capabilities, which are required for service provisioning and management of H.323 networks. With Multimedia Conference Manager you can configure your current internetwork to route bit-intensive data such as audio, telephony, video and audio telephony, and data conferencing using existing telephone and ISDN links, without degrading the current level of service in the network. In addition, you can implement H.323-compliant applications on existing networks in an incremental fashion without upgrades.

With Multimedia Conference Manager, you can provide the following services:

- Identification of H.323 traffic and application of appropriate policies
- Limiting of H.323 traffic on LANs and WANs
- User accounting for records based on service utilization
- Insertion of QoS for the H.323 traffic generated by applications such as VoIP, data conferencing, and video conferencing
- Implementation of security for H.323 communications

Video

Cisco 2600 series, 3600 series, and 7200 series routers and the Cisco MC3810 multiservice concentrator support the H.323 gatekeeper (sometimes referred to as Multimedia Conference Manager) with voice gateway image with Resource Reservation Protocol (RSVP) to ATM SVC mapping. This feature delivers H.323 gatekeeper, proxy, and voice gateway solutions with routing as a single Cisco IOS image. In addition, it enables H.323 RSVP reservations to be mapped to ATM non-real-time variable bit rate (nRTVBR) SVCs to guarantee quality of service (QoS) for video applications over ATM backbones.

Cisco supports video traffic within a data stream in three ways:

- Video in pass-through mode—Using this method, video traffic received from a video codec connected to a universal I/O serial port can be transported on a dedicated time slot between systems using the time-division multiplexing (TDM) functionality of the T1/E1 trunk.
- Video over ATM AAL1—A serial stream from a video codec connected to a serial port can be converted to ATM and transported across an ATM network using AAL1 circuit emulation service (CES) encapsulation.
- Video over ATM PVCs and switched virtual circuits (SVCs)—A serial stream from a video codec connected to a Cisco MC3810 multiservice concentrator using the plug-in Video Dialing Module (VDM) can be converted to ATM and transported across an ATM network using AAL1 CES.

Fax Gateways

Fax applications enable Cisco AS5300 universal access servers to send and receive faxes across packet-based networks using modems or VFCs. Some of the benefits of the fax gateway are as follows:

- Universal inbox for fax and e-mail—Faxes and e-mails can go to the same mailbox using DID numbers. E-mail and fax recipients can be combined.
- Toll bypass—In an enterprise environment in which offices in different cities are connected using a WAN, toll charges can be bypassed by transmitting faxes over the network connection. Because a fax message is stored on the mail server until Simple Mail Transfer Protocol (SMTP) forwards messages to the recipient, SMTP can forward fax e-mail attachments during off-peak hours (for example, during evenings and weekends), thereby reducing long-distance charges.
- Broadcast to multiple recipients—E-mail fax attachments can be sent to multiple recipients simultaneously.
- Improve robustness—The Fax Relay Packet Loss Concealment feature improves the robustness of the facsimile relay. It eliminates fax failures and lost data caused by excessive page errors. Field diagnostics and troubleshooting capabilities are improved by available debug commands. Statistics give better visibility into the real-time fax operation in the gateway, allowing for improved field diagnostics and troubleshooting.
- Cost savings and port density using T.37/T.38 Fax Gateway—The cost of maintaining one architecture (either fax or voice) is eliminated. Service providers can do the following:
  - Use a single port for voice, fax relay, and store-and-forward fax. For smaller points of presence (POPs), the single-port configuration for these technologies is even more significant because mixed traffic can be handled more efficiently, requiring only a single pool of ports versus splitting traffic across two pools.
  - Offer the new service of a single number for subscriber voice and fax access. The applications that use a single number for voice and fax require only half as many DNIS numbers and dial peers as would be required with separate voice and fax applications.
  - Offer applications that require toggling from voice to fax. Applications such as never-busy fax service can be addressed once the gateway can dynamically switch from fax relay to fax store and forward.
- Interoperability with T.37 fax relay for VoIP H.323—The Cisco 2600 and 3600 series routers and Cisco MC3810 multiservice concentrator gateways with ITU-T T.38 fax relay capability can interoperate with third-party gateways and gatekeepers over an IP H.323 network. The goal is to work with third-party gateways and gatekeepers to provide ITU-T standards-based T.38 fax relay services for multivendor networks.

The Cisco 2600 and 3600 series routers and Cisco MC3810 multiservice concentrator gateways provide standards-based toll bypass for fax and voice calls. In addition to existing voice and fax toll bypass capabilities, the multiservice gateways provide toll bypass for fax relay with the standards-based ITU-T T.38 fax relay implementation.