CISCO SYSTEMS

MIX-Multichannel T1/E1 Port Adapter Installation and Configuration

Product Numbers: PA-MCX-2TE1(=), PA-MCX-4TE1(=), PA-MCX-8TE1(=)
Platform Supported: Cisco 7200 VXR

CONTENTS

MIX-Multichannel T1/E1 Port Adapter Installation and Configuration ■

MIX-Multichannel T1/E1 Port Adapter Installation and Configuration

Preface

This preface describes the objectives and organization of this document and explains how to find additional information on related products and services. This preface contains the following sections:

Objectives

This document describes how to install and configure the two-port MIX-Multichannel T1/E1 port adapter (PA-MCX-2TE1[=]), the four-port MIX-Multichannel T1/E1 port adapter (PA-MCX-4TE1[=]), and the eight-port MIX-Multichannel T1/E1 port adapter (PA-MCX-8TE1[=]), hereafter referred to as the PA-MCX port adapters. These port adapters are used in the Cisco 7200 VXR routers, which consist of the four-slot Cisco 7204VXR and the six-slot Cisco 7206VXR.

Organization

This document contains the following chapters:

Section	Title	Description
Chapter 1	Overview	Describes the PA-MCX port adapters, and their LED displays, cables, and receptacles.
Chapter 2	Preparing for Installation	Describes safety considerations, tools required, and procedures you should perform before the actual installation.
Chapter 3	Removing and Installing Port Adapters	Describes the procedures for installing and removing PA-MCX port adapters in the supported platform.
Chapter 4	Configuring the PA-MCX	Provides instructions for configuring the PA-MCX port adapters on the supported platform.

Related Documentation

Your router or switch and the Cisco IOS software running on it contain extensive features and functionality, which are documented in the following resources:

- Cisco IOS software:

  For configuration information and support, refer to the modular configuration and modular command reference publications in the Cisco IOS software configuration documentation set that corresponds to the software release installed on your Cisco hardware.

- Cisco 7200 VXR routers:

  For hardware installation and maintenance information, refer to the *Cisco 7200 VXR Installation and Configuration Guide*.

- For international agency compliance, safety, and statutory information for WAN interfaces:

  – *Site Preparation and Safety Guide*

  – *Regulatory Compliance and Safety Information for the Cisco 7200 Series Routers*

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

    http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit e-mail comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

The Cisco TAC website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year. The Cisco TAC website is located at this URL:

http://www.cisco.com/tac

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

http://tools.cisco.com/RPF/register/register.do

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

http://www.cisco.com/tac/caseopen

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete listing of Cisco TAC contacts, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—Your network is "down" or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Priority 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Priority 3 (P3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/index.html

C H A P T E R

1

Overview

This chapter describes the PA-MCX port adapters and contains the following sections:

Port Adapter Overview

The PA-MCX port adapters (see Figure 1-1, Figure 1-2, and Figure 1-3) are multichannel port adapters that provide T1/E1 connectivity for data and voice traffic. The PA-MCX ports can be configured either as DS1/PRI ports for data traffic, or as packet voice ports that, when used in conjunction with a digital voice port adapter, allow Cisco 7200 VXR routers to become dedicated packet voice hubs or packet voice gateways that connect to both private branch exchanges (PBXs) and the Public Switched Telephone Network (PSTN). This allows packet voice and packet fax calls to be placed over the WAN and sent through the gateway into the traditional circuit-switched voice infrastructure.

Figure 1-1   PA-MCX-2TE1 Port Adapter
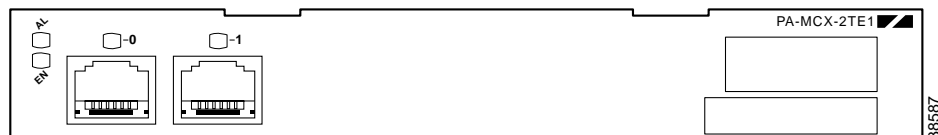
Figure 1-2   PA-MCX-4TE1 Port Adapter
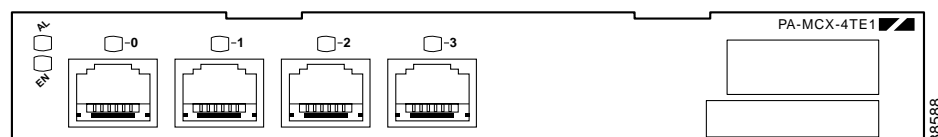
Figure 1-3   PA-MCX-8TE1 Port Adapter
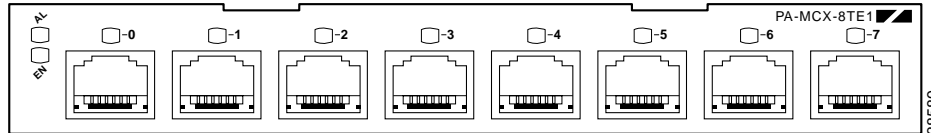
Channelized T1/E1 Overview

When you are running channelized data, each DS1 interface can provide up to 24 T1 channel groups if your PA-MCX is configured for T1, or 31 E1 channel groups if your PA-MCX is configured for E1. The T1 groups are numbered from 0 to 23 and the E1 groups are numbered from 0 to 30. Each T1 channel group provides up to twenty-four 64-kbps time slots (DS0 channels), which are numbered 1 to 24. Each E1 channel group provides up to thirty-one 64-kbps time slots (E1 channels), which are numbered 1 to 31. Multiple time slots can be mapped to a single channel group. Each channel group is presented to the system as a serial interface that can be configured individually. Usable bandwidth for each channel group is calculated as n x 56 kbps or n x 64 kbps, where n is a number of DS0 time slots (1 to 24) or E1 channels (1 to 31).

When you are running ISDN PRI, each T1 interface provides 23 bearer (B) channels that can transmit and receive data at the rate of 64 kbps, full-duplex, and one data (D) channel that can transmit and receive data at the rate of 64 kbps, full-duplex. Each E1 interface provides 30 bearer (B) channels that can transmit and receive data at the rate of 64 kbps, full-duplex, and one data (D) channel that can transmit and receive data at the rate of 64 kbps, full-duplex. The B channels are used for transmitting user data. The D channel is used for call setup control and network connection teardown, and provides the communication from the router to the ISDN switch. The B and D channels are presented to the system as serial interfaces that support High-Level Data Link Control (HDLC) and Point-to-Point Protocol (PPP) encapsulation. The multichannel PA-MCX port adapter supports dial-on-demand routing (DDR) when you are running ISDN PRI.

Each of the channels on the PA-MCX uses a portion of the bandwidth (fractional T1 or E1) or the entire bandwidth for data transmission. Usable bandwidth for each channel is n x 64 kbps or n x 56 kbps, where n is a number from 1 to 24 for T1 and 1 to 31 for E1. When you are not running at full T1/E1 speeds, the unused portion of the bandwidth cannot be used and is filled with idle channel data.

Note   Time slots on the PA-MCX port adapter are numbered 1 to 24 for T1 and 1 to 31 for E1, instead of the zero-based scheme (0 to 23 or 0 to 30) used with other Cisco products. This numbering scheme is to ensure consistency with telco numbering schemes for T1 and E1 channels within channelized equipment.

The PA-MCX supports Facility Data Link (FDL) in Extended Superframe (ESF) framing on T1 networks, as well as network and payload loopbacks. Bit error rate testing (BERT) is supported on each of the T1 or E1 links. BERT can be run only on one port at a time.

Note   On a PA-MCX configured for T1, BERT is done *only* over a framed T1 signal.

The PA-MCX port adapter does *not* support the aggregation of multiple T1s or E1s (called *inverse muxing* or *bonding*) for higher bandwidth data rates. The multichannel PA-MCX port adapter supports Cisco HDLC, Frame Relay, PPP, and Switched Multimegabit Data Service (SMDS) Data Exchange Interface (DXI) encapsulations over each T1 or E1 link. For SMDS only, DXI is sent on the T1 or E1 line, so it needs to connect to an SMDS switch that has direct DXI input.

Multichannel Packet Voice Overview

The PA-MCX contains a TDM switch that provides a non-blocking switch capacity of 2048 x 2048 64-kbps pulse code modulation (PCM) channels at 8192 Mbps and two TDM rate adoption switches that multiplex and demultiplex the input and output streams of the TDM switch.

In Voice over IP (VoIP), the digital signal processor (DSP) segments the voice signal into frames, which are then coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323. Because Voice over IP is a delay-sensitive application, you must have a well-engineered network end-to-end to use it successfully. Fine-tuning your network to adequately support Voice over IP involves a series of protocols and features geared toward quality of service (QoS). Traffic shaping considerations must be taken into account to ensure the reliability of the voice connection.

Features

The PA-MCX has the following features:

- Universal ports—Two, four, or eight interface ports per port adapter are configurable as either T1 (with integrated CSU/DSU) or E1 (with integrated G.703/G.704 120-ohm interface). Additionally, a port may be configured on a per-DS0 basis for voice termination, TDM pass-through (cross-connect), or packet data.

- Multiservice Interchange (MIX) support—Voice channels can be TDM-switched between port adapter slots in the Cisco 7200 VXR chassis. This allows DSP resources to be shared between port adapters in the same chassis or for port-to-port DS0 cross-connect between port adapter slots.

- DS0 drop and insert—Flexible TDM cross-connect capability between ports in the same port adapter is available.

- VoIP and VoFR termination—Full VoIP and Voice over Frame Relay (V0FR) gateway functionality for mixed environments is available.

- Multiple clocking options—Ports can be clocked internally from the network, or the network clock from one port can be sent to the other port on the card or to other cards across the MIX bus in the Cisco 7200 VXR chassis. In data mode, each port can be configured as a separate clock source.

- Flexible signaling support—Channel-associated signaling (CAS) and common channel signaling (CCS) support is available for both E1 and T1 applications in H.323 environments.

Port Configured as T1 Features

- DS1 100-ohm interfaces with RJ-48C connectors

- D4 Super Frame (SF) and Extended Superframe (ESF) framing

- Alternate mark inversion (AMI) or binary 8-zero substitution (B8ZS) line encoding

- Full Facility Data Link (FDL) support and FDL performance monitoring per ANSI T1.403 or AT&T TR 54016

- Selectable DSX-1 cable length in increments from 0 to 655 feet (0 to 196.5 meters)

- Selectable DS1 CSU line build-out—0, –7.5, –15, and –22.5 dB

- Selectable DS1 CSU receiver gain—26 or 36 dB

- DS1 line protection per UL1459/1950, FCC part 68

- Full support for DSX-1 Management Information Base (MIB), RFC 1406, including alarm detection and reporting
- DSX-1 MIB remote access supported

Port Configured as E1 Features

- E1 120-ohm (G.703) with RJ-48C connectors
- Software-configurable E1 national bits
- Bipolar with 3-zero substitution (B3ZS) encoding
- Full support for E1 MIB, RFC 1406, including alarm detection and reporting

Full BERT Capabilities on Each E1/T1

- Programmable pseudorandom pattern up to 24 bits in length, including 211-1, 215-1, 220-1, 220-1 QRSS, 233-1, all zeros, all ones, and alternating ones and zeros
- 32-bit-error count registers

Supported Loopbacks

- Line loopback—T1/E1 stream is loopbacked at the line interface unit (LIU) toward the network.
- Payload loopback—T1/E1 data stream is loopbacked at the framer toward the network.
- Diagnostic local loopback—T1/E1 data stream is loopbacked at the framer toward the system.
- Remote loopback—T1 stream is loopbacked at the LIU toward the network upon request from the far-end through the FDL command.

DSP Features

The following DSP features are available only when used in conjunction with a PA-VXB or PA-VXC port adapter.

- Full-featured DSP firmware—Support exists for eight standard-compression algorithms plus echo cancellation, full dual tone multi frequency (DTMF)/MF tone detection and generation, and dial-pulse generation.
- Silence suppression—To conserve network bandwidth, voice activity detection prevents sending data when no voice is present. Comfort-noise generation prevents uncomfortable dead silence on the receiving end.
- Coders-decoders (codecs)
    - G.711 (a-law/mu-law), G.729/G.729.a (with "b" variant), G.723.1, G.728, G.726
- Fax relay through T.30 support
    - V.17, V.29, V.27
- Echo cancellation—32 ms meeting G.165
- DTMF/R2/MF/SF/CP tone detection and generation
- Dial-pulse detection and generation
- Energy-based voice activity detection (VAD) and codec-specific VAD
- Comfort-noise generator

Signaling Supported for H.323 Environments

- H.323 V.2 support

- T1 CAS (robbed-bit signaling)

- CCS signaling—E1 and T1 ISDN PRI (user and network side), Q.SIG

- R2 signaling

List of Terms

Call leg—A logical connection between the router and either a telephony endpoint over a bearer channel or another endpoint using a session protocol.

Channel-associated signaling (CAS)—A form of signaling used on a T1 line. With CAS, a signaling element is dedicated to each channel in the T1 frame. This type of signaling is sometimes called robbed-bit signaling (RBS) because a bit is taken out (or robbed) from the user's data stream to provide signaling information to and from the switch.

CIR—Committed Information Rate. The average rate of information transfer a subscriber (for example, the network administrator) has stipulated for a Frame Relay PVC.

Codec—Coder-decoder compression scheme or technique. In Voice over IP, it specifies the voice coder rate of speech for a dial peer.

Dial peer—An addressable call endpoint. In Voice over IP, there are two kinds of dial peers: POTS and VoIP.

DS0—A 64-kbps channel on an E1 or T1 WAN interface.

DTMF—Dual tone multi frequency. Use of two simultaneous voice-band tones for dial (such as touch tone).

E&M—Stands for recEive and transMit (or Ear and Mouth). E&M is a trunking arrangement generally used for two-way switch-to-switch or switch-to-network connections. Cisco's E&M interface is an RJ-48 connector that allows connections to PBX trunk lines (tie lines).

FIFO—First-in, first-out. In data communication, FIFO refers to a buffering scheme in which the first byte of data entering the buffer is the first byte retrieved by the CPU. In telephony, FIFO refers to a queuing scheme in which the first calls received are the first calls processed.

FRF.11—Frame Relay Forum implementation agreement for Voice over Frame Relay (Version 1.0, May 1997). This specification defines multiplexed data, voice, fax, DTMF digit-relay, and CAS/robbed-bit signaling frame formats but does not include call setup, routing, or administration facilities.

FRF.12—FRF implementation agreement (also known as FRF.11 Annex C) developed to allow long data frames to be fragmented into smaller pieces and interleaved with real-time frames. In this way, real-time voice and non-real-time data frames can be carried together on lower-speed links without causing excessive delay to the real-time traffic.

FXO—Foreign Exchange Office. Interface that connects to the PSTN central office and is the interface offered on a standard telephone. The Cisco FXO interface is an RJ-11 connector that allows an analog connection to be directed at the PSTN central office. This interface is of value for off-premises extension applications.

FXS—Foreign Exchange Station. Interface that connects directly to a standard telephone and supplies ring, voltage, and dial tone. The Cisco FXS interface is an RJ-11 connector that allows connections to basic telephone service equipment, key sets, and PBXs.

Multilink PPP—Multilink Point-to-Point Protocol. This protocol is a method of splitting, recombining, and sequencing datagrams across multiple logical data links.

PBX—Private branch exchange. Privately owned central switching office.

PLAR—Private Line Auto Ringdown. Type of service resulting in a call attempt to some particular remote endpoint when the local extension is taken off-key.

POTS—Plain Old Telephone Service. Basic telephone service supplying standard single-line telephones, telephone lines, and access to the Public Switched Telephone Network.

POTS dial peer—Dial peer connected through a traditional telephony network. POTS peers point to a particular voice port on a voice network device.

PSTN—Public Switched Telephone Network. PSTN refers to the local telephone company.

PVC—Permanent virtual circuit.

QoS—Quality of service, which refers to the measure of service quality provided to the user.

RSVP—Resource Reservation Protocol. This protocol supports the reservation of resources across an IP network.

VoIP dial peer—Dial peer connected through a packet network; in the case of Voice over IP, this is an IP network. VoIP peers point to specific VoIP devices.

Voice Primer

To understand Cisco's voice implementations, it helps to have some understanding of analog and digital transmission and signaling. This section provides some very basic, abbreviated voice telephony information as background to help you configure Voice over IP and Voice over Frame Relay, and includes the following topics:

- Numbering Scheme
- Analog Versus Digital
- Codecs
- Delay
- Echo
- Signaling

Numbering Scheme

The standard PSTN is basically a large, circuit-switched network. It uses a specific numbering scheme, which complies with the ITU-T E.164 recommendations. For example, in North America, the North American Numbering Plan (NANP) is used, which consists of an area code, an office code, and a station code. Area codes are assigned geographically, office codes are assigned to specific switches, and station codes identify a specific port on that switch. The format in North America is 1Nxx-Nxx-xxxx, where *N* is a digit between 2 and 9 and *x* is a digit between 0 and 9. Internationally, each country is assigned a one- to three-digit country code; the country's dialing plan follows the country code. In Cisco voice implementations, numbering schemes are configured using the **destination-pattern** command.

Analog Versus Digital

Until recently, the telephone network was based on an analog infrastructure. Analog transmission is not particularly robust or efficient at recovering from line noise. Because analog signals degrade over distance, they need to be periodically amplified; this amplification boosts both the voice signal and ambient line noise, resulting in degradation of the quality of the transmitted sound.

In response to the limitations of analog transmission, the telephony network migrated to digital transmission using pulse code modulation (PCM) or adaptive differential pulse code modulation (ADPCM). In both cases, analog sound is converted into digital form by sampling the analog sound 8000 times per second and converting each sample into a numeric code.

Codecs

PCM and ADPCM are examples of "waveform" coder-decoder (codec) techniques. Waveform codecs are compression techniques that exploit the redundant characteristics of the waveform itself. In addition to waveform codecs, there are source codecs that compress speech by sending only simplified parametric information about voice transmission; these codecs require less bandwidth. Source codecs include linear predictive coding (LPC), code-excited linear prediction (CELP), and multipulse, multilevel quantization (MP-MLQ).

Coding techniques are standardized by the ITU-T in its G-series recommendations. The most popular coding standards for telephony and voice packet are:

- G.711—Describes the 64-kbps PCM voice-coding technique. In G.711, encoded voice is already in the correct format for digital voice delivery in the Public Switched Telephone Network (PSTN) or through PBXs.

- G.723.1—Describes a compression technique that can be used for compressing speech or audio signal components at a very low bit rate as part of the H.324 family of standards. This codec has two bit rates associated with it: 5.3 and 6.3 kbps. The higher bit rate is based on ML-MLQ technology and provides a somewhat higher quality of sound. The lower bit rate is based on CELP and provides system designers with additional flexibility.

- G.726—Describes ADPCM coding at 40, 32, 24, and 16 kbps. ADPCM-encoded voice can be interchanged between packet voice, PSTN, and PBX networks if the PBX networks are configured to support ADPCM.

- G.728—Describes a 16-kbps low-delay variation of CELP voice compression. CELP voice coding must be translated into a public telephony format for delivery to or through the PSTN.

- G.729—Describes CELP compression where voice is coded into 8-kbps streams. There are two variations of this standard (G.729 and G.729 Annex A) that differ mainly in computational complexity; both provide speech quality similar to 32-kbps ADPCM.

In Cisco voice implementations, compression schemes are configured using the **codec** command.

Mean Opinion Score

Each codec provides a certain quality of speech. The quality of transmitted speech is a subjective response of the listener. A common benchmark used to determine the quality of sound produced by specific codecs is the mean opinion score (MOS). With the MOS, a wide range of listeners judge the quality of a voice sample (corresponding to a particular codec) on a scale of 1 (bad) to 5 (excellent). The scores are averaged to provide the mean opinion score for that sample. Table 1-1 shows the relationship between codecs and the MOS.

Table 1-1   Compression Methods and the MOS

Compression Method	Bit Rate (kbps)	Framing Size	MOS
G.711 PCM	64	0.125	4.1
G.726 ADPCM	32	0.125	3.85
G.728 LD-CELP	16	0.625	3.61
G.729 CS-ACELP	8	10	3.92
G.729 x 2 Encodings	8	10	3.27
G.729 x 3 Encodings	8	10	2.68
G.729a CS-ACELP	8	10	3.7
G.723.1 MP-MLQ	6.3	30	3.9
G.723.1 ACELP	5.3	30	3.65

Although it might seem logical from a financial standpoint to convert all calls to low-bit rate codecs to save on infrastructure costs, you should exercise additional care when designing voice networks with low-bit-rate compression. There are drawbacks to compressing voice. One of the main drawbacks is signal distortion due to multiple encoding (called *tandem encoding*). For example, when a G.729 voice signal is tandem encoded three times, the MOS from 3.92 (very good) to 2.68 (unacceptable). Another drawback is codec-induced delay with low-bit-rate codecs.

Delay

One of the most important design considerations in implementing voice is minimizing one-way, end-to-end delay. Voice traffic is real-time traffic; if there is too long a delay in voice packet delivery, speech is unrecognizable. Delay is inherent in voice networking and is caused by a number of different factors. An acceptable delay is less than 200 milliseconds.

There are basically two kinds of delay inherent in today's telephony networks: propagation delay and handling delay. Propagation delay is caused by the characteristics of the speed of light traveling through a fiber-optic-based or copper-based media. Handling delay (sometimes called *serialization delay*) is caused by the devices that handle voice information. Handling delays have a significant impact on voice quality in a packetized network.

Codec-induced delays are considered a handling delay. Table 1-2 shows the delay introduced by different codecs.

Table 1-2   Codec-Induced Delays

Codec	Bit Rate (kbps)	Compression Delay (ms)
G.711 PCM	64	0.75
G.726 ADPCM	32	1
G.728 LD-CELP	16	3 to 5
G.729 CS-ACELP	8	10
G.729a CS-ACELP	8	10
G.723.1 MP-MLQ	6.3	30
G.723.1 ACELP	5.3	30

Another handling delay is the time it takes to generate a voice packet. In Voice over IP, the DSP generates a frame every 10 milliseconds. Two of these frames are then placed within one voice packet; the packet delay is therefore 20 milliseconds.

Another source of handling delay is the time it takes to move the packet to the output queue. Cisco IOS software expedites the process of determining packet destination and getting the packet to the output queue. The actual delay at the output queue is another source of handling delay and should be kept to under 10 milliseconds whenever possible by using whatever queuing methods are optimal for your network. Output queue delays are a quality of service (QoS) issue in Voice over IP for Cisco 7200 VXR routers, and are discussed in the "Configuring IP Networks for Real-Time Voice Traffic" section on page 4-15.

In Voice over Frame Relay, you need to make sure that voice traffic is not crowded out by data traffic. Strategies on how to manage Voice over Frame Relay voice traffic are discussed in the "Configuring Voice over Frame Relay" section on page 4-37.

Jitter

Jitter is another factor that affects delay. Jitter occurs when there is a variation between when a voice packet is expected to be received and when it actually is received, causing a discontinuity in the real-time voice stream. Voice devices such as the Cisco 7200 VXR routers with PA-MCX port adapters compensate for jitter by setting up a playout buffer to play back voice in a smooth fashion. Playout control is handled through Real-Time Transfer Protocol (RTP) encapsulation, either by selecting adaptive or nonadaptive playout-delay mode. In either mode, the default value for nominal delay is sufficient.

End-to-End Delay

Figuring out the end-to-end delay is not difficult if you know the end-to-end signal paths or data paths, the codec, and the payload size of the packets. Adding the delays from the endpoints to the codecs at both ends, the encoder delay (which is 5 milliseconds for G.711 and G.726 codecs and 10 milliseconds for the G.729 codec), the packetization delay, and the fixed portion of the network delay yield the end-to-end delay for the connection.

Echo

Echo is hearing your own voice in the telephone receiver while you are talking. When timed properly, echo is reassuring to the speaker; if the echo exceeds approximately 25 milliseconds, it can be distracting and cause breaks in the conversation. In a traditional telephony network, echo is normally caused by a mismatch in impedance from the four-wire network switch conversion to the two-wire local loop and is controlled by echo cancelers. In voice packet-based networks, echo cancelers are built into the low-bit-rate codecs and are operated on each digital signal processor (DSP). Echo cancelers are limited by design by the total amount of time they wait for the reflected speech to be received, which is known as an echo trail. The echo trail is normally 32 milliseconds.

In Cisco voice implementations, echo cancelers are enabled using the **echo-cancel enable** command. The echo trails are configured using the **echo-cancel-coverage** command. For example, Voice over IP has configurable echo trails of 16, 24, and 32 milliseconds.

Signaling

Although there are various types of signaling used in telecommunications today, this document describes only those with direct applicability to Cisco voice implementations. The first one involves access signaling, which determines when a line has gone off-hook or on-hook (in other words, dial tone). Foreign Exchange Office (FXO) and Foreign Exchange Station (FXS) are types of access signaling. There are two common methods of providing this basic signal:

- Loop start is the most common technique for access signaling in a standard PSTN end-loop network. When a handset is picked up (goes off-hook), this action closes the circuit that draws current from the telephone company central office (CO), indicating a change in status. This change in status signals the CO to provide dial tone. An incoming call is signaled from the CO to the handset by sending a signal in a standard on/off pattern, which causes the telephone to ring.

- Ground start is another access signaling method used to indicate on-hook or off-hook status to the CO, but this signaling method is primarily used on trunk lines or tie lines between PBXs. Ground start signaling works by using ground and current detectors. This allows the network to indicate off-hook or seizure of an incoming call independently of the ringing signal.

In Cisco voice implementations, access signaling is configured using the **signal** command.

Another signaling technique used mainly between PBXs or other network-to-network telephony switches is known as E&M. There are five types of E&M signaling, as well as two different wiring methods. The Cisco voice implementation supports E&M types I, II, III, and V, using both two-wire and four-wire implementations. In Cisco voice implementations, E&M signal types are configured using the **type** command.

LEDs

As shown in Figure 1-4, Figure 1-5, and Figure 1-6, the PA-MCX port adapters have a green enabled LED, a bicolor alarm LED, and one bicolor port status LED, one for each port on the port adapter. Table 1-3 lists the colors and functions of the LEDs.

Figure 1-4   PA-MCX-2TE1 Port Adapter Front Panel LEDs
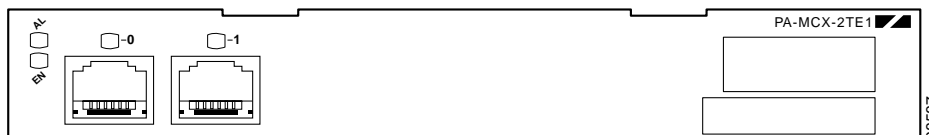
Figure 1-5   PA-MCX-4TE1 Port Adapter Front Panel LEDs
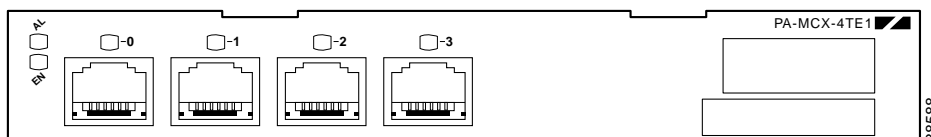
Figure 1-6   PA-MCX-8TE1 Port Adapter Front Panel LEDs
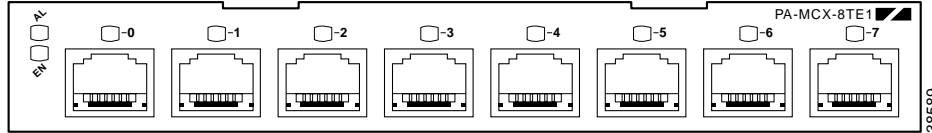
Table 1-3   PA-MCX LEDs

LED Label	Color	State	Function
EN	Green	On	Indicates the PA-MCX is powered up.
		Off	Indicates the PA-MCX is not ready or is disabled.
AL	Amber	On	Indicates an alarm condition exists on the remote end of one of the T1/E1 ports.
	Red	On	Indicates an alarm condition exists locally on one of the T1/E1 ports.
		Off	Indicates no alarms detected on any port.
0 through 7	Green	On	Indicates the port is enabled and in frame.
	Yellow	On	Indicates the port is in loopback.
		Off	Indicates that the port is not enabled, the received signal is bad, or an alarm condition exists.

Cables, Connectors, and Pinouts

The T1/E1 interface receptacles on the PA-MCX port adapters are RJ-48C for both T1 (100-ohm) and E1 (120-ohm).

After you properly connect a port to a line, it takes approximately 30 seconds for Cisco IOS to report that the line is up.

Each connection supports T1 (100-ohm) or E1 (120-ohm) interfaces that meet T1.403 and ACCUNET TR62411 standards. The RJ-48C connection does not require an external transceiver. The DS1 ports are T1 interfaces that use foil twisted-pair cables.

Shielded cables (FTP [foil twisted-pair]) with 120-ohm impedance are required to comply with CE marking requirements.

Figure 1-7 shows the PA-MCX port adapter interface cable connector. See the "Connecting Interface Cables" section on page 3-5 for directions on connecting the cables to a PA-MCX port adapter.

Figure 1-7   PA-MCX Port Adapter Interface Connector

87654321
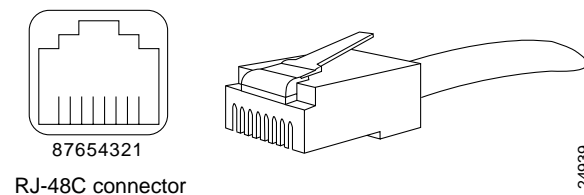
RJ-48C connector

Table 1-4 lists the signal pinouts and descriptions for the RJ-48C connector.

Table 1-4   RJ-48C Connector Pinouts

Pin	Signal
1	RX tip
2	RX ring
3	No connection
4	TX tip
5	TX ring
6	No connection
7	No connection
8	No connection

Warning   **To reduce the risk of fire, use only 26 AWG or larger telecommunication line cord.** Statement 1023

Port Adapter Slot Locations on the Supported Platform

This section discusses port adapter slot locations on the supported platform. The illustration that follows summarizes the slot location conventions.

Note   Interface ports are numbered from left to right starting with 0.

Cisco 7200 VXR Routers Slot Numbering

Figure 1-8 shows a Cisco 7206VXR with port adapters installed. In the Cisco 7206VXR, port adapter slot 1 is in the lower left position, and port adapter slot 6 is in the upper right position. (The Cisco 7204VXR is not shown; however, the PA-MCX port adapters can be installed in any available port adapter slot. Slot 0 is always reserved for the Fast Ethernet port on the I/O controller—if present.)

Figure 1-8   Port Adapter Slots in the Cisco 7206 VXR

Port adapter slot 5

Port adapter slot 3

Port adapter slot 1

Port adapter slot 6

Port adapter slot 4

Port adapter slot 2
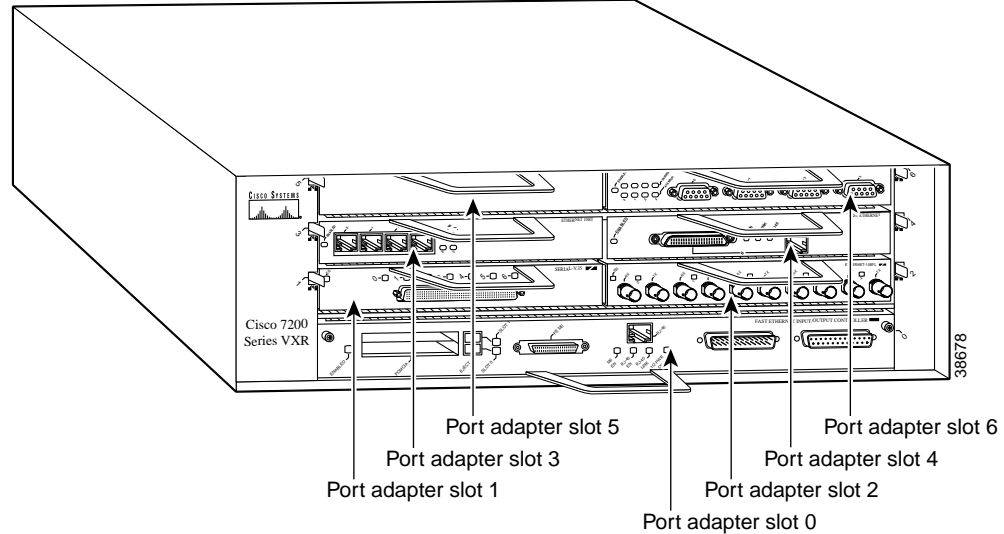
Port adapter slot 0

Identifying Interface Addresses

This section describes how to identify interface addresses for the PA-MCX port adapters in the supported platform. Interface addresses specify the actual physical location of each interface on a router or switch.

Interfaces on the PA-MCX port adapters installed in a router maintain the same address regardless of whether other port adapters are installed or removed. However, when you move a port adapter to a different slot, the first number in the interface address changes to reflect the new port adapter slot number.

Table 1-5 explains how to identify interface addresses.

Table 1-5   Identifying Interface Addresses

Platform	Interface Address Format	Numbers	Syntax
Cisco 7200 VXR routers	Port-adapter-slot-number/interface-port-number	Port adapter slot—0 through 6 (depends on the number of slots in the router)[1] Interface port—0 through 7 (depends on the number of ports in the port adapter)	1/0

1. Port adapter slot 0 is reserved for the Fast Ethernet port on the I/O controller (if present).

Cisco 7200 VXR Router Interface Addresses

This section describes how to identify the interface addresses used for the PA-MCX port adapters in Cisco 7200 VXR routers. The interface address is composed of a two-part number in the format *port-adapter-slot-number/interface-port-number*. See Table 1-5 for the interface address format.

In Cisco 7200 VXR routers, port adapter slots are numbered from the lower left to the upper right, beginning with port adapter slot 1 and continuing through port adapter slot 4 for the Cisco 7204VXR, and slot 6 for the Cisco 7206VXR. (Port adapter slot 0 is reserved for the optional Fast Ethernet port on the I/O controller—if present.)

The interface addresses of the interfaces on an eight-port PA-MCX port adapter in port adapter slot 1 are 1/0 through 1/7 (port adapter slot 1 and interfaces 0 through 7). If the PA-MCX was in port adapter slot 4, these same interfaces would be numbered 4/0 through 4/7 (port adapter slot 4 and interfaces 0 through 7).

C H A P T E R 2

Preparing for Installation

This chapter describes the general equipment, safety, and site preparation requirements for installing the PA-MCX port adapters. This chapter contains the following sections:

- Required Tools and Equipment, page 2-1
- Software and Hardware Requirements, page 2-1
- Checking Hardware and Software Compatibility, page 2-2
- Safety Guidelines, page 2-2
- FCC Class A Compliance, page 2-9

Required Tools and Equipment

You need the following tools and parts to install a port adapter. If you need additional equipment, contact a service representative for ordering information.

- PA-MCX-2TE1(=), PA-MCX-4TE1(=), or PA-MCX-8TE1(=) port adapter
- Twisted-pair cable
- Number 2 Phillips screwdriver
- Your own electrostatic discharge (ESD)-prevention equipment or the disposable grounding wrist strap included with all upgrade kits, field-replaceable units (FRUs), and spares
- Antistatic mat
- Antistatic container

Software and Hardware Requirements

Table 2-1 lists the recommended minimum Cisco IOS software release required to use the PA-MCX port adapters in the supported router platform.

Table 2-1   PA-MCX Software and Hardware Requirements

Supported Platform	Recommended Minimum Cisco IOS Release
Cisco 7204VXR and Cisco 7206VXR with NPE-225, NPE-300, NPE-400, or NPE-G1	Cisco IOS Release 12.1(5)T or a later release of Cisco IOS Release 12.1 T Cisco IOS Release 12.2(2)T or a later release of Cisco IOS Release 12.2 T Cisco IOS Release 12.2(14)S or later release of Cisco IOS Release 12.2 S Cisco IOS Release 12.3 (1)T or later release of Cisco IOS Release 12.3T

Checking Hardware and Software Compatibility

To check the minimum software requirements of Cisco IOS software with the hardware installed on your router, Cisco maintains the Software Advisor tool on Cisco.com. This tool does not verify whether modules within a system are compatible, but it does provide the minimum IOS requirements for individual hardware modules or components.

Note   Access to this tool is limited to users with Cisco.com login accounts.

To access Software Advisor, click **Login** at Cisco.com and go to **Technical Support**: **Featured Tools**: **Software Advisor**. You can also access the tool by pointing your browser directly to http://www.cisco.com/cgi-bin/Support/CompNav/Index.pl .

Choose a product family or enter a specific product number to search for the minimum supported software release needed for your hardware.

Safety Guidelines

This section provides safety guidelines that you should follow when working with any equipment that connects to electrical power or telephone wiring.

Safety Warnings

Safety warnings appear throughout this publication in procedures that, if performed incorrectly, might harm you. A warning symbol precedes each warning statement.

Warning Definition

Warning   IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Waarschuwing   BELANGRIJKE VEILIGHEIDSINSTRUCTIES

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

Varoitus   TÄRKEITÄ TURVALLISUUSOHJEITA

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET

Attention   IMPORTANTES INFORMATIONS DE SÉCURITÉ

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

Warnung   WICHTIGE SICHERHEITSHINWEISE

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza   IMPORTANTI ISTRUZIONI SULLA SICUREZZA

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

Advarsel   VIKTIGE SIKKERHETSINSTRUKSJONER

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso   INSTRUÇÕES IMPORTANTES DE SEGURANÇA

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡Advertencia!   INSTRUCCIONES IMPORTANTES DE SEGURIDAD

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Varning!   VIKTIGA SÄKERHETSANVISNINGAR

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR

Figyelem   **FONTOS BIZTONSÁGI ELOÍRÁSOK**

Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение   **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告   重要的安全性说明

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

警告   安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

주의   중요 안전 지침

이 경고 기호는 위험을 나타냅니다. 작업자가 신체 부상을 일으킬 수 있는 위험한 환경에 있습니다. 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 사고를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾으십시오.

이 지시 사항을 보관하십시오.

Aviso   INSTRUÇÕES IMPORTANTES DE SEGURANÇA

Este símbolo de aviso significa perigo. Você se encontra em uma situação em que há risco de lesões corporais. Antes de trabalhar com qualquer equipamento, esteja ciente dos riscos que envolvem os circuitos elétricos e familiarize-se com as práticas padrão de prevenção de acidentes. Use o número da declaração fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham o dispositivo.

GUARDE ESTAS INSTRUÇÕES

Advarsel   VIGTIGE SIKKERHEDSANVISNINGER

Dette advarselssymbol betyder fare. Du befinder dig i en situation med risiko for legemesbeskadigelse. Før du begynder arbejde på udstyr, skal du være opmærksom på de involverede risici, der er ved elektriske kredsløb, og du skal sætte dig ind i standardprocedurer til undgåelse af ulykker. Brug erklæringsnummeret efter hver advarsel for at finde oversættelsen i de oversatte advarsler, der fulgte med denne enhed.

GEM DISSE ANVISNINGER

تحذير   إرشادات الأمان الهامة

يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في أخر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز. قم بحفظ هذه الإرشادات

Upozorenje   VAŽNE SIGURNOSNE NAPOMENE

Ovaj simbol upozorenja predstavlja opasnost. Nalazite se u situaciji koja može prouzročiti tjelesne ozljede. Prije rada s bilo kojim uređajem, morate razumjeti opasnosti vezane uz električne sklopove, te biti upoznati sa standardnim načinima izbjegavanja nesreća. U prevedenim sigurnosnim upozorenjima, priloženima uz uređaj, možete prema broju koji se nalazi uz pojedino upozorenje pronaći i njegov prijevod.

SAČUVAJTE OVE UPUTE

Upozornění   DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY

Tento upozorňující symbol označuje nebezpečí. Jste v situaci, která by mohla způsobit nebezpečí úrazu. Před prací na jakémkoliv vybavení si uvědomte nebezpečí související s elektrickými obvody a seznamte se se standardními opatřeními pro předcházení úrazům. Podle čísla na konci každého upozornění vyhledejte jeho překlad v přeložených bezpečnostních upozorněních, která jsou přiložena k zařízení.

USCHOVEJTE TYTO POKYNY

Προειδοποίηση   ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

Αυτό το προειδοποιητικό σύμβολο σημαίνει κίνδυνο. Βρίσκεστε σε κατάσταση που μπορεί να προκαλέσει τραυματισμό. Πριν εργαστείτε σε οποιοδήποτε εξοπλισμό, να έχετε υπόψη σας τους κινδύνους που σχετίζονται με τα ηλεκτρικά κυκλώματα και να έχετε εξοικειωθεί με τις συνήθεις πρακτικές για την αποφυγή ατυχημάτων. Χρησιμοποιήστε τον αριθμό δήλωσης που παρέχεται στο τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή.

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה   **הוראות בטיחות חשובות**

סימן אזהרה זה מסמל סכנה. אתה נמצא במצב העלול לגרום לפציעה. לפני שתעבוד עם ציוד כלשהו, עליך להיות מודע לסכנות הכרוכות במעגלים חשמליים ולהכיר את הנהלים המקובלים למניעת תאונות. השתמש במספר ההוראה המסופק בסופה של כל אזהרה כד לאתר את התרגום באזהרות הבטיחות המתורגמות שמצורפות להתקן.

שמור הוראות אלה

Opomena   постои кај електричните кола и треба да ги познавате стандардните постапки за спречување на несреќни случаи. Искористете го бројот на изјавата што се наоѓа на крајот на секое предупредување за да го најдете неговиот период во преведените безбедносни предупредувања што се испорачани со уредот.
ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie   **WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA**

Ten symbol ostrzeżenia oznacza niebezpieczeństwo. Zachodzi sytuacja, która może powodować obrażenia ciała. Przed przystąpieniem do prac przy urządzeniach należy zapoznać się z zagrożeniami związanymi z układami elektrycznymi oraz ze standardowymi środkami zapobiegania wypadkom. Na końcu każdego ostrzeżenia podano numer, na podstawie którego można odszukać tłumaczenie tego ostrzeżenia w dołączonym do urządzenia dokumencie z tłumaczeniami ostrzeżeń.

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie   **DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY**

Tento varovný symbol označuje nebezpečenstvo. Nachádzate sa v situácii s nebezpečenstvom úrazu. Pred prácou na akomkoľvek vybavení si uvedomte nebezpečenstvo súvisiace s elektrickými obvodmi a oboznámte sa so štandardnými opatreniami na predchádzanie úrazom. Podľa čísla na konci každého upozornenia vyhľadajte jeho preklad v preložených bezpečnostných upozorneniach, ktoré sú priložené k zariadeniu.

USCHOVAJTE SI TENTO NÁVOD

Electrical Equipment Guidelines

Follow these basic guidelines when working with any electrical equipment:

*   Before beginning any procedures requiring access to the chassis interior, locate the emergency power-off switch for the room in which you are working.

*   Disconnect all power and external cables before moving a chassis; do not work alone when potentially hazardous conditions exist.

*   Never assume that power has been disconnected from a circuit; always check.

*   Do not perform any action that creates a potential hazard to people or makes the equipment unsafe; carefully examine your work area for possible hazards such as moist floors, ungrounded power extension cables, and missing safety grounds.

Telephone Wiring Guidelines

Use the following guidelines when working with any equipment that is connected to telephone wiring or to other network cabling:

*   Never install telephone wiring during a lightning storm.

*   Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.

*   Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.

*   Use caution when installing or modifying telephone lines.

Preventing Electrostatic Discharge Damage

Electrostatic discharge (ESD) damage, which can occur when electronic cards or components are improperly handled, results in complete or intermittent failures. Port adapters and processor modules comprise printed circuit boards that are fixed in metal carriers. Electromagnetic interference (EMI) shielding and connectors are integral components of the carrier. Although the metal carrier helps to protect the board from ESD, use a preventive antistatic strap during handling.

Following are guidelines for preventing ESD damage:

*   Always use an ESD wrist or ankle strap and ensure that it makes good skin contact.

*   Connect the equipment end of the strap to an unfinished chassis surface.

*   When installing a component, use any available ejector levers or captive installation screws to properly seat the bus connectors in the backplane or midplane. These devices prevent accidental removal, provide proper grounding for the system, and help to ensure that bus connectors are properly seated.

*   When removing a component, use any available ejector levers or captive installation screws to release the bus connectors from the backplane or midplane.

*   Handle carriers by available handles or edges only; avoid touching the printed circuit boards or connectors.

*   Place a removed board component-side-up on an antistatic surface or in a static shielding container. If you plan to return the component to the factory, immediately place it in a static shielding container.

> • Avoid contact between the printed circuit boards and clothing. The wrist strap only protects components from ESD voltages on the body; ESD voltages on clothing can still cause damage.
>
> • Never attempt to remove the printed circuit board from the metal carrier.

⚠
Caution   For safety, periodically check the resistance value of the antistatic strap. The measurement should be between 1 and 10 megohms (Mohm).

FCC Class A Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

> • Turn the television or radio antenna until the interference stops.
>
> • Move the equipment to one side or the other of the television or radio.
>
> • Move the equipment farther away from the television or radio.
>
> • Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

✎
Note   The *PA-MCX port adapters* have been designed to meet these requirements. Modifications to this product that are not authorized by Cisco Systems, Inc., could void the various approvals and negate your authority to operate the product.

⚠
Caution   This equipment will be inoperable when main power fails.

FCC Class A Compliance

CHAPTER

3

Removing and Installing Port Adapters

This chapter describes how to remove the PA-MCX port adapter from the supported platform and also how to install a new or replacement port adapter. This chapter contains the following sections:

Each port adapter circuit board is mounted to a metal carrier and is sensitive to electrostatic discharge (ESD) damage.

Note   When a port adapter slot is not in use, a blank port adapter must fill the empty slot to allow the router or switch to conform to electromagnetic interference (EMI) emissions requirements and to allow proper airflow across the port adapters. If you plan to install a new port adapter in a slot that is not in use, you must first remove the blank port adapter.

Caution   When powering off the router, wait a minimum of 30 seconds before powering it on again.

Handling Port Adapters

Caution   Always handle the port adapter by the carrier edges and handle; never touch the port adapter components or connector pins. (See Figure 3-1.)

Figure 3-1   Handling a Port Adapter

Metal carrier

Printed circuit board

H6420
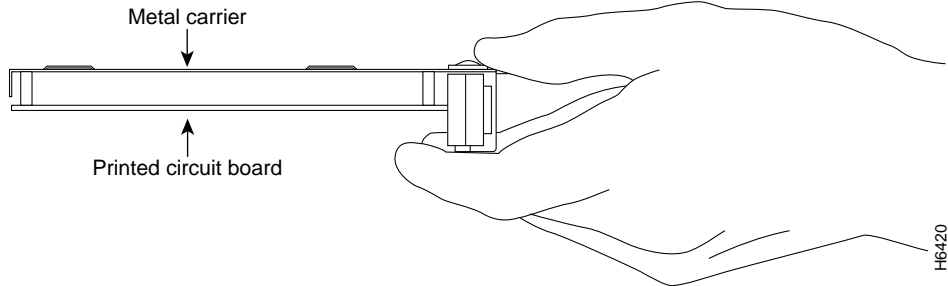
Online Insertion and Removal

Several platforms support online insertion and removal (OIR) of port adapters; therefore, you do not have to power down routers when removing and replacing a PA-MCX port adapter in Cisco 7200 VXR routers.

It is wise to gracefully shut down the system before removing a port adapter that has active traffic moving through it. Removing a module while traffic is flowing through the ports can cause system disruption. Once the module is inserted, the ports can be brought back up.

Note As you disengage the module from the router or switch, online insertion and removal (OIR) administratively shuts down all active interfaces in the module.

OIR allows you to install and replace modules while the router is operating; you do not need to notify the software or shut down the system power, although you should not run traffic through the module you are removing while it is being removed. OIR is a method that is seamless to end users on the network, maintains all routing information, and preserves sessions.

The following is a functional description of OIR for background information only; for specific procedures for installing and replacing a module in a supported platform, refer to the "Port Adapter Removal and Installation" section on page 3-3.

Each module has a bus connector that connects it to the router. The connector has a set of tiered pins in three lengths that send specific signals to the system as they make contact with the module. The system assesses the signals it receives and the order in which it receives them to determine if a module is being removed from or introduced to the system. From these signals, the system determines whether to reinitialize a new interface or to shut down a disconnected interface.

Specifically, when you insert a module, the longest pins make contact with the module first, and the shortest pins make contact last. The system recognizes the signals and the sequence in which it receives them.

When you remove or insert a module, the pins send signals to notify the system of changes. The router then preforms the following procedure:

1. Rapidly scans the system for configuration changes.

2. Initializes newly inserted port adapters or administratively shuts down any vacant interfaces.

3. Brings all previously configured interfaces on the module back to their previously installed state. Any newly inserted interface is put in the administratively shutdown state, as if it was present (but not configured) at boot time. If a similar module type is reinserted into a slot, its ports are configured and brought online up to the port count of the originally installed module of that type.

Note   Before you begin installation, read Chapter 2, "Preparing for Installation," for a list of parts and tools required for installation.

Warnings and Cautions

Observe the following warnings and cautions when installing or removing port adapters.

Caution   Do not slide a port adapter all the way into the slot until you have connected all required cables. Trying to do so disrupts normal operation of the router or switch.

Note   If a port adapter lever or other retaining mechanism does not move to the locked position, the port adapter is not completely seated in the midplane. Carefully pull the port adapter halfway out of the slot, reinsert it, and move the port adapter lever or other mechanism to the locked position.

Caution   To prevent jamming the carrier between the upper and the lower edges of the port adapter slot, and to ensure that the edge connector at the rear of the port adapter mates with the connection at the rear of the port adapter slot, make certain that the carrier is positioned correctly, as shown in the cutaway in the following illustrations.

Warning   **When performing the following procedures, wear a grounding wrist strap to avoid ESD damage to the card. Some platforms have an ESD connector for attaching the wrist strap. Do not directly touch the midplane or backplane with your hand or any metal tool, or you could shock yourself.**

Port Adapter Removal and Installation

In this section, the illustration that follows gives step-by-step instructions on how to remove and install port adapters in Cisco 7200 VXR routers.

Cisco 7200 Series—Removing and Installing a Port Adapter

Step 1

To remove the port adapter, place the port adapter lever in the unlocked position. (See A.) The port adapter lever remains in the unlocked position.

Step 2

Grasp the handle of the port adapter and pull the port adapter from the router, about halfway out of its slot. If you are removing a blank port adapter, pull the blank port adapter completely out of the chassis slot.

Step 3

With the port adapter halfway out of the slot, disconnect all cables from the port adapter. After disconnecting the cables, pull the port adapter from its chassis slot.

Step 4

To insert the port adapter, carefully align the port adapter carrier between the upper and the lower edges of the port adapter slot. (See B.)

Step 5

Carefully slide the new port adapter halfway into the port adapter slot. (See B.)

Step 6

With the port adapter halfway into the slot, connect all required cables to the port adapter. After connecting all required cables, carefully slide the port adapter all the way into the slot until the port adapter is seated in the router midplane.

Step 7

After the port adapter is properly seated, lock the port adapter lever. (See A.)

Port adapter lever
(locked position)
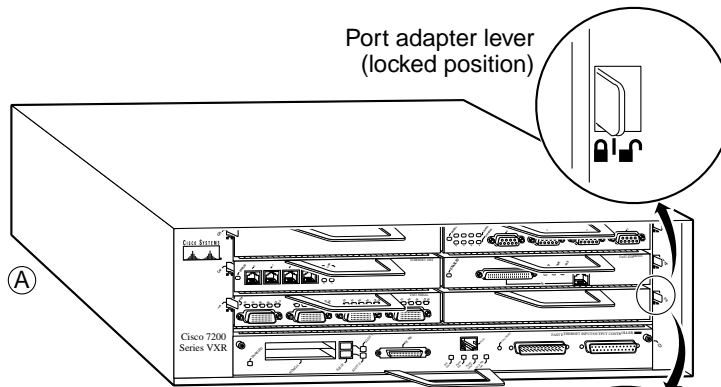
Note: This adapter removal applies to any port or service adapter.

Port adapter lever
(unlocked position)

Slot guide
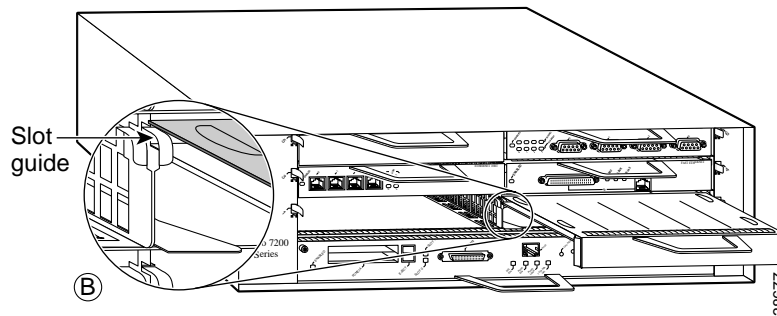
Connecting Interface Cables

The PA-MCX port adapters use twisted-pair cables with RJ-48C connectors to connect to a PBX or to the PSTN.

To connect twisted-pair cables with RJ-48C connectors to the PA-MCX port adapter, proceed as follows:

Step 1   Attach the cable directly to one of the RJ-48C ports on the PA-MCX port adapter.

Step 2   Attach the network end of the cable to your external equipment.

Step 3   Repeat Step 1 and Step 2 for the other PA-MCX ports.

Figure 3-2   Connecting the PA-MCX Twisted-Pair Cable with RJ-48C Connector
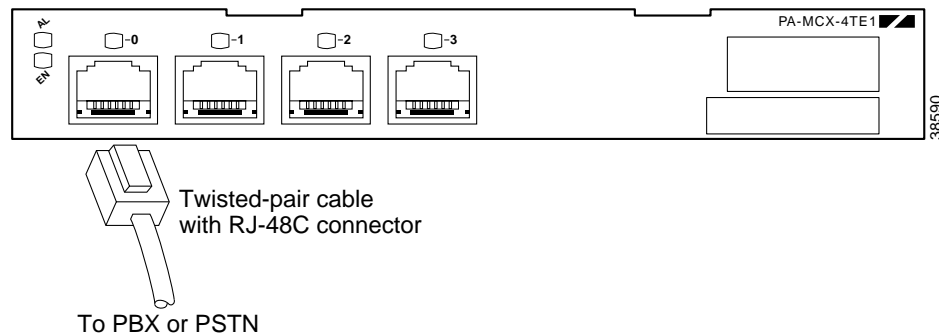
Note   Port adapters have a handle attached, but this handle is not shown in Figure 3-2 to allow a full view of the detail on each port adapter's faceplate.

Warning   **To reduce the risk of fire, use only 26 AWG or larger telecommunication line cord.** Statement 1023

Configuring the PA-MCX

To continue your PA-MCX port adapter installation, you must configure the card type as either T1 or E1 and then configure the interfaces.

This chapter contains the following sections:

- Using the EXEC Command Interpreter, page 4-1
- Configuring the Interfaces, page 4-2
- Configuring Voice over IP, page 4-12
- Configuring Voice over Frame Relay, page 4-37
- Checking the Configuration, page 4-38

Using the EXEC Command Interpreter

You modify the configuration of your router through the software command interpreter called the *EXEC* (also called enable mode). You must enter the privileged level of the EXEC command interpreter with the **enable** command before you can use the **configure** command to configure a new interface or change the existing configuration of an interface. The system prompts you for a password if one has been set.

The system prompt for the privileged level ends with a pound sign (#) instead of an angle bracket (>). At the console terminal, use the following procedure to enter the privileged level:

Step 1 At the user-level EXEC prompt, enter the **enable** command. The EXEC prompts you for a privileged-level password as follows:

```
Router> enable

Password:
```

Step 2 Enter the password (the password is case sensitive). For security purposes, the password is not displayed.

When you enter the correct password, the system displays the privileged-level system prompt (#):

```
Router#
```

To configure the new interfaces, proceed to the "Configuring the Interfaces" section on page 4-2.

Configuring the Interfaces

The PA-MCX interfaces can be configured as data-only interfaces or as TDM cross-connects to a digital voice port adapter. After you verify that the new PA-MCX is installed correctly (the enabled LED goes on), use the privileged-level **configure** command to configure the new interfaces. Have the following information available:

- Protocols you plan to route on each new interface
- IP addresses, if you plan to configure the interfaces for IP routing
- Voice network plan
- Clock timing source you plan to use for each new interface and clock speeds for external timing

If you installed a new PA-MCX or if you want to change the configuration of an existing interface, you must enter configuration mode to configure the new interfaces. If you replaced a PA-MCX that was previously configured, the system recognizes the new interfaces and brings each of them up in their existing configuration.

For a summary of the configuration options available and instructions for configuring interfaces on a PA-MCX, refer to the appropriate configuration publications listed in the "Related Documentation" section on page viii.

You execute configuration commands from the privileged level of the EXEC command interpreter, which usually requires password access. Contact your system administrator, if necessary, to obtain password access. (See the "Using the EXEC Command Interpreter" section on page 4-1 for an explanation of the privileged level of the EXEC.)

This section contains the following subsections:

- Shutting Down an Interface, page 4-2
- Performing a Basic Configuration, page 4-4
- Configuring the Controller, page 4-6
- Performing a Basic Data Interface Configuration, page 4-7
- Configuring Cyclic Redundancy Checks, page 4-9
- Configuring Multichannel ISDN PRI Interfaces, page 4-9
- Configuring the Interface for DSPfarm, page 4-11

Shutting Down an Interface

Before you remove an interface that you will not replace, or replace port adapters, use the **shutdown** command to shut down (disable) the interfaces to prevent anomalies when you reinstall the new or reconfigured port adapter. When you shut down an interface, it is designated *administratively down* in the **show** command displays.

Follow these steps to shut down an interface:

Step 1   Enter the privileged level of the EXEC command interpreter (also called enable mode). (See the "Using the EXEC Command Interpreter" section on page 4-1 for instructions.)

Step 2   At the privileged-level prompt, enter configuration mode and specify that the console terminal is the source of the configuration subcommands, as follows:

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Step 3   Shut down interfaces by entering the **interface serial** subcommand (followed by the interface address of the interface), and then enter the **shutdown** command. Table 4-1 shows the command syntax.

When you have finished, press **Ctrl-Z**—hold down the **Control** key while you press **Z**—or enter **end** or **exit** to exit configuration mode and return to the EXEC command interpreter.

Table 4-1   Syntax of the shutdown Command

Platform	Command	Example

Cisco 7200 VXR series routers	**interface**, followed by the *type* (**serial**) and *slot/port* (port-adapter-slot-number/ interface-port-number)
	
	 shutdown
		The example is for interface 0 and interface 1 on a port adapter in port adapter slot 6.
		
		 ```Router(config-if)# interface serial 6/0```
		 ```Router(config-if)# shutdown```
		 ```Router(config-if)# interface serial 6/1```
		 ```Router(config-if)# shutdown```
		 Ctrl-Z
		 ```Router#```

Note   If you need to shut down additional interfaces, enter the **interface serial** subcommand (followed by the interface address of the interface) for each of the interfaces on your port adapter. Use the **no shutdown** command to enable the interface.

Step 4   Write the new configuration to NVRAM as follows:

```
Router# copy running-config startup-config
[OK]
Router#
```

The system displays an OK message when the configuration has been stored in NVRAM.

Step 5   Verify that new interfaces are now in the correct state (shut down) using the **show interfaces** command (followed by the interface type and interface address of the interface) to display the specific interface. Table 4-2 provides examples.

Table 4-2   Examples of the show interfaces Command

Platform	Command	Example

Cisco 7200 VXR series routers	**show interfaces serial**, followed by *slot/port* (port-adapter-slot-number/ interface-port-number)	The example is for interface 0 on a port adapter in port adapter slot 6.
		
		 ```Router# show interfaces serial 6/0```
		
		 ```Serial 6/0 is administratively down,```
		 ```line protocol is down```
		
		 ```[Additional display text omitted from```
		 ```this example]```

Step 6   Reenable interfaces by doing the following:

    a.   Repeat Step 3 to reenable an interface. Substitute the **no shutdown** command for the **shutdown** command.

b. Repeat Step 4 to write the new configuration to memory. Use the
copy running-config startup-config command.

c. Repeat Step 5 to verify that the interfaces are in the correct state. Use the
show interfaces command followed by the interface type and interface address of the interface.

For complete descriptions of software configuration commands, refer to the publications listed in the "Related Documentation" section on page viii.

Performing a Basic Configuration

Following are instructions for a basic configuration: specifying card and service type, enabling an interface, and specifying IP routing. You might also need to enter other configuration subcommands, depending on the requirements for your system configuration and the protocols you plan to route on the interface. For complete descriptions of configuration subcommands and the configuration options available for *serial* interfaces, refer to the appropriate software documentation.

Specifying Card Type is Required

Because the PA-MCX port adapter can be configured for E1 or T1 connectivity, you **must** specify the card type as E1 or T1, as described in the following procedure. There is no default card type. The port adapter is not functional until the card type is set. Information about the port adapter is not indicated in the output of any show commands unless the card type has been set to E1 or T1.

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time you can exit the privileged level and return to the user level by entering **disable** at the prompt as follows:

```
Router# disable

Router>
```

Step 1 Enter configuration mode and specify that the console terminal is the source of the configuration subcommands, as follows:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Step 2 Specify whether the card is to be used as T1 or E1 by using the **card type** command in configuration mode.

- The example below sets the card in slot 1 to T1:

```
Router(config)# card type t1 1
```

- The example below sets the card in slot 1 to E1:

```
Router(config)# card type e1 1
```

Note To change the card type of the PA-MCX after the **card type** command has been entered, you must remove the card from the router, save the running configuration to NVRAM, and reboot the router. When the router has finished rebooting, reinsert the card and repeat Step 2

Or you can save the running configuration to the TFTP server and edit the card type in the saved file. Then use the **copy tftp://**<*tftp address*>*/file name* **system://startup-config** command to copy the configuration back to the router, and then reload.

Step 3 Specify whether the port is to be configured as a data-only port or as a TDM cross-connect to a digital voice port adapter by using the **service-type** {**data** | **ccs-voice** | **cas-voice**}command in controller mode. The example below sets the first port in slot 1 to data:

```
Router(config)# controller t1 1/0
Router(config-controller)# service-type data
```

No voice features are supported in data mode.

The example below sets the second port in slot 1 to common channel signalling (CCS) voice:

```
Router(config)# controller t1 1/1
router(config-controller)# service-type ccs-voice
```

This mode is used to connect to the PSTN or a PBX that supports CCS (such as ISDN PRI). In this mode, an external clock can be configured as the source clock for the entire router using the **frame-clock-select** command.

The example below sets the second port in slot 1 to channel associated signalling (CAS) voice:

```
Router(config)# controller t1 1/1
router(config-controller)# service-type cas-voice
```

This mode is used to connect to the PSTN or a PBX that supports CAS (such as T1 RBS or E1 R2). In this mode, an external clock can be configured as the source clock for the entire router using the **frame-clock-select** command.

Note When configuring an external clock in either CCS voice or CAS voice mode, it is important to ensure that all ports configured for this mode use the same clock, or framing slips may occur.

Note When a port is set to CAS voice mode, 64Kbs data channel-groups can also be configured on that same T1 port.

The default is ccs-voice.

If you have configured ports on your PA-MCX for data only, proceed to the next section, "Configuring the Controller" and the "Performing a Basic Data Interface Configuration" section on page 4-7. If you have configured ports on your PA-MCX for TDM cross-connect, proceed to the "Configuring the Interface for DSPfarm" section on page 4-11.

Configuring the Controller

The following steps make up a basic controller configuration for the PA-MCX on the Cisco 7200 VXR platform:

Step 1   Enter configuration mode and specify that the console terminal is the source of the configuration subcommands, as follows:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Step 2   Choose a controller by entering the **controller t1 or controller e1** subcommand, followed by the interface address of the interface you plan to configure. Table 4-3 provides examples.

Table 4-3   Examples of the controller Subcommand

Platform	Command	Example

Cisco 7200 VXR routers	**controller t1**, followed by *slot/port* (port-adapter-slot-number/interface-port-number)	The example is for the first interface of a port adapterin port adapter slot 6.
		
		`Router(config)# controller t1 6/0`
		`Router(config-controller)#`

	controller e1, followed by *slot/port* (port-adapter-slot-number/interface-port-number)	The example is for the second interface of a port adapter in port adapter slot 6.
		
		`Router(config)# controller e1 6/1`
		`Router(config-controller)#`

Step 3   In controller configuration mode, enter the **framing [sf | esf]** configuration subcommand to set the framing format for T1, as in the following example:

```
Router(config-controller)# framing esf
```

Enter the **framing crc4** configuration subcommand to set the framing format for E1, as in the following example:

```
Router(config-controller)# framing crc4
```

Step 4   Enter the **linecode b8zs** subcommand to select the line coding for T1:

```
Router(config-controller)# linecode b8zs
Router(config-controller)#
```

Enter the **linecode hdb3** subcommand to select the line coding for E1:

```
Router(config-controller)# linecode hdb3
Router(config-controller)#
```

Step 5   Enter the **clock source {internal | line}** configuration subcommand to set the clock source, as in the following example:

```
router(config-controller)# clock source internal
```

Use the **no** form of this command to restore the default, line.

Step 6   Enter the **channel-group** *number* **time slots** *value* **{speed [56 | 64]}** configuration subcommand to set the channel group, as in the following example:

```
router(config-controller)# channel-group 0 timeslots 12 speed 64
```

✎

Note   The channel-group number can be from 0 to 23 and the time slot value can be from 1 to 24 for T1. The channel-group number can be from 0 to 30 and the time slot value can be from 1 to 31 for E1. The maximum number of channel groups per each eight-port PA-MCX is 128.

Step 7   Enter the **pri-group time slots** *range* configuration subcommand to set the PRI group, as in the following example:

```
router(config-controller)# pri-group timeslots 12
```

✎

Note   The channel-group number can be from 0 to 23 and the time slot value can be from 1 to 24 for T1. The channel-group number can be from 0 to 30 and the time slot value can be from 1 to 31 for E1.

Step 8   Enter the **description line** (*up to 80 characters describing this controller)* configuration subcommand to set the description, as in the following example:

```
router(config-controller)# description Arizona 3 Router; location: building 2
```

Step 9   Enter the **cablelength {long [gain26 | gain36] [0db | -7.5db | -15db | -22.5db]}** configuration subcommand to set the cable length, as in the following example:

```
router(config-controller)# cablelength long gain26 -15db
```

Enter the **no** form of this command to restore the default, gain 36, 0 dB.

Step 10   For T1 enter the **fdl {att | ansi}** configuration subcommand to set the Facility Data Link (FDL), as in the following example:

```
router(config-controller)# fdl ansi
```

Use the **no** form of this command to disable FDL.

✎

Note   The **fdl** configuration subcommand is not allowed in Super Frame mode.

Step 11   Enter the **shutdown** configuration subcommand to shut down the controller, as in the following example:

```
router(config-controller)# shutdown
```

To exit controller configuration mode and return to global configuration mode, enter the **exit** command. To exit configuration mode and return to privileged EXEC mode, use the **end** command or press **Ctrl-Z**.

Performing a Basic Data Interface Configuration

Following are instructions for a basic data interface configuration: enabling the interface and specifying IP routing. You might also need to enter other configuration subcommands, depending on the requirements for your system configuration and the protocols you plan to route on the interface. To configure a basic TDM cross-connect to a digital voice card, proceed to the "Configuring the Interface for DSPfarm" section on page 4-11. For complete descriptions of configuration subcommands and the configuration options available for serial interfaces, refer to the appropriate software documentation.

In the following procedure, press the **Return** key after each step unless otherwise noted. At any time you can exit the privileged level and return to the user level by entering **disable** at the prompt as follows:

```
Router# disable

Router>
```

Step 1 Enter configuration mode and specify that the console terminal is the source of the configuration subcommands, as follows:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Step 2 Specify the first interface to configure by entering the **interface serial** subcommand, followed by the interface address of the interface you plan to configure. Table 4-4 provides an example.

Table 4-4   Example of the interface serial Subcommand

Platform	Command	Example
Cisco 7200 VXR routers	**interface serial**, followed by *slot/port* (port-adapter-slot-number/ interface-port-number)	The example is for the first interface of a port adapter in port adapter slot 6. `Router(config)# interface serial 6/0` `Router(config-if)#`

Step 3 Assign an IP address and subnet mask to the interface with the **ip address** configuration subcommand, as in the following example:

```
Router(config-if)# ip address 10.1.15.1 255.255.255.0
Router(config-if)#
```

Step 4 Add any other interface subcommands required to enable routing protocols and adjust the interface characteristics.

Step 5 After including all of the configuration subcommands to complete your configuration, press **Ctrl-Z**—hold down the **Control** key while you press **Z**—or enter **end** or **exit** to exit configuration mode.

Step 6 Write the new configuration to NVRAM as follows:

```
Router# copy running-config startup-config
[OK]
Router#
```

This completes the procedure for creating a basic configuration.

Configuring Cyclic Redundancy Checks

Table 4-5 summarizes cyclic redundancy check (CRC) commands. For more information, see the remainder of this section.

Table 4-5   CRC Commands

Purpose	Command	Example	Further Information

Enable 32-bit CRC	**crc** *size*	The example enables 32-bit CRC on a serial interface:
		
		`Router(config)# interface serial 3/0:0`
		`Router(config-if)# crc 32`
			"Configuring Cyclic Redundancy Checks"

Return to default 16-bit CRC	**no crc** *size*	The example disables 32-bit CRC on a serial interface and returns to the default 16-bit CRC:
		
		`Router(config)# interface serial 3/0:0`
		`Router(config-if)# no crc 32`
			"Configuring Cyclic Redundancy Checks"

CRC is an error-checking technique that uses a calculated numeric value to detect errors in transmitted data. All interfaces use a 16-bit CRC (CRC-CITT) by default but also support a 32-bit CRC. The sender of a data frame calculates the frame check sequence (FCS). Before it sends a frame, the sender appends the FCS value to the message. The receiver recalculates the FCS and compares its calculation to the FCS from the sender. If there is a difference between the two calculations, the receiver assumes that a transmission error occurred and sends a request to the sender to resend the frame.

Enable 32-bit CRC using the **crc 32** command. Before you can enable 32-bit CRC, you must use the **interface serial** command (followed by the interface address of the interface) to select the interface on which you want to enable 32-bit CRC.

In the example that follows, 32-bit CRC is specified:

```
Router(config-if)# crc 32
```

Use the **no crc 32** command to disable CRC-32 and return the interface to the default CRC-16 (CRC-CITT) setting.

When you have finished, press **Ctrl-Z**—hold down the **Control** key while you press **Z**—or enter **end** or **exit** to exit configuration mode and return to the EXEC command interpreter prompt. Then write the new configuration to NVRAM using the **copy running-config startup-config** command.

For command descriptions, refer to the *Configuration Fundamentals Configuration Guide* publication. For more information, see the "Related Documentation" section on page viii.

To check the interface configuration using **show** commands, proceed to the "Checking the Configuration" section on page 4-38.

Configuring Multichannel ISDN PRI Interfaces

Following are instructions for a basic multichannel ISDN PRI configuration: enabling a controller and specifying IP routing. You might also need to enter other configuration subcommands, depending on the requirements for your system configuration and the protocols you plan to route on the interface. For complete descriptions of configuration subcommands and the configuration options available, refer to the publications listed in the "Related Documentation" section on page viii.

The PRI group must be mapped before the multichannel controller can be configured (there is only one PRI group for each controller). The following are controller commands used to map the PRI group:

- **isdn switch-type** *switch-type*

- **controller t1** *port-adapter-slot-number/port-number*

- **clock source** *line*

- **linecode** *b8zs*

- **framing** *esf*

- **loopback** [**diagnostic** | **local** | **remote**]

- **shutdown**

- **pri-group** [**timeslots** *range* {**56** | **64**}]

    The value pri-group timeslots is a number between 1 and 24 for T1 or 1 and 31 for E1. Time slots 1 to 23 represent the B channels, and time slot 24 represents the D channel for T1. Time slots 1 to 15 and 17 to 31 represent the B channels and time slot 16 represents the D channel for E1. You can enter time slots individually and separate them by commas or enter them as a range separated by a hyphen (for example, 1-3, 8, 9-18). The default DS0 speed of the PRI group is 64 kbps.

Note   If you do not specify the time slots, the controller is configured for 23 B channels (time slots 1 to 23) and one D channel (time slot 24) for T1. The controller is configured for 30 B channels and one D channel (time slot 16) for E1.

In the following procedure for a basic multichannel ISDN PRI configuration, press **Return** after each configuration step:

Step 1   At the privileged-level prompt, enter configuration mode and specify that the console terminal will be the source of the configuration subcommands:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

Step 2   Identify the ISDN switch type. In the following example, the primary-5ess switch (a switch for the United States) is identified as the switch type:

```
Router(config)# isdn switch-type primary-5ess
```

Note   The ISDN switch type that you identify is for all ISDN ports installed in the router.

Step 3   Choose a controller (T1 or E1), set the clock source, specify the framing and line code, and PRI group time slots as described in the "Configuring the Controller" section on page 4-6 and the "Performing a Basic Data Interface Configuration" section on page 4-7.

Step 4   Write the new configuration to memory:

```
Router# write memory
```

The system displays an OK message when the configuration is stored.

Step 5   Exit the privileged level and return to the user level by entering **disable** at the prompt:

```
Router# disable
```

```
Router>
```

This completes the procedure for configuring multichannel ISDN PRI interfaces. Proceed to the "Checking the Configuration" section on page 4-38 to check the interface configuration using **show** commands.

Configuring the Interface for DSPfarm

This section describes the procedure for enabling the PA-MCX interfaces to cross-connect to a digital voice port adapter for voice communications. After configuring the PA-MCX interfaces, see the "Configuring Voice over IP" section on page 4-12 for information on configuring your router for Voice over IP.

> **Note**   The PA-MCX must have a digital voice port adapter installed in the same router for it to function as a voice-enabled port adapter.

Before using the **configure** command, you must enter the privileged level of the EXEC command interpreter with the **enable** command. The system prompts you for a password if one has been set.

Use the following procedure to configure the PA-MCX interfaces. Press the **Return** key after each configuration step unless otherwise noted.

Step 1   Configure the controllers and interfaces as described in the "Configuring the Controller" section on page 4-6 and the "Performing a Basic Data Interface Configuration" section on page 4-7.

Step 2   Use the **frame-clock-select** *priority carrier-type controller* command in configuration mode to specify the clock source. This command may be used to specify backup clock sources, as shown in the example below:

```
Router(config)# frame-clock-select 1 T1 1/0
Router(config)# frame-clock-select 2 T1 1/1
```

The example above assigns T1 1/0 as the primary clock source. If that clock fails, T1 1/1 becomes the primary clock source.

Step 3   Use the **ds0-group** *number* **timeslots** *range* **type** command to create DS0 groups.

```
Router(config-controller)# ds0-group 1 timeslots 1-24 type e&m-wink-start
```

> **Note**   The time slot range for a T1 card is 1 to 24; the time slot range for an E1 card is 1 to 30.

Step 4   Change the shutdown state to up and enable the interface:

```
Router(config-controller)# no shutdown
```

The **no shutdown** command passes an **enable** command to the PA-MCX port adapter. It also causes the PA-MCX port adapter to configure itself based on the previous configuration commands sent.

Configuring Voice over IP

Voice over IP (VoIP) enables a Cisco 7200 VXR router to carry voice traffic (for example, telephone calls and faxes) over an IP network.

Voice over IP offers the following benefits:

- Toll bypass
- Remote PBX presence over WANs
- Unified voice and data trunking
- Plain Old Telephone Service (POTS)-Internet telephony gateways

Prerequisite Tasks

Before you can configure your Cisco 7200 series, Cisco 7200 VXR, or Cisco 7500 series router to use Voice over IP, you must first:

- Establish a working IP network. For more information about configuring IP, refer to the "IP Overview" and "IP Addressing and Services" chapters in the Cisco IOS Release 12.0 *Network Protocols Configuration Guide, Part 1*.
- Install the PA-MCX port adapter in your router.
- Ensure that a PA-VXB or PA-VXC port adapter is installed in your router.
- Complete your company's dial plan.
- Establish a working telephony network based on your company's dial plan.
- Integrate your dial plan and telephony network into your existing IP network topology. Merging your IP and telephony networks depends on your particular IP and telephony network topology. In general, we recommend the following suggestions:
  - Use canonical numbers wherever possible. It is important to avoid situations where numbering systems are significantly different on different routers or access servers in your network.
  - Make routing or dialing transparent to the user—for example, avoid secondary dial tones from secondary switches, where possible.
  - Contact your PBX vendor for instructions about how to reconfigure the appropriate PBX interfaces.

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

How Voice over IP Handles a Typical Telephone Call

Before configuring Voice over IP on your Cisco 7200 series, Cisco 7200 VXR, or Cisco 7500 series router, it helps to understand what happens at an application level when you place a call using Voice over IP. The general flow of a two-party voice call using Voice over IP is as follows:

1. The user picks up the handset; this signals an off-hook condition to the signaling application part of Voice over IP in the Cisco 7200 series, Cisco 7200 VXR, or Cisco 7500 series router.

2. The session application part of Voice over IP issues a dial tone and waits for the user to dial a telephone number.

3. The user dials the telephone number; those numbers are accumulated and stored by the session application.

4. After enough digits are accumulated to match a configured destination pattern, the telephone number is mapped to an IP host through the dial plan mapper. The IP host has a direct connection to either the destination telephone number or a PBX that is responsible for completing the call to the configured destination pattern.

5. The session application then runs the H.323 session protocol to establish a transmission and a reception channel for each direction over the IP network. If the call is being handled by a PBX, the PBX forwards the call to the destination telephone. If Resource Reservation Protocol (RSVP) has been configured, the RSVP reservations are put into effect to achieve the desired quality of service over the IP network.

6. The codecs are enabled for both ends of the connection and the conversation proceeds using Real-Time Transport Protocol/User Datagram Protocol/Internet Protocol (RTP/UDP/IP) as the protocol stack.

7. Any call-progress indications (or other signals that can be carried in-band) are cut through the voice path as soon as an end-to-end audio channel is established. Signaling that can be detected by the voice ports (for example, in-band DTMF digits after the call setup is complete) is also trapped by the session application at either end of the connection and carried over the IP network encapsulated in Real-Time Conferencing Protocol (RTCP) using the RTCP Advanced Peer-to-Peer Networking (APPN) extension mechanism.

8. When either end of the call hangs up, the RSVP reservations are torn down (if RSVP is used) and the session ends. Each end becomes idle, waiting for the next off-hook condition to trigger another call setup.

Configuration Tasks

To configure Voice over IP on the Cisco 7200 series, Cisco 7200 VXR, or Cisco 7500 series router, you need to perform the following steps:

Step 1   Configure your IP network to support real-time voice traffic. Fine-tuning your network to adequately support VoIP involves a series of protocols and features geared toward quality of service (QoS). To configure your IP network for real-time voice traffic, you need to take into consideration the entire scope of your network, and then select and configure the appropriate QoS tool or tools:

- RSVP
- Multilink PPP with interleaving
- RTP header compression
- Custom queuing
- Weighted fair queuing

See the "Configuring IP Networks for Real-Time Voice Traffic" section on page 4-15 for information about how to select and configure the appropriate QoS tools to optimize voice traffic on your network.

Step 2   (Optional.) If you plan to run Voice over IP over Frame Relay, you need to take certain factors into consideration when configuring Voice over IP for it to run smoothly over Frame Relay. For example, a public Frame Relay cloud provides no guarantees for QoS. See the "Configuring Voice over Frame Relay" section on page 4-37 for information about deploying Voice over IP over Frame Relay.

Step 3   Use the **num-exp** command to configure number expansion if your telephone network is configured so that you can reach a destination by dialing only a portion (an extension number) of the full E.164 telephone number. See the "Configuring Number Expansion" section on page 4-20 for information about number expansion.

Step 4   Use the **dial-peer voice** command to define dial peers and switch to the dial-peer configuration mode. Each dial peer defines 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 router, and two from the perspective of the destination router. Dial peers are used to apply attributes to call legs and to identify call origin and destination. There are two different kinds of dial peers:

- 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. To minimally configure a POTS dial peer, you need to configure the following two characteristics: associated telephone number and logical interface. Use the **destination-pattern** command to associate a telephone number with a POTS peer. Use the **port** command to associate a specific logical interface with a POTS peer. In addition, you can specify direct inward dialing for a POTS peer by using the **direct-inward-dial** command.

- VoIP—Dial peer describing the characteristics of a packet network connection; in the case of Voice over IP, this is an IP network. VoIP peers point to specific VoIP devices. To minimally configure a VoIP peer, you need to configure the following two characteristics: associated destination telephone number and a destination IP address. Use the **destination-pattern** command to define the destination telephone number associated with a VoIP peer. Use the **session-target** command to specify a destination IP address for a VoIP peer.

In addition, you can use VoIP peers to define characteristics such as IP precedence, additional QoS parameters (when RSVP is configured), codec, and voice activity detection (VAD). Use the **ip precedence** command to define IP precedence. If you have configured RSVP, use either the **req-qos** or **acc-qos** command to configure QoS parameters. Use the **codec** command to configure specific voice coder rates. Use the **vad** command to disable voice activation detection and the transmission of silence packets.

See the "Configuring Dial Peers" section on page 4-21 and the "Optimizing Dial Peer and Network Interface Configurations" section on page 4-34 for additional information about configuring dial peers and dial-peer characteristics.

Step 5   You need to configure your router to support voice ports. In general, voice-port commands define the characteristics associated with a particular voice-port signaling type. Voice ports on the Cisco 7200 series, Cisco 7200 VXR, and Cisco 7500 series routers support three basic voice signaling types:

- FXO—Foreign Exchange Office interface
- FXS—Foreign Exchange Station interface
- E&M—"RecEive and TransMit" interface, or the "Ear and Mouth" interface

Under most circumstances, the default voice-port command values are adequate to configure FXO and FXS ports to transport voice data over your existing IP network. Because of the inherent complexities involved with PBX networks, E&M ports might need specific voice-port values configured, depending on the specifications of the devices in your telephony network. For information about configuring voice ports, see the "Configuring Voice Ports" section on page 4-27.

Configuring IP Networks for Real-Time Voice Traffic

You need to have a well-engineered network end-to-end when you run delay-sensitive applications such as VoIP. Fine-tuning your network to adequately support VoIP involves a series of protocols and features geared toward quality of service (QoS). It is beyond the scope of this document to explain the specific details relating to wide-scale QoS deployment. Cisco IOS software provides many tools for enabling QoS on your backbone, such as random early detection (RED), weighted random early detection (WRED), fancy queuing (meaning custom, priority, or weighted fair queuing), and IP precedence. To configure your IP network for real-time voice traffic, you must consider the entire scope of your network, and then select the appropriate QoS tool or tools.

The important thing to remember is that QoS must be configured throughout your network—not just on the Cisco 7200 series, Cisco 7200 VXR, or Cisco 7500 series router running VoIP—to improve voice network performance. Not all QoS techniques are appropriate for all network routers. Edge routers and backbone routers in your network do not necessarily perform the same operations; the QoS tasks they perform might differ as well. To configure your IP network for real-time voice traffic, you need to take into consideration the functions of both edge and backbone routers in your network, and then select the appropriate QoS tool or tools.

In general, edge routers perform the following QoS functions:

- Packet classification
- Admission control
- Bandwidth management
- Queuing

In general, backbone routers perform the following QoS functions:

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

Scalable QoS solutions require cooperative edge and backbone functions.

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

- Configuring RSVP for Voice, page 4-15
- Configuring Multilink PPP with Interleaving, page 4-17
- Configuring RTP Header Compression, page 4-18
- Configuring Custom Queuing, page 4-19
- Configuring Weighted Fair Queuing, page 4-20

Each of these tasks is discussed in the following sections.

Configuring RSVP for Voice

RSVP allows end systems to request a particular quality of service (QoS) from the network. Real-time voice traffic requires network consistency. Without consistent QoS, real-time traffic can experience jitter, insufficient bandwidth, delay variations, or information loss. RSVP works in conjunction with current queuing mechanisms. It is up to the interface queuing mechanism (such as weighted fair queuing or weighted random early detection) to implement the reservation.

RSVP can be equated to a dynamic access list for packet flows.

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

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

Enable RSVP

To minimally configure RSVP for voice traffic, you must enable RSVP on each interface where priority needs to be set.

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

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

This command starts RSVP and sets the bandwidth and single-flow limits. The default maximum bandwidth is up to 75 percent of the bandwidth available on the interface. By default, the amount reservable by a flow can be up to the entire reservable bandwidth.

On subinterfaces, this command applies the more restrictive of the available bandwidths of the physical interface and the subinterface.

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

Cisco 7200 series, Cisco 7200 VXR, and Cisco 7500 series routers running VoIP and configured for RSVP request allocations according to the following formula:

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

For G.729, the allocation is 24,000 bps. For G.711, the allocation is 80,000 bps.

RSVP Configuration Example

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

```
interface DSPfarm 1/0/0
 ip rsvp bandwidth 100 32
 fair-queue
 end
!
dial-peer voice 1211 voip
 req-qos controlled-load
!
dial-peer voice 1212 voip
 req-qos controlled-load
```

Configuring Multilink PPP with Interleaving

Multiclass Multilink PPP interleaving allows large packets to be multilink-encapsulated and fragmented into smaller packets to satisfy the delay requirements of real-time voice traffic; small real-time packets, which are not multilink-encapsulated, are transmitted between fragments of the large packets. The interleaving feature also provides a special transmit queue for the smaller, delay-sensitive packets, enabling them to be transmitted earlier than other flows. Interleaving provides the delay bounds for delay-sensitive voice packets on a slow link that is used for other best-effort traffic.

Note   Interleaving applies only to interfaces that can configure a multilink bundle interface. These include virtual templates, dialer interfaces, and ISDN BRI or PRI interfaces.

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

You should configure Multilink PPP if the following conditions exist in your network:

- Point-to-point connection using PPP encapsulation
- Slow links

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

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

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

To configure Multilink PPP and interleaving on a configured and operational interface or virtual interface template, use the following commands in interface mode:

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

Note   The **ip rtp reserve** command can be used instead of configuring RSVP. If you configure RSVP, this command is not required.

For more information about Multilink PPP, refer to the "Configuring Media-Independent PPP and Multilink PPP" chapter in the Cisco IOS Release 12.0 *Dial Solutions Configuration Guide*.

Multilink PPP Configuration Example

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

```
interface virtual-template 1
 ppp multilink
 encapsulated ppp
 ppp multilink interleave
 ppp multilink fragment-delay 20
 ip rtp reserve 16384 100 64

multilink virtual-template 1
```

Configuring RTP Header Compression

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

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

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

Figure 4-1   RTP Header Compression

Before RTP header compression:

After RTP header compression:
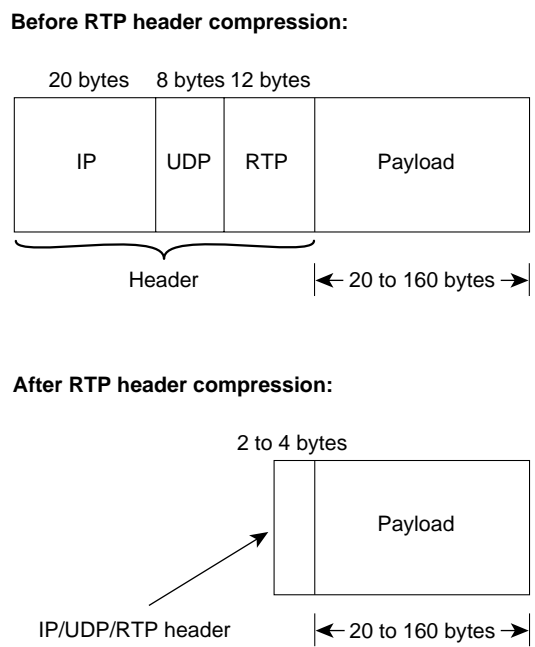
You should configure RTP header compression if the following conditions exist in your network:

- Slow links
- Need to save bandwidth

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

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

- Enabling RTP Header Compression on a Serial Interface
- Changing the Number of Header Compression Connections

Enabling RTP Header Compression on a Serial Interface

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

ip rtp header-compression [**passive**]

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

Changing the Number of Header Compression Connections

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

ip rtp compression connections *number*

RTP Header Compression Configuration Example

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

```
interface serial 0
 ip rtp header-compression
 encapsulation ppp
 ip rtp compression-connections 25
```

Configuring Custom Queuing

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

```
16384 = 4(number of voice ports in the Cisco 7200 VXR router)
```

Custom queuing and other methods for identifying high-priority streams should be configured for these port ranges.

Configuring Weighted Fair Queuing

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

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

Configuring Number Expansion

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

Creating a Number Expansion Table

In the example in Figure 4-2, a small company wants to use Voice over IP to integrate its telephony network with its existing IP network. The destination pattern (or expanded telephone number) associated with Router A (located to the left of the IP cloud) is (408) 555-xxxx, where xxxx identifies the individual dial peers by extension. The destination pattern (or expanded telephone number) associated with Router B (located to the right of the IP cloud) is (729) 411-xxxx.

Figure 4-2   Sample Voice over IP Network
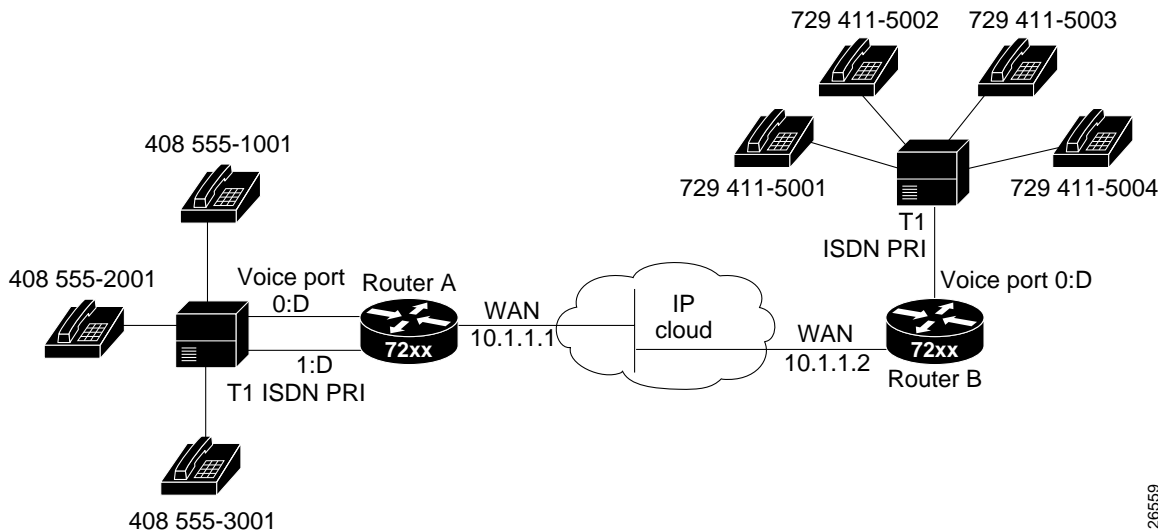
Table 4-6 shows the number expansion table for this scenario.

Table 4-6   Sample Number Expansion Table

Extension	Destination Pattern	Num-Exp Command Entry
1001	4085551001	num-exp 1001 4085551001
2001	4085552001	num-exp 2001 4085552001
3...	4085553...	num-exp 3... 4085553...
5001	7294115001	num-exp 5001 7294115001
5002	7294115002	num-exp 5002 7294115002
5...	7294115...	num-exp 5... 7294115...

Note   You can use the period symbol (.) to represent variables (such as extension numbers) in a telephone number.

The information included in this example needs to be configured on both Router A and Router B.

Expanding a Number

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

```
num-exp extension-number extension-string
```

You can verify the number expansion information by using the **show num-exp** command to verify that you have mapped the telephone numbers correctly.

After you have configured dial peers and assigned destination patterns to them, you can verify number expansion information by using the **show dialplan number** command to see how a telephone number maps to a dial peer.

Configuring Dial Peers

The key point to understanding how Voice over IP functions is to understand dial peers. Each dial peer defines the characteristics associated with a call leg, as shown in Figure 4-3 and Figure 4-4. A call leg is a discrete segment of a call connection that lies between two points in the connection. All of the call legs for a particular connection have the same connection ID.

There are two different kinds of dial peers:

- 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.

- VoIP—Dial peer describing the characteristics of a packet network connection; in the case of Voice over IP, this is an IP network. VoIP peers point to specific VoIP devices.

An end-to-end call comprises four call legs, two from the perspective of the source router as shown in Figure 4-3, and two from the perspective of the destination router as shown in Figure 4-4. A dial peer is associated with each one of these call legs. Dial peers are used to apply attributes to call legs and to identify call origin and destination. Attributes applied to a call leg include QoS, codec, VAD, and fax rate.

Figure 4-3   Dial Peer Call Legs from the Perspective of the Source Router
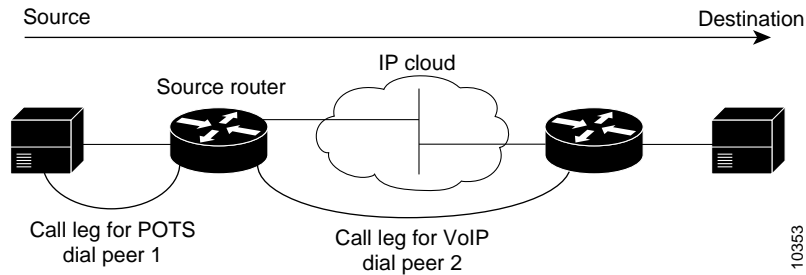
Figure 4-4   Dial Peer Call Legs from the Perspective of the Destination Router
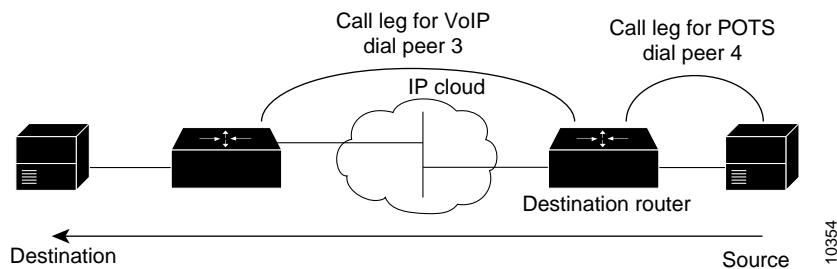
Inbound Versus Outbound Dial Peers

Dial peers are used for both inbound and outbound call legs. It is important to remember that these terms are defined from the *router's* perspective. An inbound call leg originates *outside* the router. An outbound call leg originates *from* the router.

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

POTS peers associate a telephone number with a particular voice port so that incoming calls for that telephone number can be received and outgoing calls can be placed. VoIP peers point to specific devices (by associating destination telephone numbers with a specific IP address) so that incoming calls can be received and outgoing calls can be placed. Both POTS and VoIP peers are needed to establish Voice over IP connections.

Establishing communication using Voice over IP is similar to configuring an IP static route; you are establishing a specific voice connection between two defined endpoints. As shown in Figure 4-5, for outgoing calls (from the perspective of the POTS dial peer 1), the POTS dial peer establishes the source (through the originating telephone number or voice port) of the call. The VoIP dial peer establishes the destination by associating the destination telephone number with a specific IP address.

Figure 4-5   Outgoing Calls from the Perspective of POTS Dial Peer 1
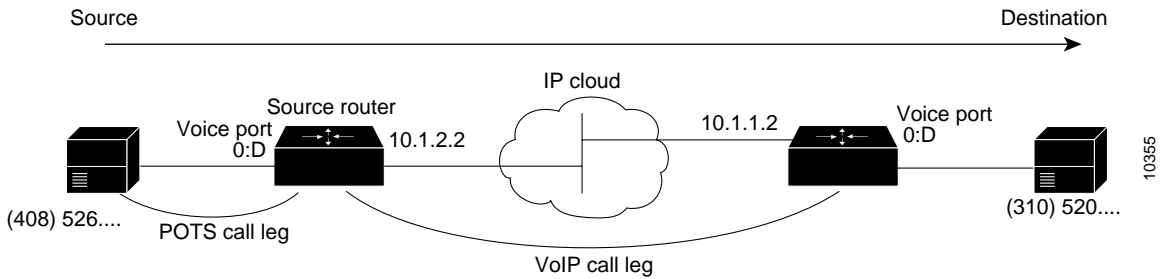
To configure call connectivity between the source and destination as illustrated in Figure 4-5, enter the following commands on router 10.1.2.2:

```
dial-peer voice 1 pots
 destination-pattern 1408526....
 port 1/0/0

dial-peer voice 2 voip
 destination-pattern 1310520....
 session target ipv4:10.1.1.2
```

In the previous configuration example, the last four digits in the VoIP dial peer's destination pattern were replaced with wildcards. This means that from router 10.1.2.2, calling any number string that begins with the digits "1310520" results in a connection to router 10.1.1.2. This implies that router 10.1.1.2 services all numbers beginning with those digits. From router 10.1.1.2, calling any number string that begins with the digits "1408526" will result in a connection to router 10.1.2.2. This implies that router 10.1.2.2 services all numbers beginning with those digits. For more information about stripping and adding digits, see the "Outbound Dialing on POTS Peers" section on page 4-25.

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

Figure 4-6   Outgoing Calls from the Perspective of POTS Dial Peer 2
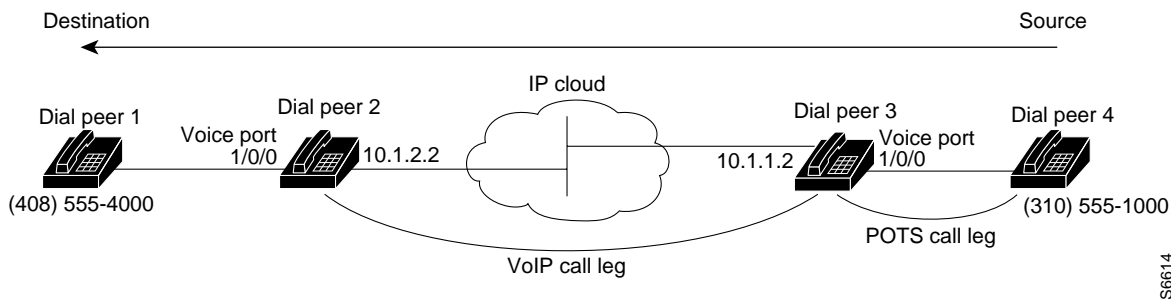
To complete the end-to-end call between dial peer 1 and dial peer 4 as illustrated in Figure 4-6, enter the following commands on router 10.1.1.2:

```
dial-peer voice 4 pots
 destination-pattern 1310555....
 port 1/0/0

dial-peer voice 3 voip
 destination-pattern 1408555....
 session target ipv4:10.1.2.2
```

Creating a Peer Configuration Table

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

Using the example in Figure 4-2, Router A, with an IP address of 10.1.1.1, connects a small sales branch office to the main office through Router B. There are three telephones in the sales branch office that need to be established as dial peers. Router B, with an IP address of 10.1.1.2, is the primary gateway to the main office; as such, it needs to be connected to the company's PBX. There are four devices that need to be established as dial peers in the main office, all of which are basic telephones connected to the PBX. Figure 4-2 shows a diagram of this small voice network.

Table 4-7 shows the peer configuration table for the example illustrated in Figure 4-2.

Table 4-7   Peer Configuration Table for Sample Voice over IP Network

| Dial Peer Tag | Ext | Commands | | | | |
		Dest-Pattern	Type	Session-Target	Codec	QoS
Router A						
1	6....	+1408555....	POTS			
10		+1729411....	VoIP	IPV4 10.1.1.2	G.729	Best Effort
Router B						
11		+1408555....	VoIP	IPV4 10.1.1.1	G.729	Best Effort
4	2....	+1729411....	POTS			

Configuring POTS Peers

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

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

```
dial-peer voice number pots
```

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

To configure the identified POTS peer, use the following commands in dial-peer configuration mode:

	Command	Purpose
Step 1	**destination-pattern** *string*	Define the telephone number associated with this POTS dial peer.
Step 2	**port** *controller number***:D**	Associate this POTS dial peer with a specific logical dial interface.

Outbound Dialing on POTS Peers

When a router receives a voice call, it selects an outbound dial peer by comparing the called number (the full E.164 telephone number) in the call information with the number configured as the destination pattern for the POTS peer. The router then strips out the left-justified numbers corresponding to the destination pattern matching the called number. If you have configured a prefix, the prefix will be put in front of the remaining numbers, creating a dial string, which the router will then dial. If all numbers in the destination pattern are stripped out, the user receives (depending on the attached equipment) a dial tone.

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

Direct Inward Dial for POTS Peers

Direct inward dial (DID) is used to determine how the called number is treated for incoming POTS call legs. As shown in Figure 4-7, incoming means from the perspective of the router. In this case, it is the call leg coming into the router to be forwarded through to the appropriate destination pattern.

Figure 4-7   Incoming and Outgoing POTS Call Legs
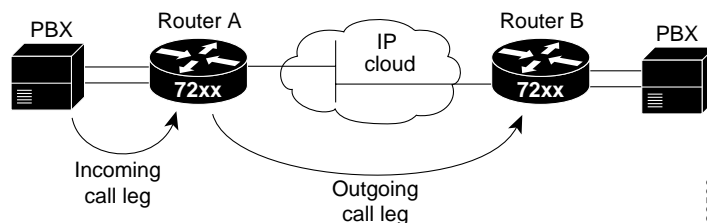
Unless otherwise configured, when a call arrives on the router, the router presents a dial tone to the caller and collects digits until it can identify the destination dial peer. After the dial peer has been identified, the call is forwarded through the next call leg to the destination.

There are cases when it might be necessary for the router to use the called number Dialed Number Identification Service (DNIS) to find a dial peer for the outgoing call leg—for example, if the switch connecting the call to the router has already collected the digits. DID enables the router to match the called number with a dial peer and then directly place the outbound call. With DID, the router does not present a dial tone to the caller and does not collect digits; it forwards the call directly to the configured destination.

To use DID and an incoming called number, a dial peer must be associated with the incoming call leg. It is helpful to understand the logic behind the algorithm used to associate the incoming call leg with the dial peer.

The algorithm used to associate incoming call legs with dial peers uses three inputs (which are derived from signaling and interface information associated with the call) and four defined dial peer elements. The three signaling inputs are:

• Called number (DNIS)—Set of numbers representing the destination, which is derived from the ISDN setup message or CAS DNIS.

- Calling number (ANI)—Set of numbers representing the origin, which is derived from the ISDN setup message or CAS DNIS.

- Voice port—Voice port carrying the call.

The four defined dial peer elements are:

- Destination pattern—Pattern representing the phone numbers to which the peer can connect.

- Answer address—Pattern representing the phone numbers from which the peer can connect.

- Incoming called number—Pattern representing the phone numbers that associate an incoming call leg to a peer based on the called number or DNIS.

- Port—Port through which calls to this peer are placed.

Using the elements, the algorithm is as follows:

```
For all peers where call type (VoIP versus POTS) matches dial peer type:
if the type is matched, associate the called number with the incoming called-number
 else if the type is matched, associate calling-number with answer-address
 else if the type is matched, associate calling-number with destination-pattern
 else if the type is matched, associate voice port to port
```

This algorithm shows that if a value is not configured for answer address, the origin address is used because, in most cases, the origin address and answer address are the same.

To configure DID for a particular POTS dial peer, use the following commands, initially in global configuration mode:

	Command	Purpose
Step 1	**dial-peer voice** *number* **pots**	Enter the dial-peer configuration mode to configure a POTS peer.
Step 2	**direct-inward-dial**	Specify direct inward dial for this POTS peer.

Note   Direct inward dial is configured for the calling POTS dial peer.

Configuring VoIP Peers

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

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

```
dial-peer voice number voip
```

The *number* value of the **dial-peer voice voip** command is a tag that uniquely identifies the dial peer.

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

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

Verifing Configuration

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

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

- Use the **show dialplan number** command to show the dial peer to which a particular number (destination pattern) resolves.

Tips

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

- Ping the associated IP address to confirm connectivity.

- Use the **show dial-peer voice** command to verify that the operational status of the dial peer is up.

- Use the **show dialplan number** command on the local and remote routers to verify that the data is configured correctly on both.

- If you have configured number expansion, use the **show num-exp** command to check that the partial number on the local router maps to the correct full E.164 telephone number on the remote router.

- If you have configured a codec value, there can be a problem if both VoIP dial peers on either side of the connection have incompatible codec values. Make sure that both VoIP peers have been configured with the same codec value.

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

- Use the **debug cch323 rtp** command to check RTP packet transport.

- Use the **debug cch323 h225** command to check the call setup.

Configuring Voice Ports

Voice ports on Cisco 7200 series, Cisco 7200 VXR, and Cisco 7500 series routers support three basic voice signaling types:

- FXO—Foreign Exchange Office interface. The FXO interface allows a connection to be directed to the PSTN's central office (or to a standard PBX interface, if the local telecommunications authority permits). This interface is of value for off-premises extension applications.

- FXS—The Foreign Exchange Station interface allows connection for basic telephone equipment, key sets, and PBXs, and supplies ring, voltage, and dial tone.

- E&M—The "Ear and Mouth" interface (or "RecEive and TransMit" interface) allows connection for PBX trunk lines (tie lines). It is a signaling technique for two-wire and four-wire telephone and trunk interfaces.

In general, voice-port commands define the characteristics associated with a particular voice-port signaling type. Under most circumstances, the default voice-port command values are adequate to configure FXO and FXS ports to transport voice data over your existing IP network. Because of the inherent complexities involved with PBX networks, E&M ports might need specific voice-port values configured, depending on the specifications of the devices in your telephony network.

Configuring FXO or FXS Voice Ports

Under most circumstances, the default voice-port values are adequate for both FXO and FXS voice ports. If you need to change the default configuration for these voice ports, perform the following tasks. Items included in Step 1 and Step 2 are required; items included in Step 3 are optional.

Step 1   Identify the voice port and enter the voice-port configuration mode by using the **voice-port** command.

Step 2   Configure the following mandatory voice-port parameters by using the indicated commands:

- Dial type (FXO only) using the **dial-type** command
- Signal type using the **signal** command
- Call progress tone using the **cptone** command
- Ring frequency (FXS only) using the **ring frequency** command
- Ring number (FXO only) using the **ring number** command

Step 3   Configure one or more of the following optional voice-port parameters by using the indicated commands:

- PLAR connection mode using the **connection plar** command
- Music threshold using the **music-threshold** command
- Description using the **description** command
- Comfort noise (if VAD is activated—VAD is a dial-peer command) using the **comfort-noise** command

To configure FXO and FXS voice ports, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal**	Enter the global configuration mode.
Step 2	**voice-port** *slot-number/subunit-number/port*	Identify the voice port you want to configure and enter the voice-port configuration mode.
Step 3	**dial-type** {**dtmf**	**pulse**}	(For FXO ports only.) Select the appropriate dial type for out-dialing.
Step 4	**signal** {**loop-start**	**ground-start**}	Select the appropriate signal type for this interface.

	Command	Purpose
Step 5	**cptone** *country*	Select the appropriate voice call progress tone for this interface.
		The default for this command is **us**. For a list of supported countries, refer to the *Voice, Video, and Home Applications Command Reference*.
Step 6	**ring number** *number*	(For FXO ports only.) Specify the maximum number of rings to be detected before answering a call.
Step 7	**connection plar** *string*	(Optional.) Specify the Private Line Auto Ringdown (PLAR) connection if this voice port is used for a PLAR connection. The *string* value specifies the destination telephone number.
Step 8	**music-threshold** *number*	(Optional.) Specify the threshold (in decibels) for on-hold music. Valid entries are from –70 to –30.
Step 9	**description** *string*	(Optional.) Attach descriptive text about this voice-port connection.
Step 10	**comfort-noise**	(Optional.) Specify that background noise will be generated.

Validation Tips

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

- Pick up the handset of an attached telephony device and check for a dial tone.

- If you have dial tone, check for dual tone multifrequency (DTMF) detection. If the dial tone stops when you dial a digit, then the voice port is most likely configured properly.

- Use the **show voice-port** command to verify that the data configured is correct.

Troubleshooting Tips

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

- Ping the associated IP address to confirm connectivity.

- Use the **show voice-port** command to make sure that the port is enabled. If the port is offline, use the **no shutdown** command.

- If you have configured E&M interfaces, make sure that the values pertaining to your specific PBX setup, such as timing or type, are correct.

- Check to see if the voice network module has been correctly installed. For more information, refer to the installation document *Voice Network Module and Voice Interface Card Configuration Note* that came with your voice network module.

Fine-Tuning FXO and FXS Voice Ports

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

Note   In most cases, the default values for voice-port tuning commands are sufficient.

To configure voice-port tuning for FXO and FXS voice ports, perform the following steps:

Step 1 Identify the voice port and enter the voice-port configuration mode using the **voice-port** command.

Step 2 For each of the following parameters, select the appropriate value using the commands indicated:

- Input gain using the **input gain** command
- Output attenuation using the **output attenuation** command
- Echo cancel coverage using the **echo-cancel enable** and **echo-cancel coverage** commands
- Nonlinear processing using the **non-linear** command
- Initial digit timeouts using the **timeouts initial** command
- Interdigit timeouts using the **timeouts interdigits** command
- Timing other than timeouts, using the **timing digit**, **timing inter-digit**, **timing pulse-digit**, and **timing pulse-inter-digit** commands

To fine-tune FXO or FXS voice ports, use the following commands beginning in privileged EXEC mode:

:

	Command	Purpose
Step 1	**configure terminal**	Enter the global configuration mode.
Step 2	**voice-port** *slot-number/subunit-number/port*	Identify the voice port you want to configure and enter the voice-port configuration mode.
Step 3	**echo-cancel enable**	Enable echo cancellation of voice that is sent out the interface and received back on the same interface.
Step 4	**echo-cancel coverage** *value*	Adjust the size (in milliseconds) of the echo cancel. Acceptable values are 16, 24, and 32.
Step 5	**non-linear**	Enable nonlinear processing, which shuts off any signal if no near-end speech is detected. (Nonlinear processing is used with echo cancellation.)
Step 6	**timeouts initial** *seconds*	Specify the number of seconds the system waits for the caller to input the first digit of the dialed digits. Valid entries for this command are from 0 to 120.
Step 7	**timeouts interdigit** *seconds*	Specify the number of seconds the system will wait (after the caller has input the initial digit) for the caller to input a subsequent digit. Valid entries for this command are from 0 to 120.
Step 8	**timing digit** *milliseconds*	If the voice-port dial type is DTMF, configure the DTMF digit signal duration. The range of the DTMF digit signal duration is from 50 to 100. The default is 100.
Step 9	timing inter-digit *milliseconds*	If the voice-port dial type is DTMF, configure the DTMF interdigit signal duration. The range of the DTMF interdigit signal duration is from 50 to 500. The default is 100.

	Command	Purpose
Step 10	**timing pulse-digit** *milliseconds*	(FXO ports only.) If the voice-port dial type is pulse, configure the pulse digit signal duration. The range of the pulse digit signal duration is from 10 to 20. The default is 20.
Step 11	**timing pulse-inter-digit** *milliseconds*	(FXO ports only.) If the voice-port dial type is pulse, configure the pulse interdigit signal duration. The range of the pulse interdigit signal duration is from 100 to 1000. The default is 500.

Note After you change any voice-port command, it is a good idea to cycle the port by using the **shutdown** and **no shutdown** commands.

Configuring E&M Voice Ports

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

To configure an E&M voice port, perform the following steps. Items included in Step 1 and Step 2 are required; items included in Step 3 are optional.

Step 1   Identify the voice port and enter the voice-port configuration mode using the **voice-port** command.

Step 2   For each of the following required parameters, select the appropriate parameter value using the commands indicated:

- Dial type using the **dial-type** command
- Signal type using the **signal** command
- Call progress tone using the **cptone** command
- Operation using the **operation** command
- Type using the **type** command
- Impedance using the **impedance** command

Step 3   Select one or more of the following optional parameters, using the indicated commands:

- Connection mode using the **connection plar** command
- Music threshold using the **music-threshold** command
- Description using the **description** command
- Comfort tone (if VAD is activated) using the **comfort-noise** command

To configure E&M voice ports, use the following commands beginning in privileged EXEC mode:

	Command	Purpose
Step 1	**configure terminal**	Enter the global configuration mode.
Step 2	**voice-port** *slot-number/subunit-number/port*	Identify the voice port you want to configure and enter the voice-port configuration mode.

	Command	Purpose
Step 3	dial-type {dtmf	pulse}	Select the appropriate dial type for out-dialing.
Step 4	signal {wink-start	immediate	delay-dial}	Select the appropriate signal type for this interface.
Step 5	cptone {australia	brazil	china	finland	france	germany	japan	northamerica	unitedkingdom}	Select the appropriate voice call progress tone for this interface.
Step 6	connection plar *string*	(Optional.) Specify the Private Line Auto Ringdown (PLAR) connection if this voice port is used for a PLAR connection. The *string* value specifies the destination telephone number.
Step 7	music-threshold *number*	(Optional.) Specify the threshold (in decibels) for on-hold music. Valid entries are from –70 to –30.
Step 8	description *string*	(Optional.) Attach descriptive text about this voice port connection.
Step 9	comfort-noise	(Optional.) Specify that background noise will be generated.

Validation Tips

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

- Pick up the handset of an attached telephony device and check for a dial tone.

- If you have a dial tone, check for DTMF detection. If the dial tone stops when you dial a digit, then the voice port is most likely configured properly.

- Use the **show voice-port** command to verify that the data configured is correct.

Troubleshooting Tips

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

- Ping the associated IP address to confirm connectivity.

- Use the **show voice-port command** to make sure that the port is enabled. If the port is offline, use the **no shutdown** command.

- If you have configured E&M interfaces, make sure that the values pertaining to your specific PBX setup, such as timing or type, are correct.

- Check to see if the voice network module has been correctly installed. For more information, refer to the installation document *Voice Network Module and Voice Interface Card Configuration Note* that came with your voice network module.

Fine-Tuning E&M Voice Ports

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

Note In most cases, the default values for voice-port tuning commands are sufficient.

To configure voice-port tuning for E&M voice ports, perform the following steps:

Step 1 Identify the voice port and enter the voice-port configuration mode by using the **voice-port** command.

Step 2 For each of the following parameters, select the appropriate value, using the commands indicated:

- Input gain using the **input gain** command
- Output attenuation using the **output attenuation** command
- Echo cancel coverage using **echo-cancel enable** and **echo-cancel coverage** commands
- Nonlinear processing using the **non-linear** command
- Initial digit timeouts using the **timeouts initial** command
- Interdigit timeouts using the **timeouts interdigit** command
- Timing other than timeouts using the **timing clear-wait**, **timing delay-duration**, **timing delay-start**, **timing dial-pulse min-delay**, **timing digit**, **timing inter-digit**, **timing pulse**, **timing pulse-inter-digit**, **timing wink-duration**, and **timing wink-wait** commands

To fine-tune E&M voice ports, use the following commands beginning in privileged EXEC mode :

	Command	Purpose
Step 1	**configure terminal**	Enter the global configuration mode.
Step 2	**voice-port** *slot-number/subunit-number/port*	Identify the voice port you want to configure and enter the voice-port configuration mode.
Step 3	**echo-cancel enable**	Enable echo cancellation of voice that is sent out the interface and received back on the same interface.
Step 4	**echo-cancel coverage** *value*	Adjust the size (in milliseconds) of the echo cancel. Acceptable values are 16, 24, and 32.
Step 5	**non-linear**	Enable nonlinear processing, which shuts off any signal if no near-end speech is detected. (Nonlinear processing is used with echo cancellation.)
Step 6	**timeouts initial** *seconds*	Specify the number of seconds the system waits for the caller to input the first digit of the dialed digits. Valid entries for this command are from 0 to 120.
Step 7	**timeouts interdigit** *seconds*	Specify the number of seconds the system waits (after the caller has input the initial digit) for the caller to input a subsequent digit. Valid entries for this command are from 0 to 120.

	Command	Purpose
Step 8	**timing clear-wait** *milliseconds* **timing delay-duration** *milliseconds* **timing delay-start** *milliseconds* **timing dial-pulse min-delay** *milliseconds* **timing digit** *milliseconds* **timing inter-digit** *milliseconds* **timing pulse** *pulse-per-second* **timing pulse-inter-digit** *milliseconds* **timing wink-duration** *milliseconds* **timing wink-wait** *milliseconds*	Specify timing parameters. Valid entries for **clear-wait** are from 200 to 2000 milliseconds (ms). Valid entries for **delay-duration** are from 100 to 5000 ms. Valid entries for **delay-start** are from 20 to 2000 ms. Valid entries for **dial-pulse min-delay** are from 0 to 5000 ms. Valid entries for **digit** are from 50 to 100 ms. Valid entries for **inter-digit** are from 50 to 500 ms. Valid entries for **pulse** are from 10 to 20 ms. Valid entries for **pulse-inter-digit** are 100 to 1000 ms. Valid entries for **wink-duration** are from 100 to 400 ms. Valid entries for **wink-wait** are from 100 to 5000 ms.

Note   After you change any voice-port command, it is a good idea to cycle the port by using the **shutdown** and **no shutdown** commands.

Optimizing Dial Peer and Network Interface Configurations

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

- Configuring IP Precedence for Dial Peers
- Configuring RSVP for Dial Peers
- Configuring Codec and VAD for Dial Peers

Configuring IP Precedence for Dial Peers

If you want to give real-time voice traffic a higher priority than other network traffic, you can weight the voice data traffic associated with a particular VoIP dial peer by using IP precedence. IP precedence scales better than RSVP but provides no admission control.

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

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

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

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

```
dial-peer voice 103 voip
 ip precedence 5
```

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

Configuring RSVP for Dial Peers

If you have configured your WAN or LAN interfaces for RSVP, you must configure the QoS for any associated VoIP peers. To configure quality of service for a selected VoIP peer, use the following commands, beginning in global configuration mode:

	Command	Purpose
Step 1	**dial-peer voice** *number* **voip**	Enter the dial-peer configuration mode to configure a VoIP peer.
Step 2	**req-qos** [**best-effort** | **controlled-load** | **guaranteed-delay**]	Specify the desired quality of service to be used.

Note   We suggest that you select **controlled-load** for the requested quality of service.

For example, to specify guaranteed delay QoS for VoIP dial peer 108, enter the following:

```
dial-peer voice 108 voip
 destination-pattern +1408528
 req-qos guaranteed-delay
 session target ipv4:10.0.0.8
```

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

To generate an SNMP trap message if the reserved QoS is less than the configured value for a selected VoIP peer, use the following commands, beginning from the global configuration mode:

	Command	Purpose
Step 1	**dial-peer voice** *number* **voip**	Enter the dial-peer configuration mode to configure a VoIP peer.
Step 2	**acc-qos** [**best-effort** | **controlled-load** | **guaranteed-delay**]	Specify the QoS value below which an SNMP trap will be generated.

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

Configuring Codec and VAD for Dial Peers

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

Configuring Codec for a VoIP Dial Peer

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

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

The default for the **codec** command is **g729r8**; normally the default configuration for this command is the most desirable. If, however, you are operating on a high-bandwidth network and voice quality is of the highest importance, you should configure the **codec** command for **g711alaw** or **ulaw**. Using this value results in better voice quality, but it also requires higher bandwidth requirements for voice.

For example, to specify a codec rate of G.711a-law for VoIP dial peer 108, enter the following:

```
dial-peer voice 108 voip
 destination-pattern +1408528
 codec g711alaw
 session target ipv4:10.0.0.8
```

Configuring VAD for a VoIP Dial Peer

To disable the transmission of silence packets for a selected VoIP peer, use the following commands, beginning in global configuration mode:

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

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

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

```
dial-peer voice 108 voip
destination-pattern +1408528
vad
session target ipv4:10.0.0.8
```

Configuring Voice over Frame Relay

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

For Frame Relay links with slow output rates (less than or equal to 64 kbps), where data and voice are being transmitted over the same PVC, we recommend the following solutions:

- Separate DLCIs for voice and data—By providing a separate subinterface for voice and data, you can use the appropriate QoS tool per line. For example, each DLCI would use 32 kbps of a 64 kbps line.

  - Apply adaptive traffic shaping to both DLCIs.

  - Use RSVP or IP precedence to prioritize voice traffic.

  - Use compressed RTP to minimize voice packet size.

  - Use weighted fair queuing to manage voice traffic.

- Lower MTU size—Voice packets are generally small. By lowering the maximum transmission unit (MTU) size (for example, to 300 bytes), large data packets can be broken up into smaller data packets that can more easily be interwoven with voice packets.

> **Note**   Lowering the MTU size affects data throughput speed.

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

  - Use RSVP or IP precedence to prioritize voice traffic.

  - Use compressed RTP to minimize voice packet header size.

- Traffic shaping—Use adaptive traffic shaping to throttle back the output rate based on the backward explicit congestion notification (BECN). If the feedback from the switch is ignored, packets (both data and voice) might be discarded. Because the Frame Relay switch does not distinguish between voice and data packets, voice packets could be discarded, which would result in a deterioration of voice quality.

  - Use RSVP, compressed RTP, reduced MTU size, and adaptive traffic shaping based on BECN to hold the data rate to the CIR.

  - Use generic traffic shaping to obtain a low interpacket wait time. For example, set Bc to 4000 to obtain an interpacket wait of 125 ms.

Voice over Frame Relay Configuration Example

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

```
interface serial 1/1
MTU 300
no ip address
```

```
encapsulation frame-relay
no ip route-cache
no ip mroute-cache
fair-queue 64 256 1000
frame-relay ip rtp header-compression

interface serial 1/1.1
MTU 300
ip address 10.0.0.5 255.0.0.0
ip rsvp bandwidth 48 48
no ip route-cache
no ip mroute-cache
bandwidth 64
traffic-shape rate 32000 4000 4000
frame-relay interface-dlci 16
frame-relay ip rtp header-compression
```

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

- MTU size is 300 bytes.

- No IP address is associated with this serial interface. The IP address must be assigned for the subinterface.

- Encapsulation method is Frame Relay.

- Fair queuing is enabled.

- IP RTP header compression is enabled

The subinterface has been configured as follows:

- MTU size is inherited from the main interface.

- IP address for the subinterface is specified.

- Bandwidth is set to 64 kbps.

- RSVP is enabled to use the default value, which is 75 percent of the configured bandwidth.

- Generic traffic shaping is enabled with 32 kbps CIR where $Bc = 4000$ bits and $Be = 4000$ bits.

- Frame Relay DLCI number is specified.

- IP RTP header compression is enabled.

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

For more information about Frame Relay, refer to the Cisco IOS Release 12.0 *Wide-Area Networking Configuration Guide*.

Checking the Configuration

After configuring the new interface, use the **show** commands to display the status of the new interface or all interfaces, and use the **ping** command to check connectivity. This section includes the following subsections:

Using show Commands to Verify the New Interface Status

Table 4-8 demonstrates how you can use the **show** commands to verify that new interfaces are configured and operating correctly and that the *PA-MCX* appears in them correctly. Sample displays of the output of selected **show** commands appear in the sections that follow. For complete command descriptions and examples, refer to the publications listed in the "Related Documentation" section on page viii.

Troubleshooting Tips

If information about the PA-MCX port adapter is not indicated in show command output, it is probably because the card type has not been specified.

Because the PA-MCX port adapter can be configured for E1 or T1 connectivity, you **must** specify the card type as E1 or T1, as described in "Performing a Basic Configuration" section on page 4-4. There is no default card type. The port adapter is not functional until the card type is set.

> **Note** The outputs that appear in this document may not match the output you receive when running these commands. The outputs in this document are examples only.

Table 4-8   Using show Commands

Command	Function	Example
show version or **show hardware**	Displays system hardware configuration, the number of each interface type installed, Cisco IOS software version, names and sources of configuration files, and boot images	Router# **show version**
show controllers	Displays all the current interface processors and their interfaces	Router# **show controllers**
show diag *slot*	Displays types of port adapters installed in your system and information about a specific port adapter slot, interface processor slot, or chassis slot	Router# **show diag 2**
show protocols	Displays protocols configured for the entire system and for specific interfaces	Router# **show protocols**
show running-config	Displays the running configuration file	Router# **show running-config**
show startup-config	Displays the configuration stored in NVRAM	Router# **show startup-config**

If an interface is shut down and you configured it as up, or if the displays indicate that the hardware is not functioning properly, ensure that the interface is properly connected and terminated. If you still have problems bringing up the interface, contact a service representative for assistance. This section includes the following subsections:

- Using the show version or show hardware Commands, page 4-40

- Using the show diag Command, page 4-41

- Using the show interfaces Command, page 4-41

Choose the subsection appropriate for your system. Proceed to the "Using the ping Command to Verify Network Connectivity" section on page 4-42 when you have finished using the **show** commands.

Using the show version or show hardware Commands

Display the configuration of the system hardware, the number of each interface type installed, the Cisco IOS software version, the names and sources of configuration files, and the boot images, using the **show version** (or **show hardware**) command.

Note The outputs that appear in this document may not match the output you receive when running these commands. The outputs in this document are examples only.

Following is an example of the **show version** command from a Cisco 7200 VXR router with the *PA-MCX*:

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 7200 Software (C7200-IS-M), Version 12.1(20000628:194205)]
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Fri 30-Jun-00 07:45 by nyv
Image text-base: 0x60008960, data-base: 0x612AE000

ROM: System Bootstrap, Version 12.0(19990210:195103) [12.0XE 104], DEVELOPMENT E
BOOTFLASH: 7200 Software (C7200-BOOT-M), Version 12.1(20000621:184]

Router uptime is 1 day, 2 hours, 22 minutes
System returned to ROM by reload
System image file is "tftp://172.168.0.0/c7200-is-mz.delt4"

cisco 7206VXR (NPE300) processor (revision B) with 57344K/40960K bytes of memor.
Processor board ID 11060156
R7000 CPU at 262Mhz, Implementation 39, Rev 1.0, 256KB L2, 2048KB L3 Cache
6 slot VXR midplane, Version 2.0

Last reset from power-on
Channelized E1, Version 1.0.
Bridging software.
X.25 software, Version 3.0.0.
Primary Rate ISDN software, Version 1.1.
4 Ethernet/IEEE 802.3 interface(s)
1 FastEthernet/IEEE 802.3 interface(s)
12 Serial network interface(s)
6 Channelized E1/PRI port(s)
12 Channelized T1/PRI port(s)
1 Voice resource(s)
125K bytes of non-volatile configuration memory.

20480K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
4096K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x0
```

Using the show diag Command

Display the types of port adapters installed in your system (and specific information about each) using the **show diag** *slot* command, where *slot* is the *port adapter slot* in a Cisco 7200 VXR router.

Note   The outputs that appear in this document may not match the output you receive when running these commands. The outputs in this document are examples only.

Following is an example of the **show diag** *slot* command that shows a PA-MCX in port adapter slot 5 of a Cisco 7200 VXR router:

```
Router# show diag 5
Slot 5:
        PA-MCX-8TE1 Port adapter, 8 ports
        Port adapter is analyzed
        Port adapter insertion time 1d02h ago
        EEPROM contents at hardware discovery:
        Hardware Revision       : 1.0
        PCB Serial Number       : 0001608`252
        Part Number             : 73-4118-01
        Board Revision          : 09
        RMA Test History        : 00
        RMA Number              : 0-0-0-0
        RMA History             : 00
        Deviation Number        : 0-0
        Product Number          : P@PA-MCX-8TE1
        Top Assy. Part Number   : 800-05358-01
        EEPROM format version 4
        EEPROM contents (hex):
          0x00: 04 FF 40 01 7A 41 01 00 C1 8B 30 30 30 31 36 30
          0x10: 38 60 32 35 32 82 49 10 16 01 42 30 39 03 00 81
          0x20: 00 00 00 00 04 00 80 00 00 00 00 CB 94 50 40 50
          0x30: 41 2D 4D 43 58 2D 38 54 45 31 20 20 20 20 20 20
          0x40: 20 C0 46 03 20 00 14 EE 01 FF FF FF FF FF FF FF
          0x50: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x60: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
          0x70: FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

Using the show interfaces Command

The **show interfaces** command displays status information (including the physical slot and interface address) for the interfaces you specify. The example that follows specifies DSPfarm interfaces.

For complete descriptions of interface subcommands and the configuration options available for **Cisco 7200 series** interfaces, refer to the publications listed in the "Related Documentation" section on page viii.

Note   The outputs that appear in this document may not match the output you receive when running these commands. The outputs in this document are examples only.

Following is an example of the **show interfaces serial** command for Cisco 7200 VXR routers. In this example, the PA-MCX port adapter is located in port adapter slot 3.

```
Router# show interfaces serial 3/0
Serial3/0:0 is down, line protocol is down
  Hardware is PA-MCX-2TE1
```

```
        MTU 1500 bytes, BW 1984 Kbit, DLY 20000 usec,
           reliability 255/255, txload 1/255, rxload 1/255
        Encapsulation HDLC, crc 16, loopback not set
        Keepalive set (10 sec)
        Last input never, output never, output hang never
        Last clearing of "show interface" counters never
        Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
        Queueing strategy: weighted fair
        Output queue: 0/1000/64/0 (size/max total/threshold/drops)
           Conversations  0/0/16 (active/max active/max total)
           Reserved Conversations 0/0 (allocated/max allocated)
           Available Bandwidth 1488 kilobits/sec
        5 minute input rate 0 bits/sec, 0 packets/sec
        5 minute output rate 0 bits/sec, 0 packets/sec
           0 packets input, 0 bytes, 0 no buffer
           Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
           0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
           0 packets output, 0 bytes, 0 underruns
           0 output errors, 0 collisions, 0 interface resets
           0 output buffer failures, 0 output buffers swapped out
           0 carrier transitions    alarm present
        Timeslot(s) Used:1-31, subrate: 64Kb/s, transmit delay is 0 flags
Serial3/1:0 is down, line protocol is down
```

Proceed to the next section, "Using the ping Command to Verify Network Connectivity," to check network connectivity of the *PA-MCX* and switch or router.

Using the ping Command to Verify Network Connectivity

Using the **ping** command, you can verify that an interface port is functioning properly. This section provides a brief description of this command. Refer to the publications listed in the "Related Documentation" section on page viii for detailed command descriptions and examples.

The **ping** command sends echo request packets out to a remote device at an IP address that you specify. After sending an echo request, the system waits a specified time for the remote device to reply. Each echo reply is displayed as an exclamation point (!) on the console terminal; each request that is not returned before the specified timeout is displayed as a period (.). A series of exclamation points (!!!!!) indicates a good connection; a series of periods (.....) or the messages [timed out] or [failed] indicate a bad connection.

Following is an example of a successful **ping** command to a remote server with the address 10.0.0.10:

```
Router# ping 10.0.0.10 <Return>
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/15/64 ms
Router#
```

If the connection fails, verify that you have the correct IP address for the destination and that the device is active (powered on), and repeat the **ping** command.