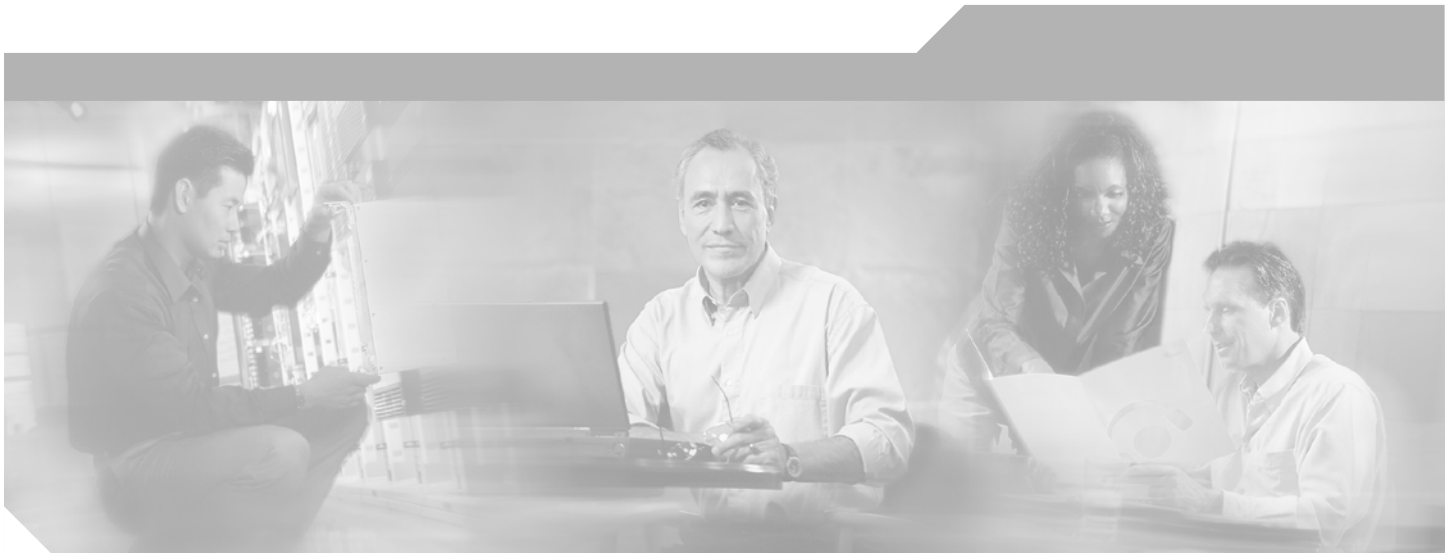


Cisco MeetingPlace Audio Server 5.2 Customer Engineering Guide (for Cisco MeetingPlace 8112)

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number: OL-

The following information is for FCC compliance of Class A devices: 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.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your 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.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

Cisco MeetingPlace Audio Server 5.2 Customer Engineering Guide (for Cisco MeetingPlace 8112)

CONTENTS

Introduction

This document provides the following information on MeetingPlace Audio Server (formerly named MeetingServer) 5.2 software and hardware:

- hardware and software functional descriptions
- installation procedures
- software configuration procedures
- maintenance and troubleshooting

Naming Convention

Throughout the remainder of this document we refer to these products in the following manner:

- Cisco MeetingPlace as MeetingPlace
- Cisco MeetingPlace 8112 server (formerly known as M3) as 8112 server
- Cisco MeetingPlace 8106 server as 8106 server

Hardware and software version

The information in this document reflects MeetingPlace Audio Server 5.2 software for the 8112 server unless otherwise indicated.

Who should use this guide

This document supports Application Consultants, Installation Specialists, and Field Engineers responsible for installing the MeetingPlace Audio Server 5.2 software and the 8112 server, and for properly trained MeetingPlace System Managers responsible for maintenance. Document users should have a solid understanding of voice and data communication terminology and concepts.

How to use this guide

If the document is viewed as an Adobe Acrobat PDF file, the following items can be clicked to jump to the referenced location in the document:

- page numbers in the table of contents
- any references to figures, tables, or sections in the text
- page numbers in the text

To visually group information, this document uses bulleted lists and tables. This document also contains an index.

To streamline document use for more experienced users, many terms are introduced without definition. For those unfamiliar with these terms, Appendix G, "Glossary" contains a glossary. In addition, there is a list of acronyms in Appendix F, "Acronyms".

Visual cues used in this guide

Special information in this guide looks like this:

Warning **These messages alert you to dangerous situations or conditions that require your attention.**

Caution These messages identify essential steps, actions, or system messages that should not be ignored.

Note These messages contain information about a particular subject that we want to bring to your attention. These include helpful hints and time-saving suggestions about using MeetingPlace features.

Additional resources

For information on obtaining other documentation offered by Cisco Systems, contact your MeetingPlace support or sales representative.

For system managers

The following information is available for MeetingPlace system managers.

Table 1-1 Information for MeetingPlace System Managers

Title	Description
MeetingPlace Audio Server Installation Planning Guide	Instructions and worksheets for installing or upgrading MeetingPlace and the various system options. Versions are available for the MeetingPlace 8112 platform, the MeetingPlace 8106 platform, the MeetingPlace PCI platform, and MeetingPlace Hosted Services.
MeetingPlace Audio Server System Manager's Guide	How to set up, customize, and maintain MeetingPlace. Versions are available for the MeetingPlace 8112 platform, the MeetingPlace 8106 platform, and the MeetingPlace PCI platform.
MeetingPlace Web System Manager's Guide	Describes how to set up, maintain, and use MeetingPlace Web.
MeetingPlace Directory Services System Manager's Guide	Instructions for installing and maintaining MeetingPlace Directory Services Gateway.
MeetingPlace for Outlook System Manager's Guide	Instructions for installing and maintaining MeetingPlace Outlook Gateway
MeetingPlace for Notes System Manager's Guide	Instructions for installing and maintaining MeetingPlace Notes Gateway.
MeetingPlace E-mail Gateway System Manager's Guide	Instructions for installing and maintaining MeetingPlace E-Mail Gateway.
MeetingPlace for IP Phone System Manager's Guide	Instructions for installing and maintaining the MeetingPlace for IP application on your Cisco IP phone.
MeetingPlace IM Gateway System Manager's Guide	Instructions for installing and maintaining MeetingPlace IM Gateway.
MeetingPlace Network Backup Gateway System Manager's Guide	Instructions for installing and maintaining MeetingPlace Network Backup Gateway.

For MeetingPlace users

The following information is available for MeetingPlace end users.

Table 1-2 Additional Information for MeetingPlace Users

Title	Description
MeetingPlace quick reference card	Quick tips for using MeetingPlace products and features. Quick reference cards are available for the MeetingPlace voice interface, MeetingPlace Web, MeetingPlace for Notes, MeetingPlace for Outlook, and MeetingPlace reservationless meetings.
MeetingPlace wallet card	A plastic wallet-sized card that shows the basic telephone commands for scheduling and attending meetings.
Voice quick tour	An overview of the voice user interface features for first-time users.

Online documentation

The following information about MeetingPlace is available online.

Table 1-3 Online Help Information Available for MeetingPlace

Resource	Description
MeetingPlace e-tutorials	Four-minute interactive online modules that teach the basic steps and functionality of MeetingPlace. Modules include Web Conferencing, Web Scheduling, MeetingPlace for Outlook, MeetingPlace for Notes and Voice. These online tutorials are available all day every day and help you get the most out of your MeetingPlace system.
MeetingTime Quick Tour	An overview of MeetingTime features for first-time users.
Online help	Detailed instructions for using MeetingTime and MeetingPlace Web.
MeetingPlace Reference Center	A self-service web site designed to assist end users with MeetingPlace functionality. This customizable rollout tool is included with MeetingPlace Web.

Obtaining Documentation

Cisco provides several ways to obtain documentation, 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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order annual or quarterly subscriptions through the online Subscription Store:

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

Click Subscriptions & Promotional Materials in the left navigation bar.

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 Networking Products MarketPlace:

  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.

- 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://www.cisco.com/en/US/products/products_catalog_links_launch.html

- 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/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- 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

Understanding MeetingPlace Audio Server 5.2 for 8112

This chapter describes:

- what's new in the MeetingPlace Audio Server 5.2 software
- understanding MeetingPlace Audio Server 5.2 for the 8112 server and its components
- connections to other business systems

What's new in MeetingPlace Audio Server 5.2 software

MeetingPlace Audio Server 5.2 is a comprehensive software release with new features including VoIP improvements and an extension of IP scalability to 960 user licenses. This release is available for 8112 and 8106 systems.

MeetingPlace Audio Server 5.2 adds several new features that are outlined in Table 2-1. For a detailed explanation of each feature, refer to the *MeetingPlace Audio Server System Manager's Guide.*

Table 2-1 MeetingPlace Audio Server 5.2 New Features

Area	Improvement
Voice Over Internet Protocol (VoIP)	• Increased scalability up to 960 IP ports. • SIP protocol support. • G.729a compression codec support. • Hold and transfer feature. • Multiple IP gateways. • Registration, admission, and status (RAS) support. • Extended echo cancellation limit for line echoes. This may also benefit PSTN customers, especially those who use international multi-server meetings.
Reservationless meetings	• Single number access for reservationless deployments • Reservationless meeting access configuration by profile • Profiles with greater than nine characters can initiate reservationless meetings
Hardware	• Multi Access Blade MA-4 • CD-ROM for MeetingPlace; MeetingPlace Audio Server 5.2 no longer supports a tape drive
Administrative and security	• MeetingPlace Network Backup Gateway 5.2 support • Secure system access through Secure Shell (SSH) protocol • Ability to play participant names during meetings through MeetingTime • Server patch automation • Ability to disable SNMP queries
International deployments	• German, Portuguese, and Spanish voice prompts

Note This version of the MeetingPlace Audio Server does *not* support analog trunks or alarm relay.

Note MeetingPlace Audio Server versions 5.0 and later do not support EISA or PCI platforms. However, it is possible to convert a server from PCI to 8112 or 8106 through a network transfer. For more information, see the installation and upgrade document for the appropriate version.

Note This version of the MeetingPlace Audio Server allows for telnet to be disabled through MeetingTime. If telnet is disabled, the only way to access the server is through SSH. The only SSH client supported by MeetingPlace is PuTTY. For more information on how to use SSH, refer to the Cisco TAC.

The tape drive on the 8112 server has been replaced with a CD-ROM drive. The CD-ROM drive is used for upgrading from the software from previous releases. Instructions for retrofitting the CD-ROM drive are included in the upgrade kit. Please note the following:

Note If you have a new 8112 server with MeetingPlace Audio Server 5.2 delivered fresh from the factory, the server automatically has the CD-ROM already installed and you do not need to do anything.

Note If you have an earlier version of the 8112 server, with the tape drive, you need to have a CD-ROM retrofitted on your system before you can upgrade to MeetingPlace Audio Server 5.2.
You will be contacted by Cisco TAC about having the CD-ROM retrofit done. (If you have not been contacted yet, call Cisco TAC to arrange to have the retrofit done. Do *not* attempt to do the retrofit yourself, even if you have the CD-ROM retrofit kit.)
Channel partners who upgrade the 8112 Release 5.2 upgrades on behalf of Cisco Systems must contact Cisco TAC about training on how to retrofit the CD-ROM drive on 8112 servers with tape drives.

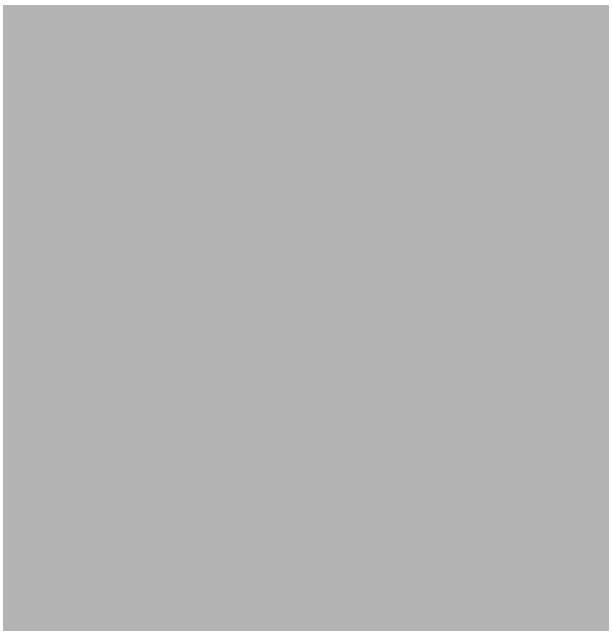
Understanding the 8112 server and its components

This section explains the 8112 server — its hardware components and software options.

MeetingPlace configurations include server hardware, server software, and desktop software components with additional software options available.

When system requirements exceed 120 user licenses (ports), the configuration includes an 8112 conference server. The server is a NEBS-compliant, rack-mountable box. See Figure 2-1.

Figure 2-1 8112 Physical Characteristics



The 8112 server has the capacity for a CPU card; a Hot Swap Controller (HSC); 12 slots for T1 Smart Blades, Smart Blades, or Multi Access Blades to provide physical connectivity to the telephone network; and four drives: two disk drives, a floppy drive, and a CD-ROM drive. Table 2-2 lists the maximum port configurations for each protocol and the hardware used to achieve them.

Table 2-2 8112 Server Hardware Configurations

Protocol	Max. Ports	Hardware configuration
T1	1152	12 T1 Smart Blades
E1	960	10 Smart Blades and 2 MA-16s
T1 PRI	736	8 Smart Blades and 2 MA-16s
IP	960	10 Smart Blades and 2 MA-16s

There is no cover or lid to open or remove to gain access to the server. From the front of the 8112 server, you can access the CPU card, HSC, Smart Blade cards, T1 Smart Blade cards, Multi Access Blade cards, redundant power supply units, fan assembly, disk drives, CD-ROM drive, and floppy drive. From the back of the 8112 server, you can access the LAN and telephony connections, and the transition modules for the CPU, Smart Blades, T1 Smart Blades, and Multi Access Blades.

The 8112 server hardware components

The 8112 server hardware components include the following:

- ***Mounting kits*** — Mechanical components necessary to mount the MeetingPlace system in one of the following configurations:
  - 19-inch or 23-inch EIA-310 rack (U.S. and Canada)
  - 19-inch or 23 inch frame-relay rack

- ***Smart Blades*** — Components required to provide physical connectivity to your telephone network.
  - *Smart Blade* — Provides both Port Resource Card (PRC) and Master Switch Controller (MSC) functionality in a single card.
  - *T1 Smart Blade* — Provides both PRC and MSC control functionality along with the necessary trunk interface functionality for digital T1 telephone lines. This Smart Blade also provides the ability to connect up to four T1 spans (96 ports) using E&M wink start, loop start, and ground start call supervision.
- ***Multi Access Blade (MA-16)*** — Includes the necessary trunk interface card functionality for T1 ISDN Primary Rate Interface (PRI), E1 digital telephony, and IP-based telephony. For T1 PRI, the MA-16 supports AT&T, Bell, and Nortel protocols. For E1, the MA-16 supports Euro ISDN and QSIG protocols. For IP, the MA-16 supports G.711 and G.729a audio encoding. Each MA-16 requires at least one Smart Blade. The MA-16 supports up to 16 PSTN spans.
- ***Multi Access Blade (MA-4)*** — Includes the necessary trunk interface card functionality for T1 ISDN PRI, E1 digital telephony, and IP-based telephony. For T1 PRI, the MA-4 supports AT&T, Bell, and Nortel protocols. For E1, the MA-4 supports Euro ISDN and QSIG protocols. For IP, the MA-4 supports G.711 and G.729a audio encoding. Each MA-4 requires at least one Smart Blade. The MA-4 supports up to four PSTN spans.
- ***Breakout box and cables —*** The breakout box provides a standard RJ-45 telephony interface for E1 and T1 PRI systems. It interfaces to a maximum of 16 cables. For each MA-16 shipped with the 8112 server, we include 16 telephony cables and two trunk interface cables (50-pin Amphenol connectors) to connect each MA-16 to the breakout box; for each MA-4 shipped with the 8112 server, we include four telephony cables and one trunk interface cable (50-pin Amphenol connector) to connect each MA-4 to the breakout box.

Note Each 8112 server comes equipped with 12 slots for Smart Blades, T1 Smart Blades, or Multi Access Blades. Each T1 Smart Blade supports 96 PSTN access ports; each MA-16 for E1 supports 480 access ports; each MA-16 for T1 PRI supports 368 access ports; each MA-16 for IP supports up to 480 access ports; each MA-4 for E1 supports 120 access ports; each MA-4 for T1 PRI supports 92 access ports; and each MA-4 for IP supports 120 access ports. See Table 2-3.

Table 2-3 Blade and Port Information

Blade	Number of Access Ports Supported
T1 Smart Blade	96
MA-16 for E1	480
MA-16 for T1 PRI	368
MA-16 for IP	480
MA-4 for E1	120
MA-4 for T1 PRI	92
MA-4 for IP	120
Smart Blade	96

Note E1, T1 PRI, and IP-based telephony require at least one Multi Access Blade and one Smart Blade. Each Smart Blade supports 96 ports.

- ***System database disks*** — The system incorporates two 36 GB disk drives for the MeetingPlace server software and the system database. Space is allocated equally on each drive, resulting in an extra database and system space as follows:
  - *System database disk 1* — Supports up to 500 MB of primary system files, 800 MB of temporary work space, and 5 GB of alternate space for storing the automatic database backup from disk 2. Disk 1 also includes 22 GB of additional storage for voice storage of user and meeting names and notes from the meeting.
  - *System database disk 2* — Supports up to 500 MB of primary system files, 800 MB of temporary work space, and 5 GB of alternate space for storing the automatic database backup from disk 1. Disk 2 also includes 22 GB of additional storage for voice storage of user and meeting names and notes from the meeting.
- ***Network interface*** — The CPU transition module has a pair of 10/100 Ethernet ports. The first port is used as the primary network interface. The second port is not used.
- ***External modem*** — The 8112 server includes an external modem connected to the system through a serial cable. The modem cable connects through the back of the server through the COM 2 connector on the CPU transition module.

MeetingPlace software

The MeetingPlace Audio Server 5.2 software uses a client-server architecture that divides computing tasks between the server and clients.The software that resides on the system database disk consists of the following:

- A real-time UNIX/POSIX-compatible operating system designed specifically for real-time intensive applications
- The system software including:
  - the MeetingPlace application software
  - a relational SQL database for storing all conference and profile information
  - the MeetingPlace options

Desktop software is installed on customer-supplied desktop computers. This software communicates with the conference server over the LAN or WAN.

For a list of all MeetingPlace Audio Server 5.2 software options, refer to the *MeetingPlace Audio Server 5.2 Installation Planning Guide*.

Understanding the 8112 server's LEDs

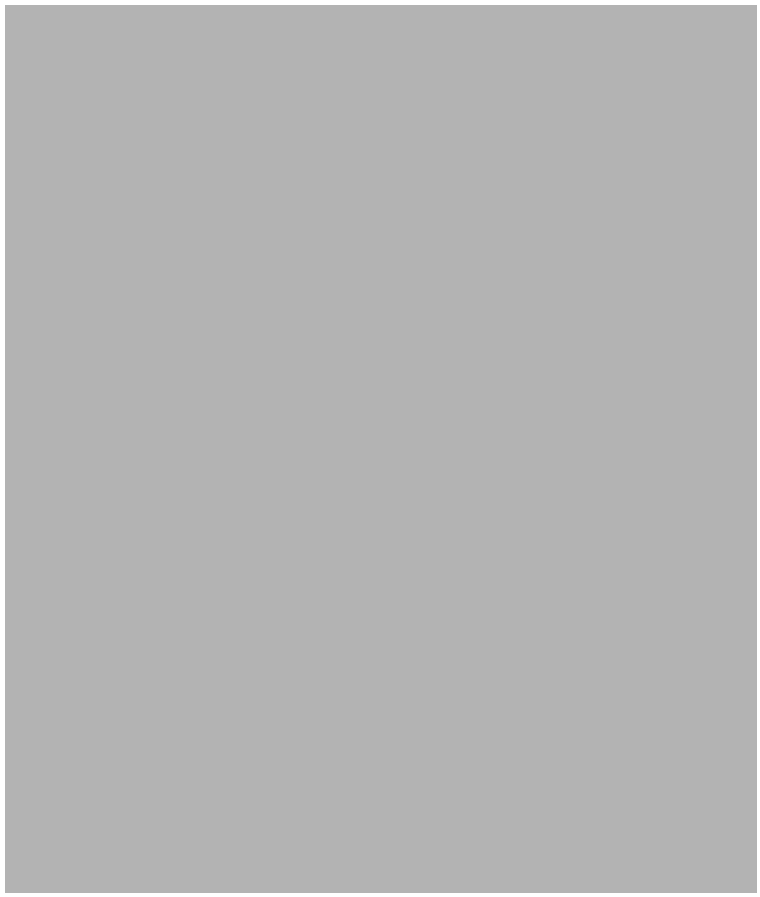
The 8112 server has system LEDs on the top panel in the front of the server. Refer to Table 2-4 for more information about the LEDs.

Table 2-4 Description of the 8112 Server's LEDs

Component	Meaning
System In Service	When on, indicates the system is in service.
Component Out of Service	When on, indicates there is a component out of service. Check the alarm table.
System Out of Service	When on, indicates the system is out of service.
Telco Major Alarm	When on, indicates a possible Telco problem that may affect service. Check the alarm table.
Telco Minor Alarm	When on, indicates a possible minor Telco problem that does not affect service. Check the alarm table.
Telco Critical Alarm	Not used, disregard.

Refer to Figure 2-2 to locate the 8112 server's LEDs.

Figure 2-2 Location of the 8112 Server's LEDs



Connections to other business systems

The MeetingPlace Audio Server 5.2 software controls the platform and provides MeetingPlace functions to desktops on the LAN. It also provides digital telephony access to Public Switched Telephone Network (PSTN) callers and IP telephony access to Voice Over IP (VoIP) callers.

The desktop software communicates with MeetingPlace over the LAN or WAN. Cisco Systems offers numerous desktop software applications including MeetingTime, MeetingPlace E-mail Gateway, MeetingPlace Outlook Gateway, MeetingPlace Notes Gateway, MeetingPlace Exchange Gateway, MeetingPlace Web Conferencing, MeetingPlace Directory Services, and MeetingPlace IP.

Refer to Figure 2-3 to view how the MeetingPlace Audio Server 5.2 interacts with other business systems.

Figure 2-3 Connections to Other Business Systems

Installing the 8112 Server

This chapter describes how to physically install the 8112 server, including the following steps:

1. Evaluating the site to ensure that all necessary facilities are available before beginning the installation process and all site requirements have been met. Refer to the "Evaluating the site" section on page 3-2.
2. Unpacking the system. Refer to the "Unpacking the 8112 server" section on page 3-10.
3. Installing the system by physically mounting the server. Refer to the "Mounting the 8112 server" section on page 3-13.
4. Connecting the components of the server to the various communications interfaces. Refer to the "Connecting the system cables" section on page 3-18 and "Installing and connecting the modem" section on page 3-40.

Note If this installation is part of a conversion from PCI to 8112, refer to the installation and upgrade document for the appropriate version. If you do not have access to this, please contact the Cisco TAC.

Important safety instructions

Save these instructions and requirements

Warning **Never install telephone wiring during a lightning storm.**

Warning **Never install a telephone jack in a wet location unless the jack is specifically designed for wet locations.**

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

Warning **Use caution when installing or modifying telephone lines.**

Warning **Supplemental earth grounding is required at all times.**

Tools used during installation

Refer to Appendix B, "Required Toolkit" for a list of tools needed for installation.

Evaluating the site

Before installing the 8112 server, make sure the MeetingPlace System Manager has provided the name of a site contact who can answer relevant questions regarding the site.

Warning **If any of the requirements in this section have not been met prior to installation, do not proceed with the installation.**

Environmental requirements

The recommended operating temperature range for MeetingPlace is 50-104 degrees Fahrenheit (10-40 degrees Celsius), with a non-condensing humidity of 5-80 percent.

It is essential to keep the server equipment properly cooled. To ensure this, the 8112 server has three internal DC powered fans cool the server. To ensure all system components are adequately cooled, the system must meet these requirements:

- at least 24 inches (60 cm) of clearance exists in the back of the 8112 server
- at least 1.75 inches (4.4 cm) of clearance exists on top of the 8112 server
- all module slots must be filled or covered (use filler panels in empty slots)
- air flow in an open frame rack must be from front to back
- air flow in an enclosed cabinet must be from front to back, bottom to top

Power requirements

Power for the rack system must come from a totally dedicated circuit breaker within 8 feet (2.43 meters) of the equipment. Do not plug any other electrical devices into an outlet connected to the circuit breaker serving the rack equipment. In addition, the site should have additional power outlets for test and maintenance equipment.

MeetingPlace power requirements are 100-115/200-230V, 6/3A, 50/60 Hz. If the power in your area is susceptible to fluctuations or interruptions, consider installing surge suppressors or connecting the servers to an Uninterruptible Power Supply (UPS). MeetingPlace does not maintain telephony connections should the system lose power.

MeetingPlace draws a maximum of 600 watts of power and produces a maximum of 2048 BTU/hour.

Table 3-1 Power Requirements by Country

Country	Clearance	Power	Socket
USA Canada	24 inches of clearance in back of server	115 VAC	NEMA 5-15R socket-outlet installed within 8 feet of the unit
Hong Kong European Union	61 cm of clearance in back of server	240 VAC	BS-1363 socket-outlet installed within 2 meters of the unit
Japan	61 cm of clearance in back of server	100 VAC (50Hz for East Japan; 60 Hz for West Japan)	NEMA 5-15R socket-outlet installed within 2 meters of unit

T1 digital trunk requirements

T1 Smart Blades support digital connections to a PBX system or to a PSTN. The framing for the digital lines can be either extended superframe (ESF) or D4. The digital lines can use either B8ZS coding or jammed bit.

Note We strongly recommend using ESF framing and B8ZS coding. Using D4 framing or jammed bit coding may produce unsatisfactory service.

Warning **Supplemental earth grounding is required at all times. This supplemental grounding consists of a grounding cable attached to supplemental ground lugs on the back of the 8112 server chassis and is permanently connected to an earth ground point at the other end via an appropriate facilities grounding terminal.**

Shielded cables must be used, and the shield must be electrically terminated at the back of the 8112 server. MeetingPlace also supports fractional T1 services and has complete flexibility to activate any or all ports on a span.

MeetingPlace can use dialed number information to connect the caller directly to a meeting or to determine the MeetingPlace services to which the caller has access.

MeetingPlace can also be configured to support devices where the T1 trunk does not provide any signaling and is always offhook. This is used in applications where a clear channel connection is required.

Table 3-2 T1 Digital Trunk Requirements by Country

Country	Requirements
US Canada Hong Kong	**Public network to CSU connection —** E&M wink start (line side and trunk side). Ground start or loop start (line side only). **(U.S. only)** — FCC and CSA-listed CSU (channel service unit) required. **Customer-supplied connectors** — USOC (male) RJ-48 jacks. Refer to the "Customer-supplied connectors" section on page 3-5. **Cisco Systems-provided cable** — 25-foot (7.6 m) shielded twisted pair cable with ferrite. **PBX to CSU connection** — FCC and CSA-listed CSU required for connections over 600 feet (182.88 m). MeetingPlace comes with a 25-foot (7.6 m) shielded cable with ferrite bead for each T1 span. The cable terminates in an RJ-48 connector, which the customer needs to interface with. Listed CSU is provided for over voltage protection for the T1 Smart Blades.
Japan	T1 connection into PBX with INS1500-to-T1 converter. **Customer-supplied connectors** — RJ-45 connector. **Cisco Systems-provided cable** — 15-meter (49.2 ft) shielded cable (male-male). One per T1 span.
Australia	Cisco Systems does not supply any T1 cables with servers shipped to Australia.

Note **(U.S. only)** The FCC Part 68 registration number is EMC USA-34550-XD-T. Be sure to use only FCC and CSA or UL-listed CSUs.

Note In some cases, the cables provided may not be appropriate for the customer's PBX or NIU side connections. If this is the case, the customer should feel free to create their own custom cables. Custom T1 CAS and IP cables require a Cat5e STP cable, with shielded RJ-45 connectors terminated to the cable shield at both ends. Add the ferrite which came on the Cisco Systems-supplied cable.

T1-supported protocols

The following are the supported protocols for T1 digital trunks:

- T1 CAS systems — E&M wink start, ground start, and loop start
- T1 PRI systems — AT&T (TR41459), Bell (NI-2), and Nortel (DMS-100)

See the "Customer-supplied connectors" section on page 3-5 for a picture of MeetingPlace digital telephony connections with T1 digital trunks.

Figure 3-1 MeetingPlace Digital Connection Requirements — T1

Customer-supplied connectors

See Table 3-3 and Table 3-4 for the wiring requirements for the customer-supplied RJ-48 connectors.

Table 3-3 Wiring of RJ-48 Connectors

Pin	Name	Description
1	T1	MeetingPlace received signal - tip
2	R1	MeetingPlace received signal - ring
4	T	MeetingPlace outgoing signal - tip
5	R	MeetingPlace outgoing signal - ring

To identify pins, hold the RJ-48 connector as if you are going to plug it in, with the tab down. Pin 1 is on the left.

If transmit and receive need to be reversed, the pins need to be reversed also. See Table 3-4.

Table 3-4 Wiring of RJ-48 Connectors when Transmit/Receive is Reversed

Pin	Name	Description
1	T	MeetingPlace outgoing signal - tip
2	R	MeetingPlace outgoing signal - ring
4	T1	MeetingPlace received signal - tip
5	R1	MeetingPlace received signal - ring

E1 digital trunk requirements

Verify the E1 digital trunk specifications agree with Table 3-5.

Table 3-5 E1 Digital Trunk Requirements

Country	Requirements
 European Union	**Connection Type** — Euro ISDN and QSIG digital telephony (E1) **Cisco Systems-supplied cable** — 25-foot (7.6 m) CAT5 cable with RJ-48c connectors at each end **Socket** — connector must be RJ-25 socket or NBNC (female) connector **Cable length** (if customer provides their own cable) — maximum cable length is 100 meters (328 ft)
 Australia	Cisco Systems does not supply any E1 cables with servers shipped to Australia.

Note In some cases, the RJ-48c cables provided may not be appropriate for the customer's PBX or NIU side connections. If this is the case, the customer should feel free to create their own custom cables. Custom E1 and T1 PRI cables require a Cat5e UTP cable and an RJ-48c connector on the breakout box side. Add the ferrite which came on the Cisco Systems-shipped cable.

Note In E1 environments, MeetingPlace can be connected directly to the PSTN, no CSU is needed.

E1-supported protocols

The following are the supported protocols for E1 digital trunks:

- Euro-ISDN (ETSI 300-102)
- QSIG (ECMA version) — channels are numbered 1-30
- QSIG (ETSI version) — channels are numbered 1-15 and 17-31

Note The MeetingPlace Audio Server 5.2 software supports only E1 PRI protocols. It does not support E1 CAS protocols.

See the "Modem requirements" section on page 3-7 for a picture of the MeetingPlace server digital telephony connections with E1 trunks.

Figure 3-2 MeetingPlace Digital Connection Requirements — E1

Modem requirements

The 8112 server includes an external modem connected to the system through a serial cable. The modem cable connects to the back of the server on the CPU transition module.

Table 3-6 Modem Requirements by Country

Country	Requirements
US Canada Hong Kong	• Cisco Systems-supplied US modem, serial cable, 6-foot (1.8 m) modem cable. • Customer-supplied standard analog telephone jack (RJ-11). Extension needs to be callable from the outside.
Japan	• Cisco Systems-supplied CE modem, serial cable, 2.5-meter (8.2 ft) modem cable. • Customer-supplied standard analog telephone jack (RJ-11). Extension needs to be callable from the outside.
European Union	• Cisco Systems-supplied global modem, serial cable. • Customer-supplied standard analog telephone jack (RJ-11). Extension needs to be callable from the outside.

LAN requirements

To connect to other applications, such as MeetingTime and MeetingPlace Web, MeetingPlace requires certain TCP/UDP ports to remain open on your network. Figure 3-3 displays the ports a server uses for communication. Unless otherwise specified, all ports listed are TCP.

Figure 3-3 TCP/UDP Port Requirements

Note The MeetingPlace server should reside on a network segment that is immune to broadcast storms. Broadcast storms can bring the server down for the duration of the storm.

LAN cable requirements

The 8112 server attaches to an Ethernet LAN. This connection provides all the communication from the MeetingPlace server to the customer's network. There are two possible scenarios for using an Ethernet LAN cable:

- connecting from the MeetingPlace CPU to the customer's network
- connecting from the MeetingPlace Multi Access Blade to the customer's network (for IP ports only)

For every configuration, you need a customer-supplied LAN cable to connect the MeetingPlace CPU to the customer's network.

For IP configurations, Cisco Systems ships the necessary LAN cables to connect the Multi Access Blade used for the IP configuration to the customer's network.

Refer to Table 3-7 for cable-specific requirements.

Table 3-7 LAN Cable Requirements

Type of LAN Cable	LAN Requirements
CPU to LAN cable (customer-supplied)	For twisted-pair Ethernet, 100Base-TX. Provide an RJ-45 jack. **Note** 10BaseT works, but is not recommended.
Multi Access Blade to LAN cable (for IP ports only) (Cisco Systems-supplied)	For twisted-pair Ethernet, Cat5e. Provide an RJ-45 connector. Cisco Systems provides a 25-foot (7.6 m) shielded cable with ferrite.
Australia	Cisco Systems does not supply any LAN cables with servers shipped to Australia.

Worksheets

Configuration worksheets are supplied in the *MeetingPlace Audio Server 5.2 Installation Planning Guide* to ensure that the MeetingPlace configuration integrates within the customer's environment. Make sure the necessary worksheets are completed before proceeding with the installation.

Unpacking the 8112 server

T1 CAS and pure IP systems are shipped in two boxes. One box contains the server and server accessories. The other box contains the modem and external cables.

T1 PRI and E1 systems are also shipped in two boxes. One box contains the server and server accessories. The other box contains the breakout box and cables, modem, and external cables.

To unpack the 8112 server, follow these steps:

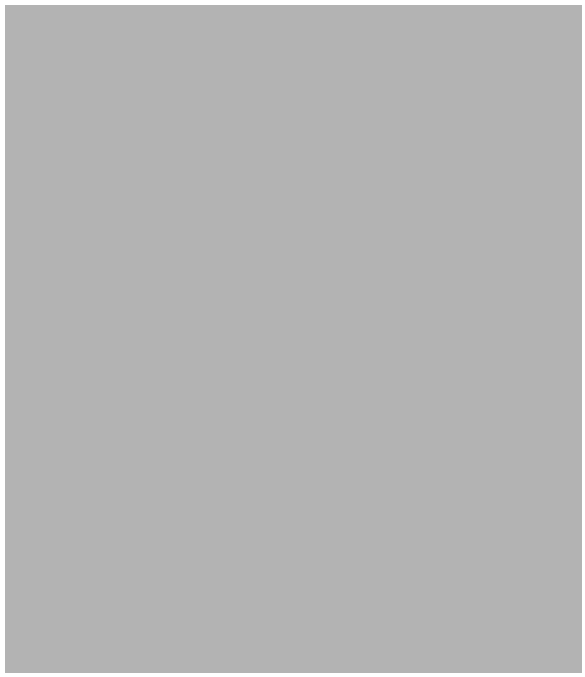
- remove the shipping material
- inspect for damage
- verify the contents of the boxes

Removing the shipping material

Warning **The server, its peripheries, and the packing materials can weigh up to 130 lbs (59 kg).**

Step 1 Make sure the packing carton is upright as in Figure 3-4.

Figure 3-4 Box Upright and Ready to be Unpacked

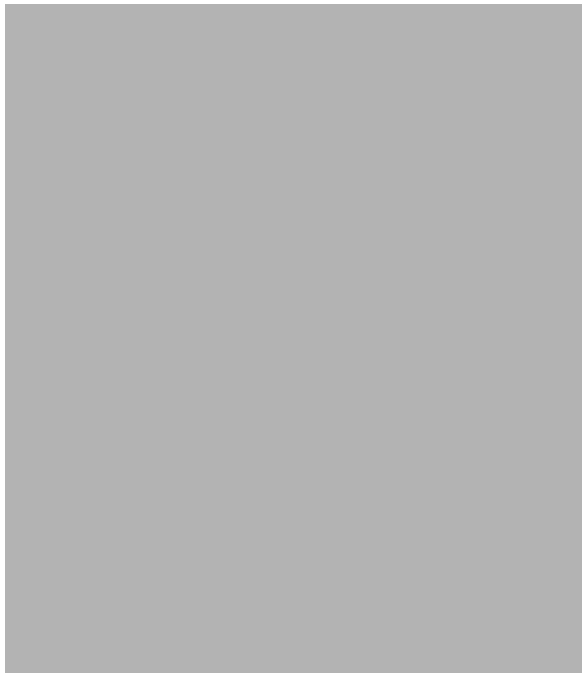


Step 2 Carefully cut the sealing tape and other packaging with a wire or box cutter and open the box.

Step 3 Remove the cardboard lid, contents (cables, documents, etc.), packing, and any foam packing material.

Step 4 Remove the outer box by lifting it straight up as in Figure 3-5.

Figure 3-5 Removing the Outer Box



Step 5 Remove the plastic covering.

Step 6 Lift the server carefully out of the carton and move it close to the location designated for the installation.

Inspecting for damage

Visually inspect the server for damage. If the server is damaged or scratched, call the Cisco TAC for instructions.

Verifying the contents of the boxes

Inspect the contents of the boxes to make sure the following are included:

Note These items are shipped in two separate boxes.

- 8112 server
- two sets of rack mount rails with 18 Phillips-head screws
- SCSI cable
- power cable
- external modem and cables (modem power cable, modem cable, and telephone extension cable)
- IP LAN cables for Multi Access Blades (for systems using IP ports). These IP LAN cables connect the Multi Access Blade to the customer's LAN

  Note The number of IP LAN cables you receive depends on the number of ports purchased for your system. You need one IP LAN cable for every Multi Access Blade in your system.

- T1 CAS telephony cables for T1 Smart Blades (for systems using T1 CAS ports). These T1 CAS telephony cables connect the T1 Smart Blades to the customer's system

  Note The number of T1 CAS telephony cables you receive depends on the number of ports purchased for your system. You need one T1 CAS telephony cable for every 24 PSTN ports being activated.

- E1 telephony cables (for systems using E1 ports). These E1 telephony cables connect the front of the breakout box to the customer's system

  Note The number of E1 telephony cables shipped with your system depends on how many Multi Access Blades are in the system. Sixteen cables are shipped for each Multi Access Blade.

- T1 PRI telephony cables (for systems using T1 PRI ports). These T1 PRI telephony cables connect the front of the breakout box to the customer's system

Note The number of T1 PRI telephony cables shipped with your system depends on how many Multi Access Blades are in the system. Sixteen cables are shipped for each Multi Access Blade.

- applicable software, manuals, and license documents

  In addition, the following items are shipped with systems requiring a breakout box (T1 PRI or E1 configuration):

- breakout box
- screws for mounting the breakout box
- trunk card interface cable assemblies (50-pin Amphenol cables)

Note The number of trunk card interface cable assemblies shipped with your system depends on how many and the type of Multi Access Blades in the system. Two cables are shipped for each MA-16 and one cable is shipped for each MA-4.

Mounting the 8112 server

This section describes how to mount and install the 8112 server for the following two types of racks:

- 19 or 23-inch frame relay rack
- 19 or 23-inch EIA equipment rack

Warning **The 8112 server must be mounted in one of these two types of racks. It cannot be placed on a surface such as the floor or a desk.**

Warning **To avoid hazards arising from uneven mechanical loading of the rack, plan your installation so that the weight of the equipment is evenly distributed in the rack and the heaviest units are mounted toward the bottom of the rack (within the limitations of equipment and cabling).**

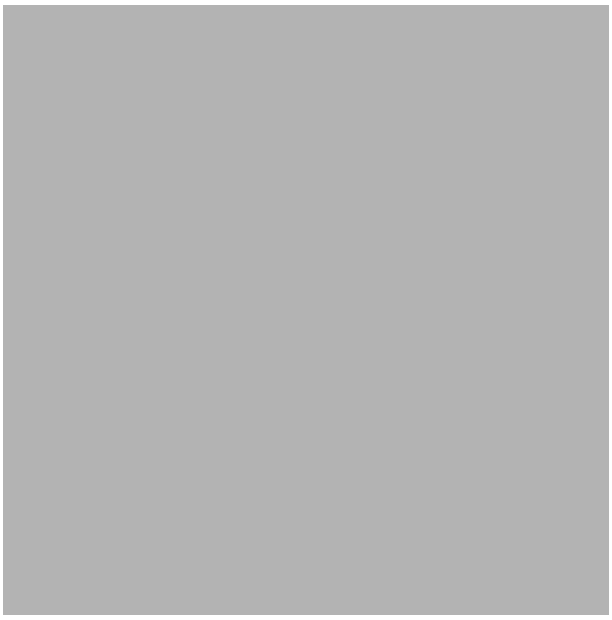
Preparing to mount the 8112 server

Before mounting the 8112 server, verify the following:

- The rack is securely bolted to the floor.
- At least 24 inches (60 cm) of clearance exists behind the server.
- At least 1.75 inches (4.4 cm) of clearance exists above the server.
- At least 1 inch (2.5 cm) of clearance exists below the server.

Note The 8112 server is 18.9 inches (48 cm) wide, 17.13 inches (43.5 cm) deep, and 21 inches (53.3 cm) high. See Figure 3-6.

Figure 3-6 8112 Server's Physical Characteristics



Mounting into a frame relay rack

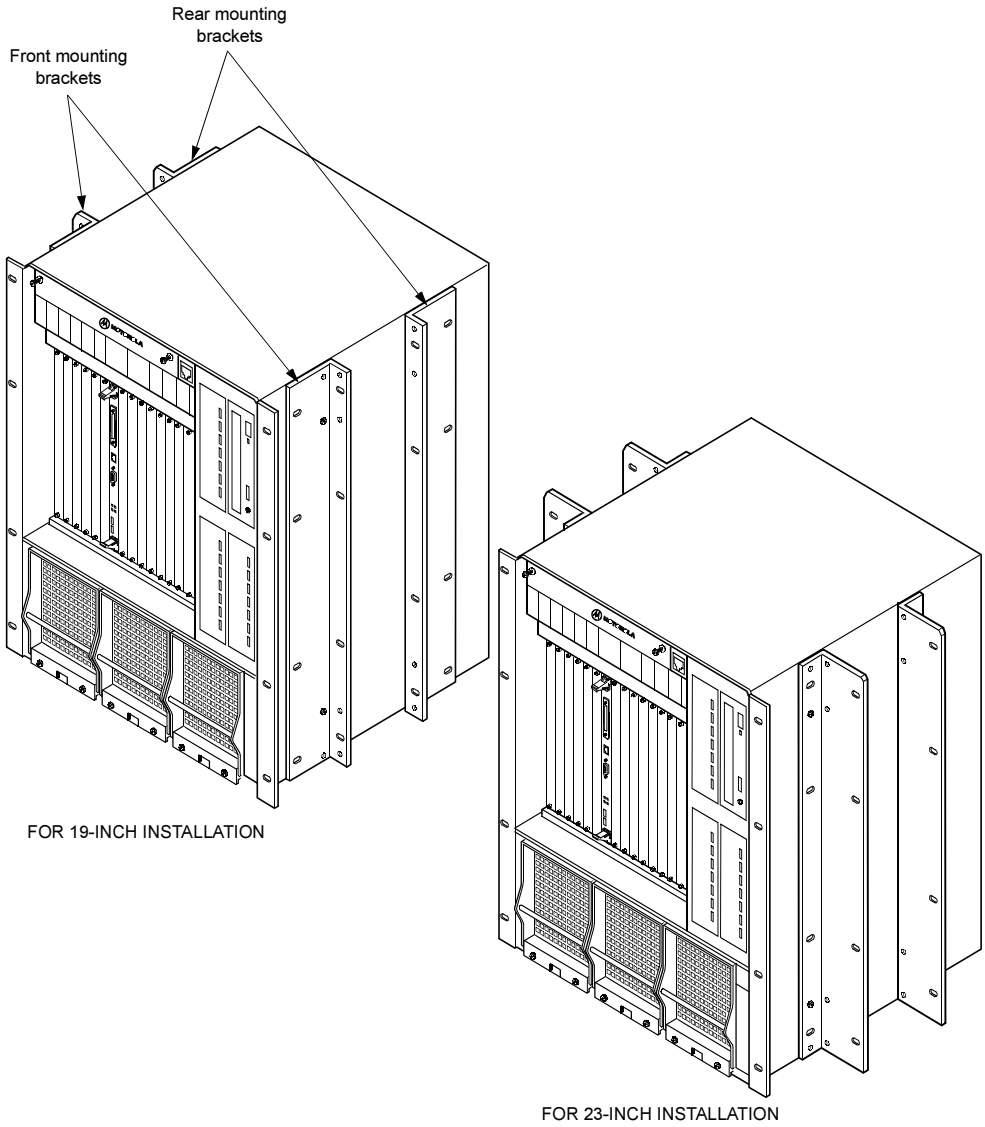
The 8112 server can be mounted in either a 19 or 23-inch frame relay rack, which is common in Central Office locations. In this configuration, the 8112 server is held along the center of the chassis.

The following procedure describes how to install the 8112 server in a 19 or 23-inch frame relay rack.

Step 1 Attach two mounting brackets to the *front* mounting holes of the server. See Figure 3-7.

- For 19-inch racks, the long side of the bracket should be fastened to the server.
- For 23-inch racks, the short side of the bracket should be fastened to the server.

Figure 3-7 Mounting into a Frame Relay Rack



Step 2 Slide the server into the front of the rack.

Step 3 Attach the server to the rack by securing it using the eight Phillips-head screws that shipped with the system.

Step 4 Attach two mounting brackets to the *rear* mounting holes of the system. See Figure 3-7.

- For 19-inch racks, the long side of the bracket should be fastened to the system.
- For 23-inch racks, the short side of the bracket should be fastened to the system.

Step 5 Secure the rear mounting bracket to the rack with the eight Phillips-head screws that shipped with the system.

Mounting into an EIA equipment rack

The 8112 server can also be mounted in a 19 or 23-inch EIA equipment rack. In this configuration, the server is mounted on the front rails.

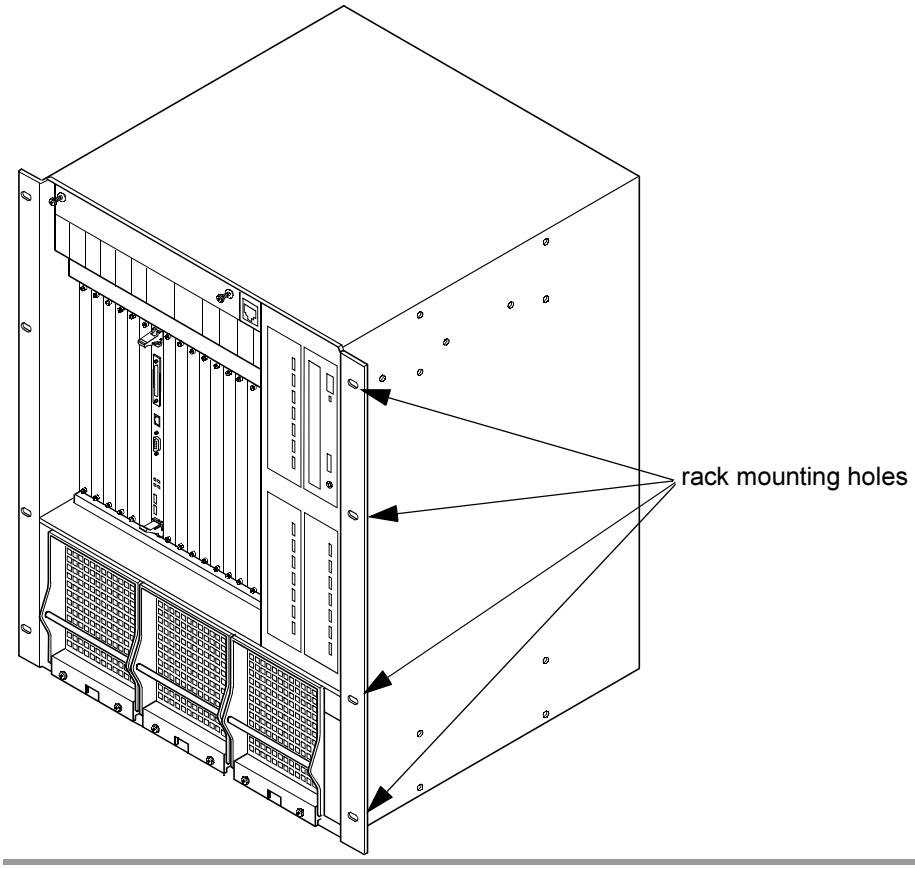
Step 1 If installing the system in a 19-inch rack, no additional mounting equipment is necessary when installing the system. Proceed to step 2 below.

If installing the system in a 23-inch rack, you must obtain extension brackets from the rack manufacturer. Install the optional extender brackets as described by the rack manufacturer.

Step 2 Slide the server into the front of the rack.

Step 3 Attach the system to the rack with eight Phillips-head screws that shipped with the system as in Figure 3-8.

Figure 3-8 Mounting into an EIA Equipment Rack



Mounting a breakout box

If your installation requires a breakout box (T1 PRI or E1 configuration), complete this section. If it does not, proceed to the "Connecting the system cables" section on page 3-18.

A breakout box provides a standard RJ-45 telephony interface. It interfaces to a maximum of 16 cables with an MA-16 and a maximum of four cables with each MA-4. The necessary number of RJ-48c cables to connect each breakout box to the customer's PBX or Telco NIU is shipped with each Multi Access Blade.

Note In some cases, the RJ-48c cables provided may not be appropriate for the customer's PBX or NIU side connections. If this is the case, the customer should feel free to create their own custom cables. These cables require an RJ-48c connector on the breakout box side.

A breakout box also includes the necessary number of 50-pin Amphenol cables. There are two 50-pin Amphenol cables provided to connect each MA-16 to the breakout box and one 50-pin Amphenol cable provided to connect each MA-4 to the breakout box.

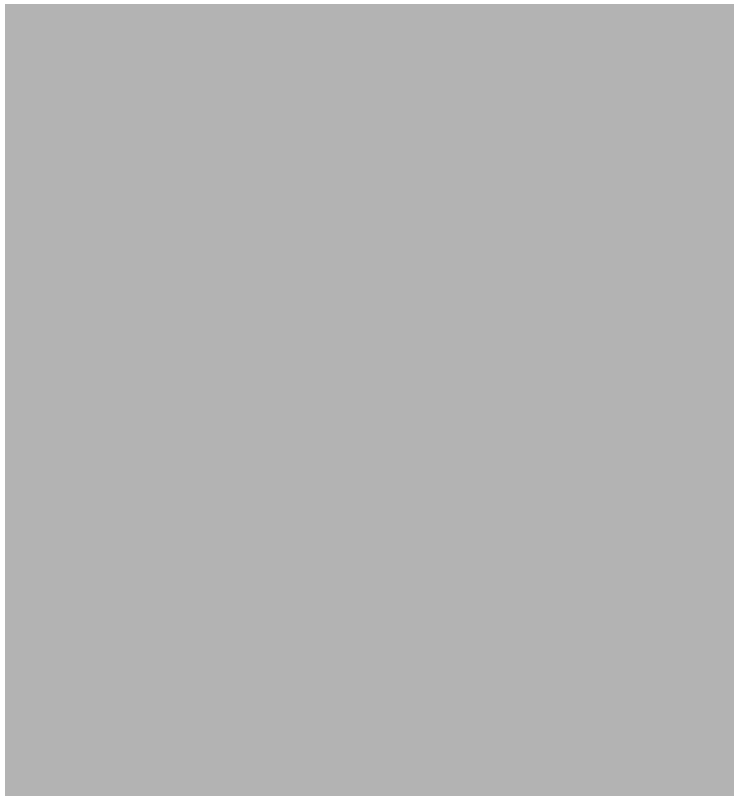
To mount a breakout box, follow these steps:

Step 1 Locate the breakout box shipped with the system.

Step 2 Locate the screws shipped with the system for mounting the breakout box.

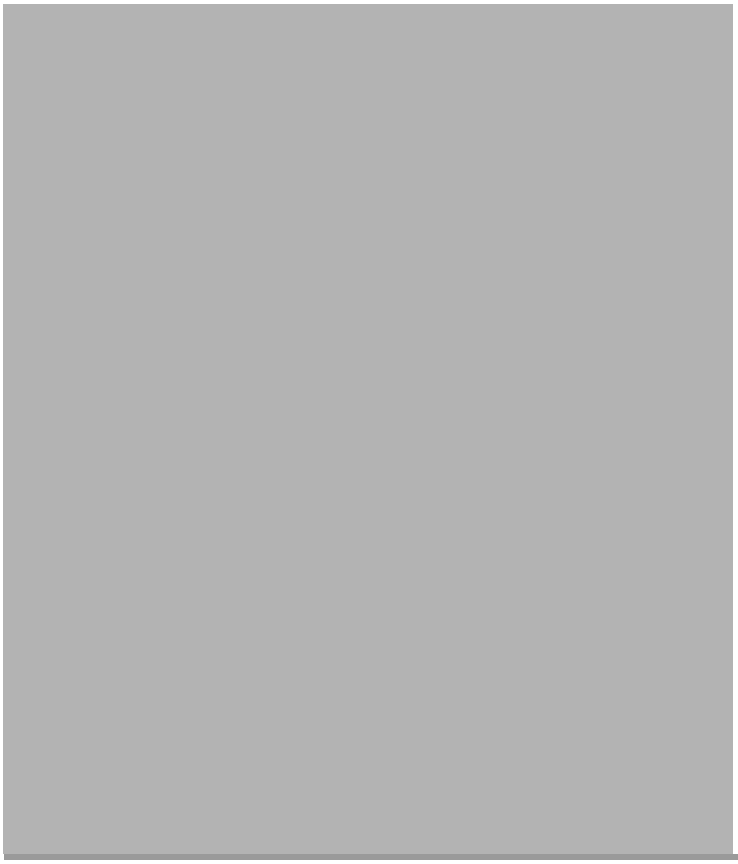
Step 3 Use a screwdriver to mount the breakout box into the position directly above the MeetingPlace server in the rack as in Figure 3-9.

Figure 3-9 Mounting the Breakout Box



If your system requires two MA-16 Multi Access Blades, you need two breakout boxes. (A fully loaded 960 port E1 system has two MA-16s and a fully loaded 736 port T1 PRI system has two MA-16s).To mount the second breakout box, follow the instructions above. Place the second breakout box directly above the first breakout box. See Figure 3-10.

Figure 3-10 System with Two Breakout Boxes



Connecting the system cables

This section describes how to connect the system cables correctly.

Connecting the power cable

Warning **To meeting grounding requirements, you must connect the power cable before connecting any other cables.**

Step 1 Locate the Cisco Systems-supplied power cable.

Step 2 Attach the socket end of the Cisco Systems-supplied power cable to the AC inlet on the back of the server. See Figure 3-11.

Figure 3-11 8112 Server's Power Cable Location

Step 3 Plug the other end of the Cisco Systems-supplied power cable into the AC power source.

Connecting the SCSI cable

Step 1 Make sure the server's power switch is set to off ("O"). See Figure 3-12.

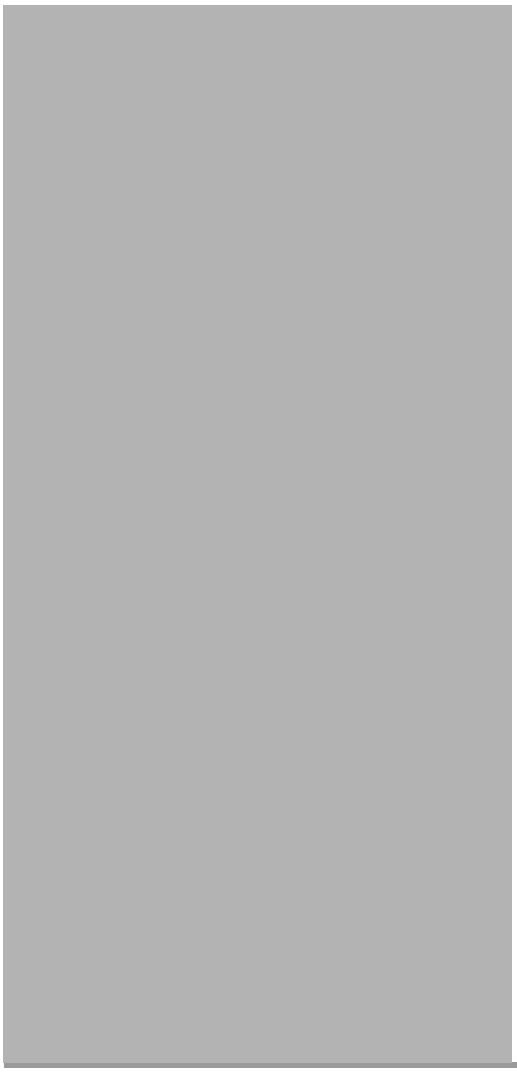
Figure 3-12 Power Switch Location

Step 2 Attach one end of the Cisco Systems-supplied SCSI cable to the SCSI connector on the back of the floppy drive housing. See Figure 3-13.

Figure 3-13 SCSI Cable Connection

Step 3 Attach the other end of the SCSI cable to the SCSI port on the CPU transition module in slot 7 on the back of the server. See Figure 3-14.

Figure 3-14 CPU Transition Module



Connecting the LAN cable to the CPU

The LAN cable is customer-supplied and connects the 8112 server to the customer's network. Refer to "LAN requirements" section on page 3-8 to verify you have the correct LAN cable and connector.

Step 1 Locate the customer-supplied LAN cable.

Step 2 Plug one end of the customer-supplied LAN cable into the customer-supplied LAN socket.

Step 3 Plug the other end of the customer-supplied LAN cable into the Ethernet connection 1 on the CPU transition module in slot 7 on the back of the server. See Figure 3-14.

Connecting telephony cables for a T1 CAS system

All MeetingPlace servers for T1 CAS configurations are shipped with the necessary number of T1 Smart Blades. Each T1 Smart Blade transition module in the back of the server has connectors for four trunk lines. Looking at the back of the server, the T1 Smart Blade transition modules begin in slot 1 on the right and move to the left.

The number of T1 CAS telephony cables shipped with the system depends on the number of ports being activated. You need one T1 CAS telephony cable for every 24 ports.

Figure 3-15 illustrates the cable connections for an 1152 port T1 CAS system. There are four T1 CAS telephony cables connected to each of the 12 T1 Smart Blade transition modules for a total of 48 T1 CAS telephony cables. Each cable holds 24 ports for a total of 1152 ports (48 x 24 = 1152).

Figure 3-15 Back of 8112 Server with T1s Connected

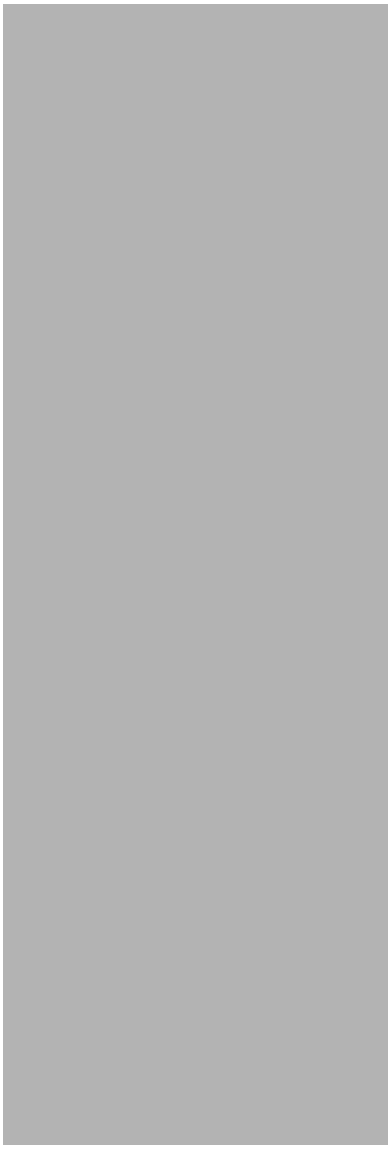
To connect the T1 CAS telephony cables for a T1 CAS system, follow these steps:

Step 1 Locate the Cisco Systems-supplied T1 CAS telephony cables, each with two RJ-48 connectors.

Step 2 Plug one end of the first Cisco Systems-supplied T1 CAS telephony cable into the customer-provided socket.

Step 3 Plug the other end of the first Cisco Systems-supplied T1 CAS telephony cable into the T1 Smart Blade transition module in the back of the server. The first T1 CAS telephony cable should be placed in the top connector slot. The second T1 CAS telephony cable should be placed in the next connector slot moving down, and so on. A maximum of four T1 CAS telephony cables can be connected to any one T1 Smart Blade transition module. See Figure 3-16.

Figure 3-16 T1 Smart Blade Transition Module



Step 4 Repeat steps 2 and 3 until all the T1 CAS telephony cables are connected.

Step 5 Install tie wraps and label the T1 CAS telephony cables as needed.

Connecting telephony cables for E1 and T1 PRI systems

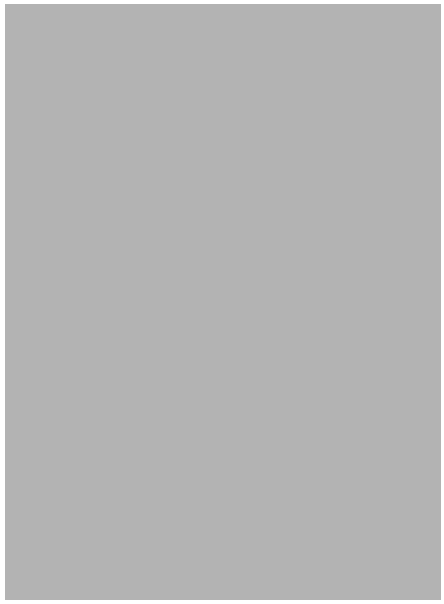
All MeetingPlace servers for E1 and T1 PRI configurations are shipped with the necessary number of Multi Access Blades. 8112 servers can have five Multi Access Blade configurations:

- one Multi Access Blade MA-16 card
- one Multi Access Blade MA-4 card
- two Multi Access Blade MA-4 cards

- one Multi Access Blade MA-16 card and one Multi Access Blade MA-4 card
- two Multi Access Blade MA-16 cards

MeetingPlace servers for E1 and T1 PRI configurations are also shipped with a breakout box and cables. The breakout box provides a standard RJ-45 telephony interface for E1 and T1 PRI systems. Also shipped are the necessary number of trunk card interface cable assemblies (50-pin Amphenol cables). These connect the breakout box to the Multi Access Blade transition modules. Figure 3-17 shows the 50-pin Amphenol cable.

Figure 3-17 50-pin Amphenol Cable



The number of E1 or T1 PRI telephony cables shipped with the system depends on the number of ports being activated. You need one E1 telephony cable for every 30 ports in an E1 system and one T1 PRI telephony cable for every 23 ports in a T1 PRI system.

Looking at the back of the server, the Multi Access Blade transition modules begin in slot 1 on the right and move to the left.

Figure 3-18 illustrates the cable connections for a 480-port E1 system from the front of the server. One breakout box services one MA-16 with 16 spans, one MA-4 with four spans, or two MA-4s with four spans each.

Note A fully loaded 960 port E1 system has two MA-16s and requires two breakout boxes. A fully loaded 736 port T1 PRI system has two MA-16s and requires two breakout boxes.

Figure 3-18 Front of 8112 Server with Cables Connected

One Multi Access Blade MA-16 card

To connect the E1 or T1 PRI telephony cables for one Multi Access Blade MA-16 card, follow these steps:

Step 1 Locate the following Cisco Systems-supplied items:

- E1 or T1 PRI telephony cables
- breakout box (should already be mounted above the MeetingPlace server)
- trunk card interface cable assemblies (50-pin Amphenol cables)

Step 2 Plug the first E1 or T1 PRI telephony cable into the customer-supplied RJ-48c socket.

Step 3 Plug the other end of the first E1 or T1 PRI telephony cable into the slot labelled 1 on the far left of the front of the breakout box. Continue from left to right as needed. See Figure 3-19.

Figure 3-19 Breakout Box, Front View

Step 4 Repeat steps 2 and 3 above until all the E1 or T1 PRI telephony cables are connected to the breakout box.

Step 5 Connect the first trunk card cable assembly (50-pin Amphenol cable) to the back of the breakout box by securing the screws on both ends. Looking at the back of the breakout box, the connector on the right of the breakout box is for spans 1-8 and the connector on the left of the breakout box is for spans 9-16. The first cable should go into the connector on the right. See Figure 3-20.

Figure 3-20 Breakout Box, Back View

Step 6 Connect the other end of the first trunk card cable assembly (50-pin Amphenol cable) into the Multi Access Blade transition module by securing the screws on both ends. The connector on the top of the Multi Access Blade transition module is for spans 1-8 and the connector on the bottom of the Multi Access Blade transition module is for spans 9-16. The first cable should go into the connector on the top. See Figure 3-21.

Figure 3-21 Multi Access Blade Transition Module

Step 7 Repeat steps 5 and 6 for the second trunk card cable assembly (50-pin Amphenol cable). The second cable should go into the connectors on the left of the breakout box and on the bottom of the Multi Access Blade.

Figure 3-23 illustrates the 8112 server's connections from the back of the server. This configuration supports 480 E1 ports with one Multi Access Blade card MA-16.

Figure 3-22 Back of Server (E1 with 1 MA-16)

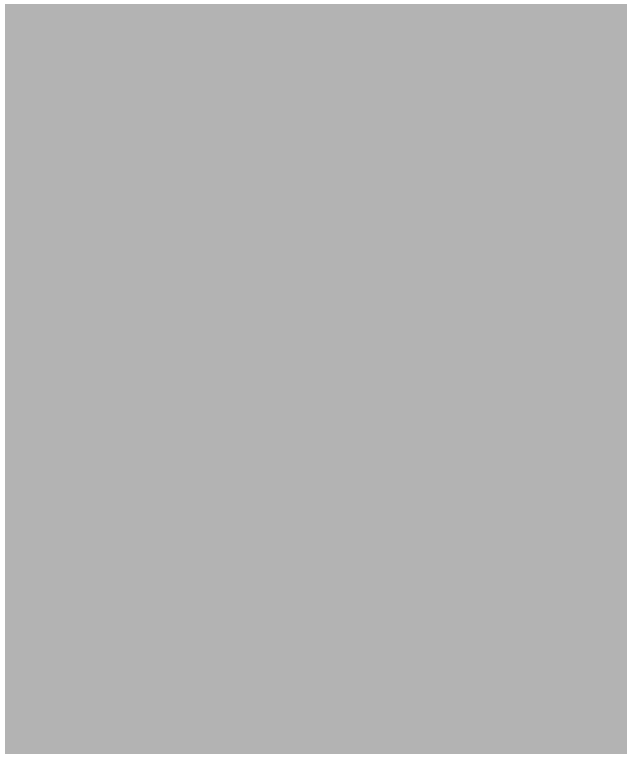
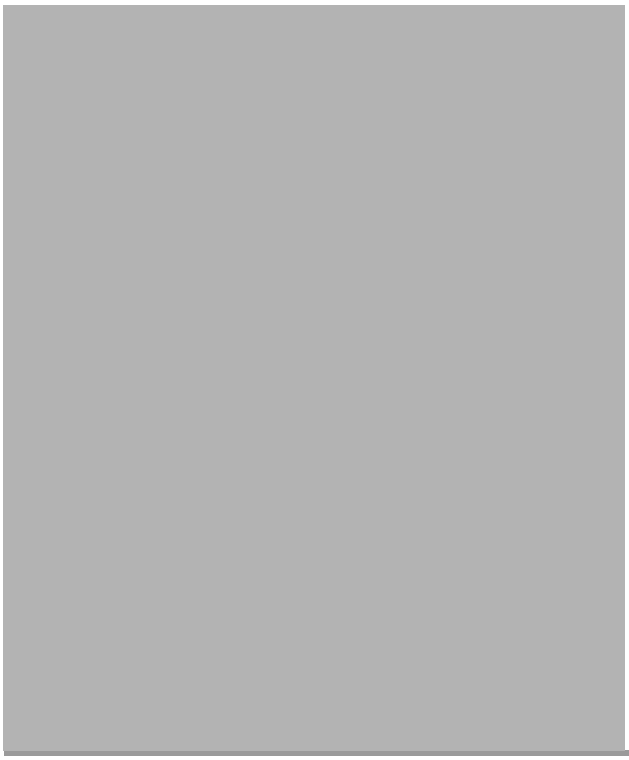


Figure 3-23 illustrates the 8112 server's connections from the back of the server. This configuration supports 368 T1 PRI ports with one Multi Access Blade card MA-16.

Figure 3-23 Back of Server (T1 PRI with 1 MA-16)



One Multi Access Blade MA-4 card

To connect the E1 or T1 PRI telephony cables for one Multi Access Blade MA-4 card, follow these steps:

Step 1 Locate the following Cisco Systems-supplied items:

- E1 or T1 PRI telephony cables
- breakout box (should already be mounted above the MeetingPlace server)
- trunk card interface cable assembly (50-pin Amphenol cable)

Step 2 Plug the first E1 or T1 PRI telephony cable into the customer-supplied RJ-48c socket.

Step 3 Plug the other end of the first E1 or T1 PRI telephony cable into the slot labelled 1 on the far left of the front of the breakout box. Continue from left to right.

Step 4 Repeat steps 2 and 3 above until all four E1 or T1 PRI telephony cables are connected to the breakout box.

Step 5 Connect the trunk card cable assembly (50-pin Amphenol cable) to the back of the breakout box by securing the screws on both ends. Looking at the back of the breakout box, put the 50-pin Amphenol cable into the connector on the right.

Step 6 Connect the other end of the trunk card cable assembly (50-pin Amphenol cable) into the Multi Access Blade transition module by securing the screws on both ends. Put the 50-pin Amphenol cable into the connector on the *bottom*, labeled *spans 9-16*.

Two Multi Access Blade MA-4 cards

To connect the E1 or T1 PRI telephony cables for two Multi Access Blade MA-4 cards, follow these steps:

Step 1 Locate the following Cisco Systems-supplied items:

- E1 or T1 PRI telephony cables
- breakout box (should already be mounted above the MeetingPlace server)
- trunk card interface cable assemblies (50-pin Amphenol cables)

Step 2 Plug the first E1 or T1 PRI telephony cable into the customer-supplied RJ-48c socket.

Step 3 Plug the other end of the first E1 or T1 PRI telephony cable into the slot labelled 1 on the far left of the front of the breakout box.

Step 4 Repeat steps 2 and 3 above until all the E1 or T1 PRI telephony cables are connected to the breakout box. Place the second, third, and fourth E1 or T1 PRI telephony cables, which correspond to the first Multi Access Blade MA-4 card, into connector slots 2, 3, and 4. Place the second set of four E1 or T1 PRI telephony cables, which corresponds to the second Multi Access Blade MA-4 card, into connector slots 9, 10, 11, and 12.

Note Slots 5-8 and 13-16 remain empty.

Step 5 Connect the trunk card cable assembly (50-pin Amphenol cable) for the first Multi Access Blade to the back of the breakout box by securing the screws on both ends. Looking at the back of the breakout box, put the first 50-pin Amphenol cable into the connector on the right.

Step 6 Connect the other end of the trunk card cable assembly (50-pin Amphenol cable) for the first Multi Access Blade into the Multi Access Blade transition module by securing the screws on both ends. Put the 50-pin Amphenol cable into the connector on the *bottom*, labeled *spans 9-16*.

Step 7 Repeat steps 5 and 6 above for the trunk card cable assembly (50-pin Amphenol cable) for the second Multi Access Blade. It should go into the connector on the left side of the breakout box and on the bottom of the Multi Access Blade in the connector labeled spans 9-16.

One Multi Access Blade MA-4 card and one Multi Access Blade MA-16 card

To connect the E1 or T1 PRI telephony cables for one Multi Access Blade MA-4 card and one Multi Access Blade MA-16 card, follow these steps:

Step 1 Locate the following Cisco Systems-supplied items:

- E1 or T1 PRI telephony cables
- breakout boxes (these should already be mounted above the MeetingPlace server)
- trunk card interface cable assemblies (50-pin Amphenol cables)

Step 2 Plug the first E1 or T1 PRI telephony cable into the customer-supplied RJ-48c socket.

Step 3 Plug the free end of the first E1 or T1 PRI telephony cable into the slot labelled 1 on the far left of the front of the first breakout box.

Step 4 Repeat steps 2 and 3 above until all the E1 or T1 PRI telephony cables are connected. Place the second, third, and fourth E1 or T1 PRI telephony cables, which correspond to the Multi Access Blade MA-4 card, into connector slots 2, 3, and 4 of the first breakout box. Place the remaining 16 E1 or T1 PRI telephony cables, which correspond to the Multi Access Blade MA-16 card, into the 16 connector slots on the front of the second breakout box. Start with the slots on the left and continue to the right.

Note Slots 5-16 in the first breakout box remain empty.

Step 5 Connect the trunk card cable assembly (50-pin Amphenol cable) for the first Multi Access Blade (the MA-4) to the back of the first breakout box by securing the screws on both ends. Looking at the back of the first breakout box, put the first 50-pin Amphenol cable into the connector on the right.

Step 6 Connect the other end of the trunk card cable assembly (50-pin Amphenol cable) for the first Multi Access Blade (the MA-4) into the Multi Access Blade transition module by securing the screws on both ends. Put the 50-pin Amphenol cable into the connector on the *bottom*, labeled *spans 9-16*.

Step 7 Repeat steps 5 and 6 above for the trunk card cable assemblies (50-pin Amphenol cables) for the second Multi Access Blade (the MA-16). The first cable should go into the connector on the left side of the breakout box and on the top of the Multi Access Blade in the connector labeled spans 1-8. The second cable should go into the connector on the right side of the breakout box and on the bottom of the Multi Access Blade in the connector labeled spans 9-16.

Two Multi Access Blade MA-16 cards

To connect the E1 or T1 PRI telephony cables for two Multi Access Blade MA-16 cards, follow these steps:

Step 1 Locate the following Cisco Systems-supplied items:

- E1 or T1 PRI telephony cables
- breakout boxes (these should already be mounted above the MeetingPlace server)
- trunk card interface cable assemblies (50-pin Amphenol cables)

Step 2 Plug the first E1 or T1 PRI telephony cable into the customer-supplied RJ-48c socket.

Step 3 Plug the other end of the first E1 or T1 PRI telephony cable into the slot labelled 1 on the far left of the front of the breakout box.

Step 4 Repeat steps 2 and 3 above until all the E1 or T1 PRI telephony cables are connected for the first MA-16. Place the second set of 16 E1 or T1 PRI telephony cables, which correspond to the second Multi Access Blade MA-16 card, into the connector slots on the second breakout box.

Step 5 Connect the trunk card cable assemblies (50-pin Amphenol cable) for the first Multi Access Blade to the back of the first breakout box by securing the screws on both ends. Looking at the back of the breakout box, put the first 50-pin Amphenol cable into the connector on the right.

Step 6 Connect the other end of the trunk card cable assembly (50-pin Amphenol cable) for the first Multi Access Blade into the Multi Access Blade transition module by securing the screws on both ends. Put the 50-pin Amphenol cable into the connector on the *bottom*, labeled *spans 9-16*.

Step 7 Repeat steps 5 and 6 above for the second trunk card cable assembly (50-pin Amphenol cable) for the first Multi Access Blade. It should go into the connector on the left side of the breakout box and on the right side of the Multi Access Blade in the connector labeled spans 9-16.

Step 8 Repeat steps 5, 6, and 7 above for the trunk card cable assemblies (50-pin Amphenol cables) for the second Multi Access Blade.

Connecting telephony cables for pure IP systems

Pure IP systems are configurations that only use IP functionality and do not have use any T1 CAS, T1 PRI or E1 functionality.

Note Pure IP systems do not use a breakout box.

All MeetingPlace servers with IP configurations are shipped with the necessary number of Multi Access Blades. Also shipped are the necessary number of IP LAN cables. The number of IP LAN cables you receive depends on the number of Multi Access Blades in your system. You need one IP LAN cable for every Multi Access Blade.

Looking at the back of the server, the Multi Access Blade transition modules for IP configurations begin in slot 16 on the left and move to the right. The Smart Blades begin in slot 1 and move to the left. They do not have any cables connected to them.

To connect the IP LAN cables, follow these steps:

Step 1 Locate the Cisco Systems-supplied IP LAN cables.

Step 2 Plug the first IP LAN cable into the customer-supplied RJ-48c socket.

Step 3 Plug the other end of the first IP LAN cable into the Ethernet 1 connector on the Multi Access Blade.

Step 4 Repeat steps 2 and 3 if you have more than one Multi Access Blade for the IP configuration.

Figure 3-24 illustrates the 8112 server's connections from the back of the server. This configuration supports 480 IP ports with one MA-16.

Figure 3-24 Back of Server (IP with 1 MA-16)

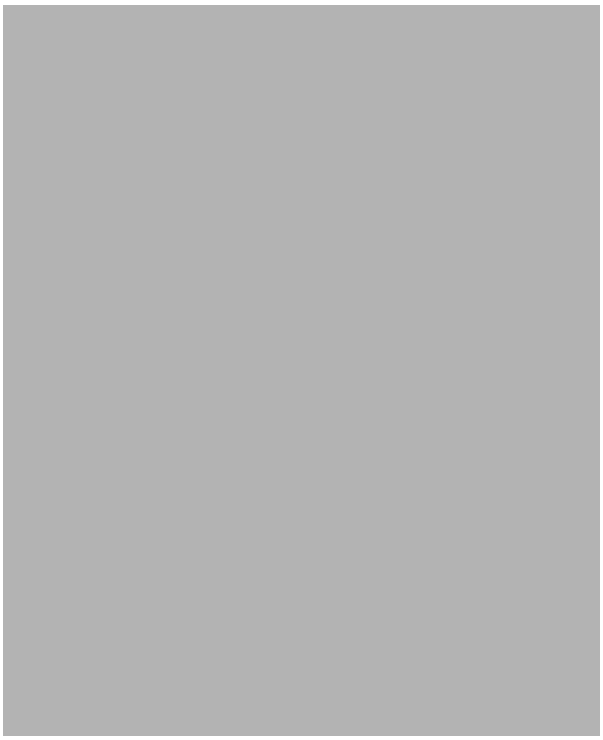


Figure 3-25 illustrates the 8112 server's connections from the back of the server. This configuration supports 120 IP ports with one MA-4.

Figure 3-25 Back of Server (IP with 1 MA-4)

Connecting telephony cables for mixed systems

A mixed system is an 8112 server with both an IP configuration and either a T1 CAS, T1 PRI, or E1 configuration.

Warning **Mixing protocols is not supported except in combination with IP ports. For example, a system cannot have both T1 and E1 ports configured but it can have T1 (either PRI or CAS) and IP ports or E1 and IP ports. Also, a system cannot have both T1 CAS and T1 PRI ports configured. Refer to Table 3-8**

Table 3-8 Allowed Blade Configurations

Not Allowed	Allowed
T1 CAS and E1	T1 PRI and IP
T1 PRI and E1	E1 and IP
T1 PRI and T1 CAS	T1 CAS and IP

All MeetingPlace servers are shipped with the necessary number of cards and cables. The number shipped depends on the type of mixed configuration.

- (For all mixed configurations) E1, T1 PRI, and IP configurations all use Multi Access Blades. The server is shipped with the necessary number of Multi Access Blades. The number of telephony cables shipped with the system depends on the number of ports being activated. You need one telephony cable for every 30 ports in an E1 system and one telephony cable for every 23 ports in a T1 PRI system.
- (For T1 CAS/IP configurations only) The server is shipped with the necessary number of T1 Smart Blades. Each T1 Smart Blade transition module in the back of the server has connectors for four trunk lines. The number of telephony cables shipped with the system depends on the number of ports being activated. You need one telephony cable for every 24 ports in a T1 CAS system. No breakout box is needed for this configuration.
- (For E1/IP and T1 PRI/IP configurations only) The server is shipped with one or two breakout boxes and cables, depending on the configuration. The necessary number of trunk card interface cable assemblies (50-pin Amphenol cables) is also shipped. These connect the breakout boxes to the Multi Access Blade transition modules.

For the non-IP portion of the mixed system:

- the T1 Smart Blade transition modules begin in slot 1 on the right and move to the left (for T1 CAS/IP configurations)
- the Multi Access Blade transition modules begin in slot 1 on the right and move to the left (for E1/IP and T1 PRI/IP configurations)

For the IP portion of the mixed system:

- the Multi Access Blade transition modules begin in slot 16 on the left and move to the right
- the Smart Blades begin after the last Multi Access Blade and do not have any cables connected to them

E1/IP or T1 PRI/IP system

To connect the telephony cables in a E1/IP or T1 PRI/IP system, follow these steps:

Step 1 Locate the following items:

- IP LAN cables
- E1 or T1 PRI telephony cables
- breakout box
- trunk card interface cable assemblies (50-pin Amphenol cables)

Step 2 Plug the IP LAN cable into the customer-supplied RJ-48c socket.

Step 3 Plug the other end of the IP LAN cable into the Ethernet 1 connector on the Multi Access Blade.

Step 4 Repeat steps 2 and 3 if you have two Multi Access Blades being used for the IP configuration.

Step 5 Depending on the configuration of your E1 or T1 PRI system, follow the steps in one of the following sections to connect the E1 or T1 PRI telephony cables:

- “One Multi Access Blade MA-16 card” section on page 3-26
- “One Multi Access Blade MA-4 card” section on page 3-30
- “Two Multi Access Blade MA-4 cards” section on page 3-31

- "One Multi Access Blade MA-4 card and one Multi Access Blade MA-16 card" section on page 3-31
- "Two Multi Access Blade MA-16 cards" section on page 3-32

Figure 3-26 illustrates a mixed system with 96 T1 CAS and 240 IP ports. Two Multi Access Blade MA-4s are used for the IP configuration and are in slots 15 and 16, shown on the left. For the T1 CAS configuration, there is a T1 Smart Blade in slot 1 and three Smart Blades in slots 2, 3, and 4.

Figure 3-26 Back of Server (Mixed System with 96 T1 CAS and 240 IP Ports)

Figure 3-27 illustrates a mixed system with 23 T1 PRI and 120 IP ports. The Multi Access Blade MA-4 used for the IP configuration is shown on the left in slot 16 and the Multi Access Blade MA-4 used for the T1 PRI configuration is shown on the right in slot 1. There is a Smart Blade in slot 2, where 23 ports are used for the T1 PRI configuration and 73 ports are used for the IP configuration and there is another Smart Blade in slot 3 to support the remaining 47 IP ports.

Figure 3-27 Back of Server (Mixed System with 23 T1 PRI and 120 IP Ports)

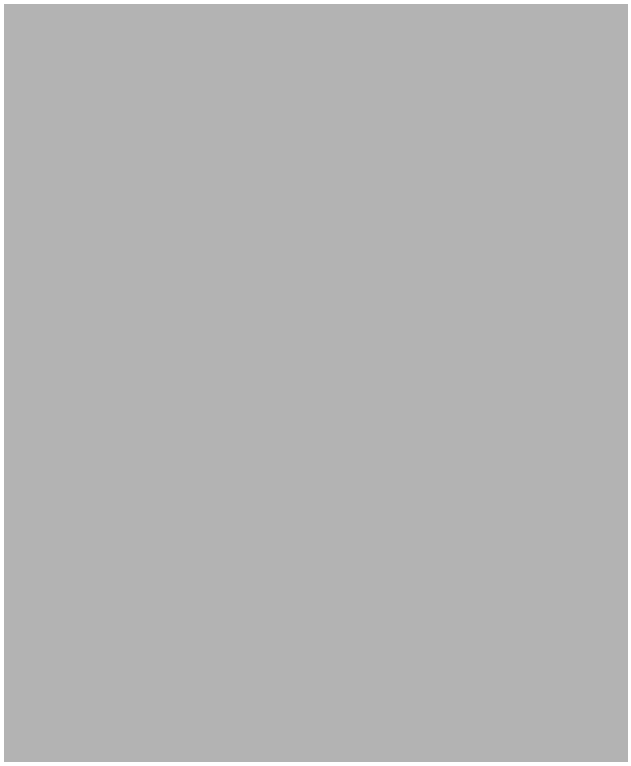
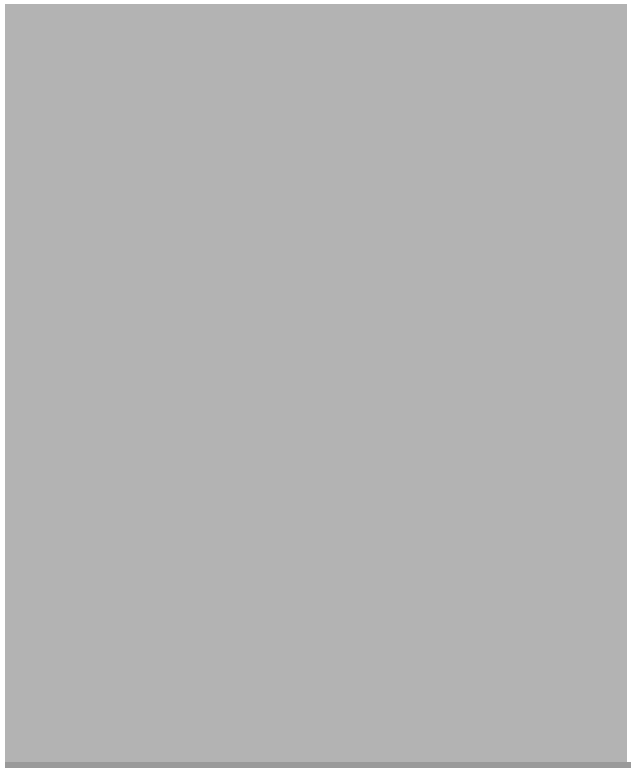


Figure 3-28 illustrates a mixed system with 480 E1 and 480 IP ports. The Multi Access Blade MA-16 used for the IP configuration is shown on the left in slot 16 and the Multi Access Blade MA-16 used for the E1 configuration is shown on the right in slot 1. There are ten Smart Blades (in slots 2, 3, 4, 5, 6, 11, 12, 13, 14, and 15) to support 960 ports.

Figure 3-28 Back of Server (Mixed System with 480 E1 and 480 IP Ports)



T1 CAS/IP system

To connect the telephony cables in a T1 CAS/IP system, follow these steps:

Step 1 Locate the following Cisco Systems-supplied items:

- IP LAN cables
- T1 CAS telephony cables

Step 2 Plug one end of the first Cisco Systems-supplied T1 CAS telephony cable into the customer-provided socket.

Step 3 Plug the other end of the first Cisco Systems-supplied T1 CAS telephony cable into the T1 Smart Blade transition module in the back of the server. The first T1 CAS telephony cable should be placed in the top most connector slot. The second T1 CAS telephony cable should be placed in the next connector slot moving down, and so on. A maximum of four T1 CAS telephony cables can be connected to any one T1 Smart Blade transition module.

Step 4 Repeat steps 2 and 3 until all the T1 CAS telephony cables are connected.

Step 5 Install tie wraps and label the T1 CAS telephony cables as needed.

Step 6 Plug the IP LAN cable into the customer-supplied RJ-48c socket.

Step 7 Plug the other end of the IP LAN cable into the Ethernet 1 connector on the Multi Access Blade transition module.

Step 8 Repeat steps 6 and 7 if you have two Multi Access Blades.

Installing and connecting the modem

This section describes how to install and connect the modem. Verify the following things are included in the modem package:

- modem
- modem cable
- modem power cable
- telephone extension cable

Installing the modem in T1 CAS and pure IP systems

Follow these instructions to install the modem in T1 CAS or pure IP systems. If you are installing a modem in a T1 PRI system or an E1 system, see "Installing the modem in T1 PRI and E1 systems" section on page 3-43.

Step 1 Place the modem on the back, right corner of the server, as you are looking at the front of the server. The modem cable connections should face the back of the server as in Figure 3-29.

The modem should remain here permanently.

Figure 3-29 Modem Placement and Connections

Step 2 Verify the modem's power switch is in the off position. The modem's power switch is on the side of the modem.

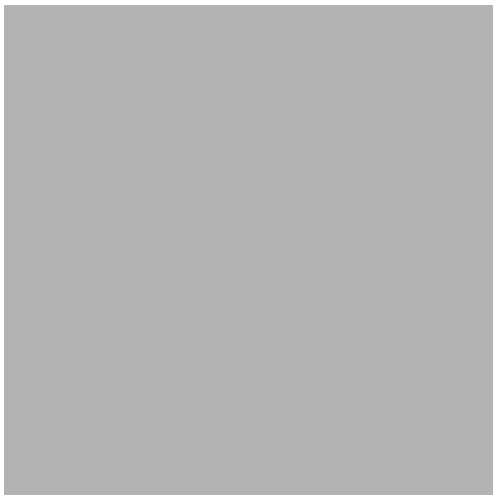
Step 3 Looking at the back of the server, connect the modem power cable to the far left position on the back of the modem. See Figure 3-29.

Step 4 Connect the other end of the modem power cable into the power outlet.

Step 5 Looking at the back of the server, connect the telephone extension cable to the far right position on the back of the modem, labeled "Line". There are two RJ-11 connectors on the modem. This cable should be placed in the far right connector. See Figure 3-29.

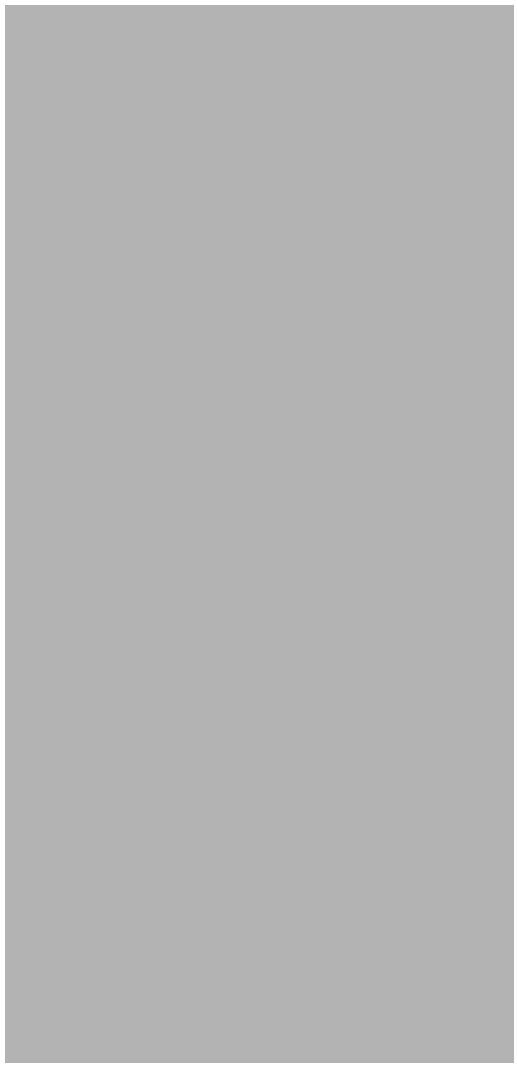
Step 6 Looking at the back of the server, connect the DB25 end (the larger connector) of the modem cable to the back of the modem. See Figure 3-30 to see which end is the DB25 end. See Figure 3-29 for the placement of the modem cable into the modem.

Figure 3-30 Modem Cable



Step 7 Connect the DB9 end (the smaller connector) of the modem cable to the COM 2 port on the CPU transition module in the back of the server. See Figure 3-30 to see which end is the DB9 end. See Figure 3-31 for the placement of the modem cable into the CPU transition module.

Figure 3-31 CPU Transition Module



Step 8 Connect the other end of the telephone extension cable to its source. The source should be a standard analog phone line, not an extension for a digital phone.

Step 9 Turn the modem power switch to the on position.

Installing the modem in T1 PRI and E1 systems

Follow these instructions to install the modem in T1 PRI and E1 systems.

Step 1 Verify the modem's power switch is in the off position. The modem's power switch is on the side of the modem.

Step 2 Looking at the back of the modem, connect the modem power cable to the far left position on the back of the modem.

Step 3 Connect the other end of the modem power cable into the power outlet.

Step 4 Looking at the back of the modem, connect the telephone extension cable to the far right position on the back of the modem, labeled “Line”. There are two RJ-11 connectors on the modem. This cable should be placed in the far right connector.

Step 5 Looking at the back of the modem, connect the DB25 end (the larger connector) of the modem cable to the back of the modem. See Figure 3-30 to see which end is the DB25 end.

Step 6 Connect the DB9 end (the smaller connector) of the modem cable to the COM 2 port on the CPU transition module in the back of the server. See Figure 3-30 to see which end is the DB9 end. See Figure 3-31 for the placement of the modem cable into the CPU transition module.

Step 7 Connect the other end of the telephone extension cable to its source. The source should be a standard analog phone line, not an extension for a digital phone.

Step 8 Turn the modem’s power switch to the on position.

Step 9 Looking at the back of the server, place the modem into the empty slot on the far left of the breakout box. See Figure 3-32. The modem should remain here permanently.

Figure 3-32 Breakout Box, Back View

Configuring the 8112 Server

This chapter explains how to configure and test a newly-installed 8112 server. It consists of the following activities:

- Connecting and setting up a laptop computer to the service port of a MeetingPlace server. Refer to "Connecting your laptop" section on page 4-1 and "Setting up your laptop" section on page 4-3.
- Powering up the server. Refer to "Powering up the server" section on page 4-17.
- Using the Command Line Interface (CLI) to configure the system using a laptop computer and information from the worksheets in the *MeetingPlace Audio Server 5.2 Installation Planning Guide*. Refer to "Configuring the system" section on page 4-18.
- Using MeetingTime to configure the system ports. Refer to "Using MeetingTime to configure ports" section on page 4-84.
- Testing the installation and configuration. Refer to "Testing the installation" section on page 4-95.

Note If this installation is part of a conversion from PCI to 8112 server, refer to the installation and upgrade document for the appropriate version. If you do not have access to this, please contact the Cisco TAC.

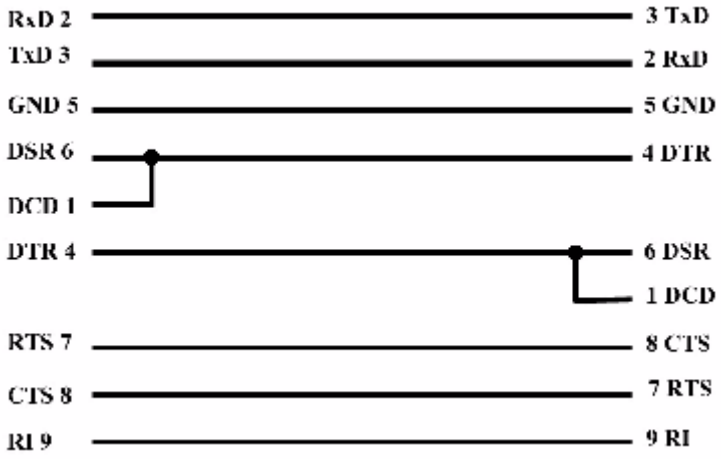
Connecting your laptop

To configure the 8112 server, you first need to connect your laptop to the server.

Step 1 Locate the female-to-female DB9 null modem cable that is part of the required toolkit listed in Appendix B, "Required Toolkit". See Figure 4-1 for cable pinouts if necessary.

Warning **Before proceeding, verify the null modem cable you are using has the correct wiring. Specifically, verify the connection between the DCD and DSR. A connectivity tester (part of the required toolkit in Appendix B, "Required Toolkit") can be used to test this.**

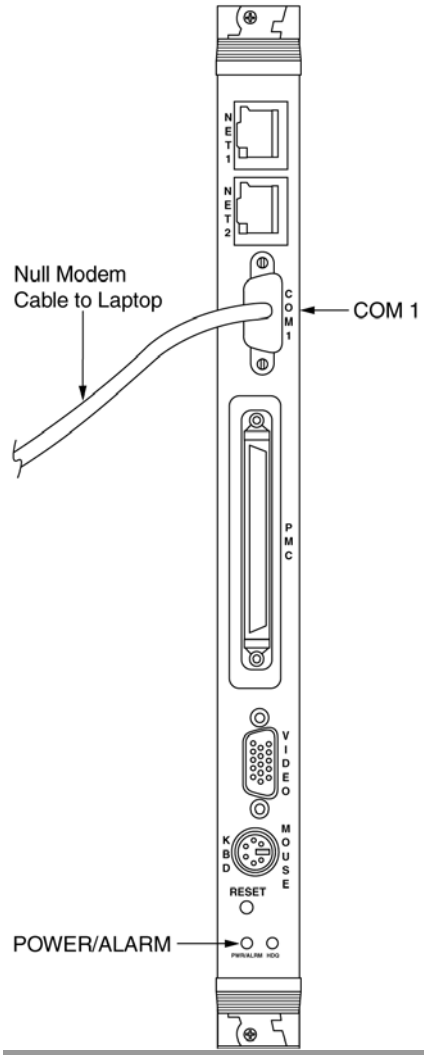
Figure 4-1 Null Modem Cable Pinouts



Step 2 Connect one end of the null modem cable to the COM 1 port on the CPU card in slot 7 in the front of the server. See Figure 4-2.

Step 3 Connect the other end of the null modem cable to the COM port on your laptop.

Figure 4-2 Null Modem Cable Connection to the 8112 Server



Setting up your laptop

The CLI command screen can be accessed by running terminal emulation software, such as ProComm, Windows Terminal, or HyperTerminal. Configure your laptop COM port with the parameters listed in Table 4-1.

Table 4-1 Laptop COM Port Parameters

Parameter	Value
Baud Rate	19200
Data Length	8 bits
Parity	None
Stop Bits	1

No phone number or area code is needed for direct connections to a COM port. Depending on the configuration of the laptop, the direct connection (9-pin connector) may be any of the COM ports, but most likely, COM 1.

Set up the terminal emulation software to emulate a VT100 terminal. If the laptop is connected to a server and the operating system is running, the login prompt appears. It is sometimes necessary to press **Enter** once or twice.

If the server is not powered on yet, you will not see the login prompt.

Note As mentioned above, there are several ways to telnet to the server. HyperTerminal is available on all operating systems. Therefore, below is an example of how to configure HyperTerminal and turn on terminal logging. If you are not using HyperTerminal, the instructions will vary. HyperTerminal is also used to connect a laptop to the front console of the server and, in this case, it does not use telnet.

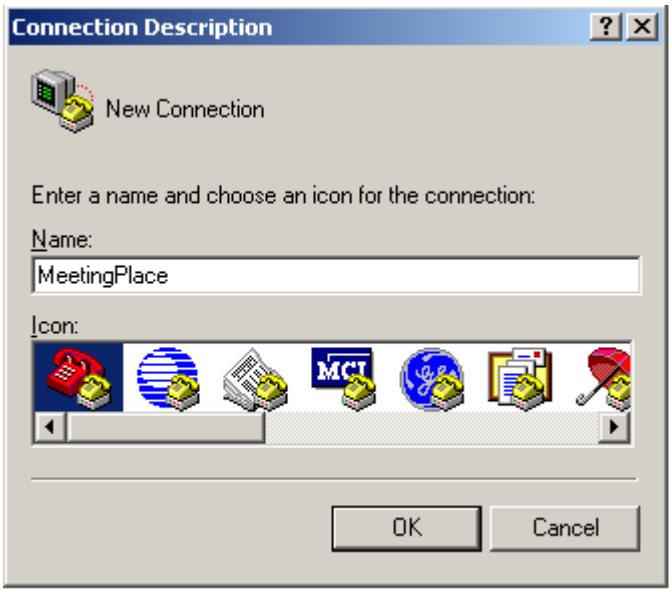
Example of setting up HyperTerminal

This section explains how to set up HyperTerminal to telnet to the MeetingPlace server. Keep in mind, there are several ways to telnet to the server. Since HyperTerminal is available on all operating systems, this is used as an example. These instructions are for Windows 2000 operating systems. If you are not using this version, the HyperTerminal instructions may vary.

Step 1 Go to **Start** | **Programs** | **Accessories** | **Communications** | **HyperTerminal**. The HyperTerminal dialog box appears.

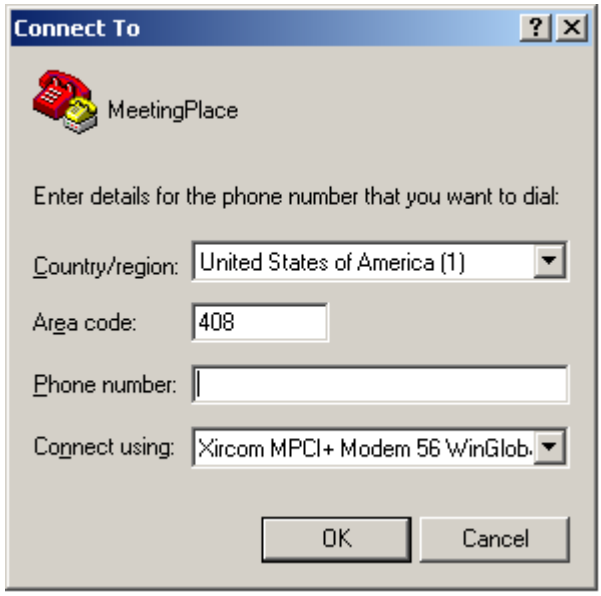
Step 2 Enter a name for your connection, for example, “MeetingPlace”. See Figure 4-3. Click **OK**.

Figure 4-3 Connection Description Dialog Box



Step 3 The Connect to... dialog box opens. See Figure 4-4.

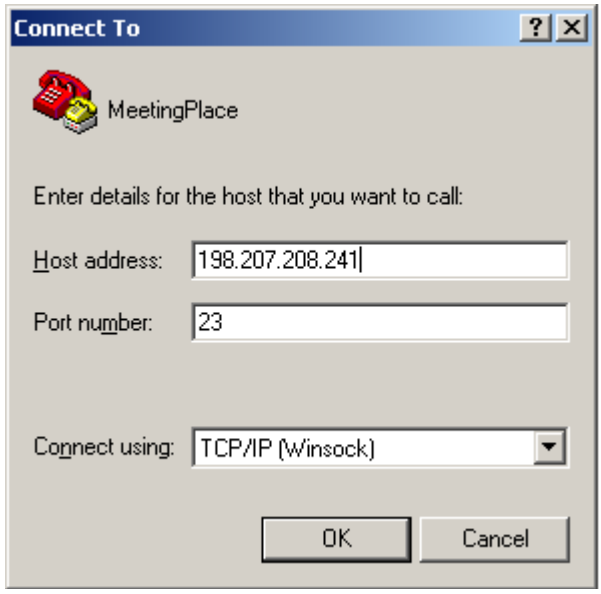
Figure 4-4 Connect To Dialog Box



Step 4 In the "Connect Using" drop down box, select "TCP/IP (Winsock)". The "Connect to..." dialog box reappears.

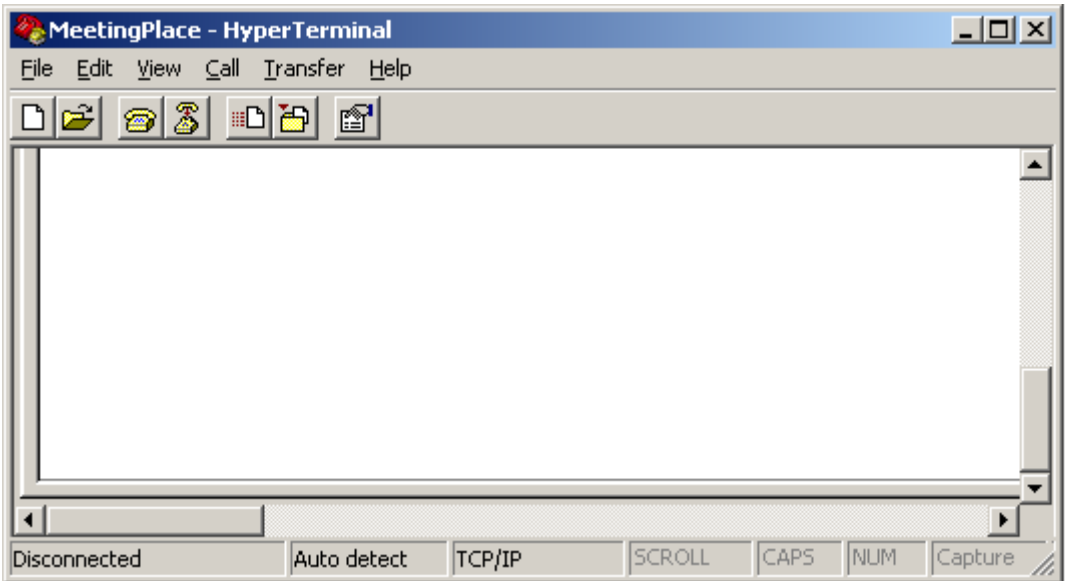
Step 5 In the "Host address" field, type **198.207.208.241**. In the "Port number" field, type **23**. See Figure 4-5. Click **OK**.

Figure 4-5 Connection Settings Dialog Box



Step 6 The HyperTerminal window appears. See Figure 4-6

Figure 4-6 HyperTerminal Window



Step 7 If the server is already powered on, press **Enter** a few times to see the MeetingPlace tech$ prompt.

If the 8112 server is not powered on yet, you do not see the login prompt.

Logging your HyperTerminal session

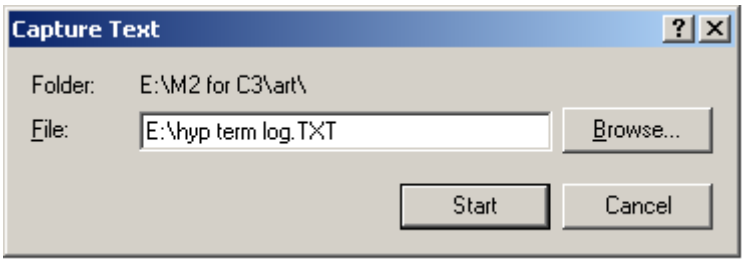
It is always a good idea to generate a log of your session so you can refer to it in the future, if necessary. This example refers to logging a session using HyperTerminal. If you are not using HyperTerminal, the instructions may vary. To turn terminal logging on in HyperTerminal:

Step 1 Go to the **Transfer** menu in the HyperTerminal window.

Step 2 Select **Capture Text**.

Step 3 Choose a location to save the file and note the location so you can retrieve the file later. Click **Start**. See Figure 4-7.

Figure 4-7 Capture Text Dialog Box



Setting up dial-up networking

This section explains how to set up dial-up networking on a Windows 2000 operating system to connect to the MeetingPlace server via a modem.

Step 1 On your Windows 2000 system, right click on the **My Network Places** icon on your desktop.

Step 2 Select **Properties**.

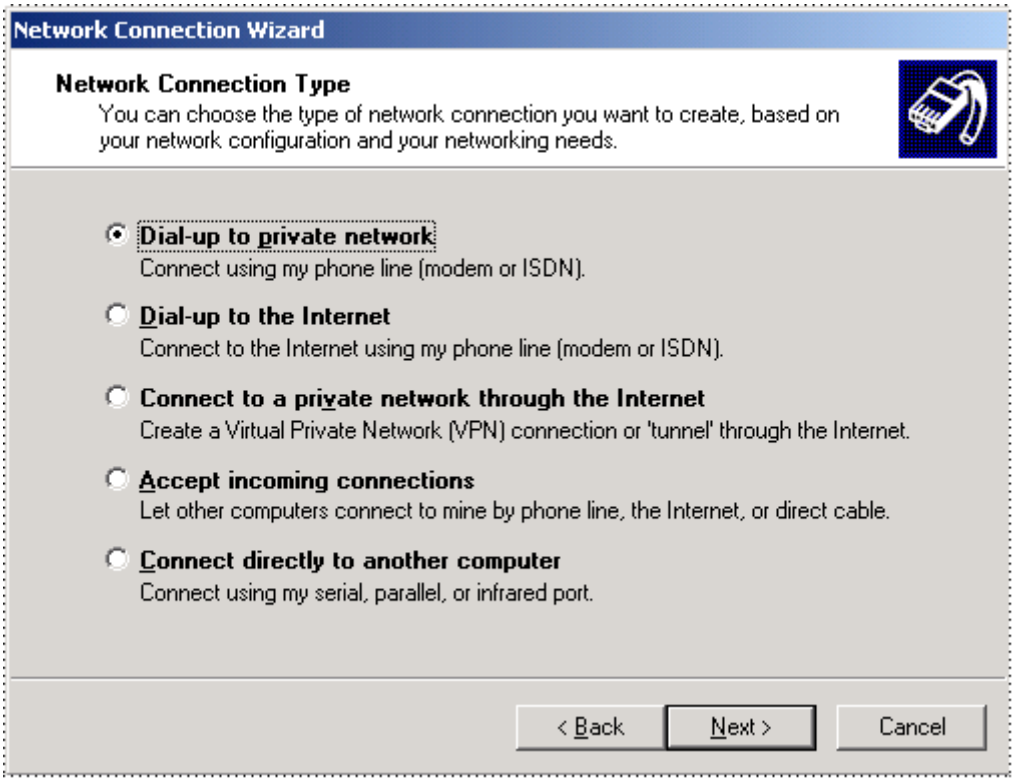
Step 3 Double click **Make New Connection**.

Step 4 The Network Connection Wizard dialog box opens as in Figure 4-8. Click **Next**.

Figure 4-8 Network Connection Wizard Dialog Box

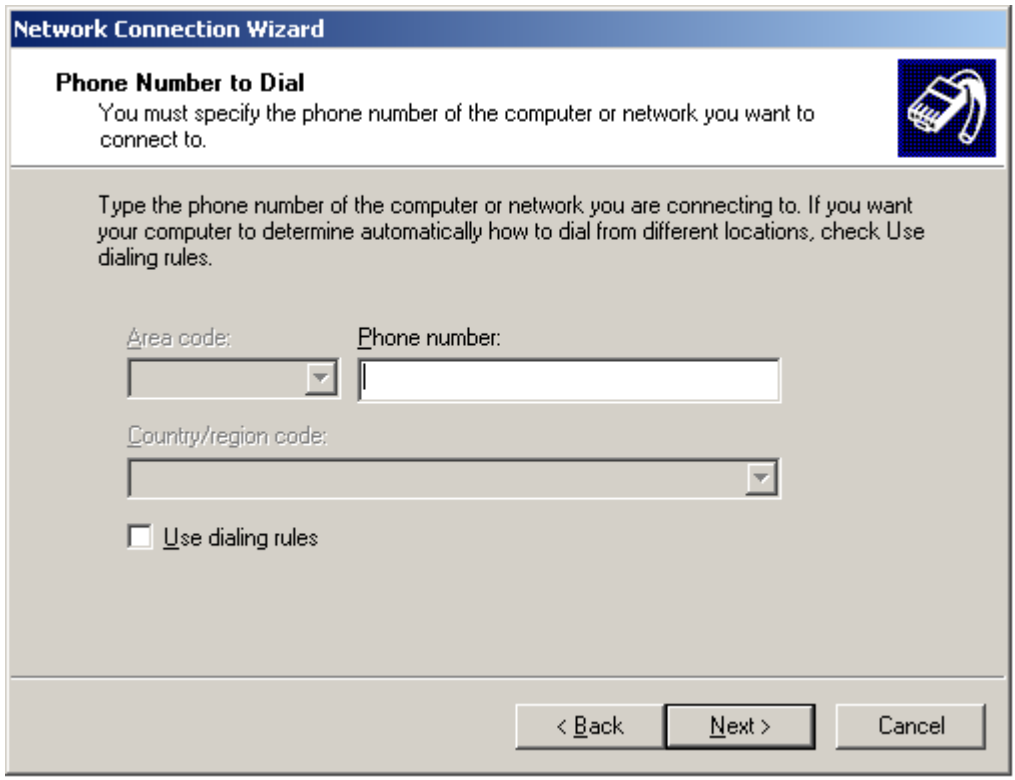
Step 5 The Network Connection Type dialog box appears as in Figure 4-9. Select **Dial-up to private network** and click **Next**.

Figure 4-9 Network Connection Type Dialog Box



Step 6 See Figure 4-10. If you have more than one dial-up device on your computer, you may not see this dialog box at this time. Instead you may see a dialog box asking you to choose a dial-up device. Choose the dial-up device you want to use and press **Next**. You should then see the dialog box in Figure 4-10.

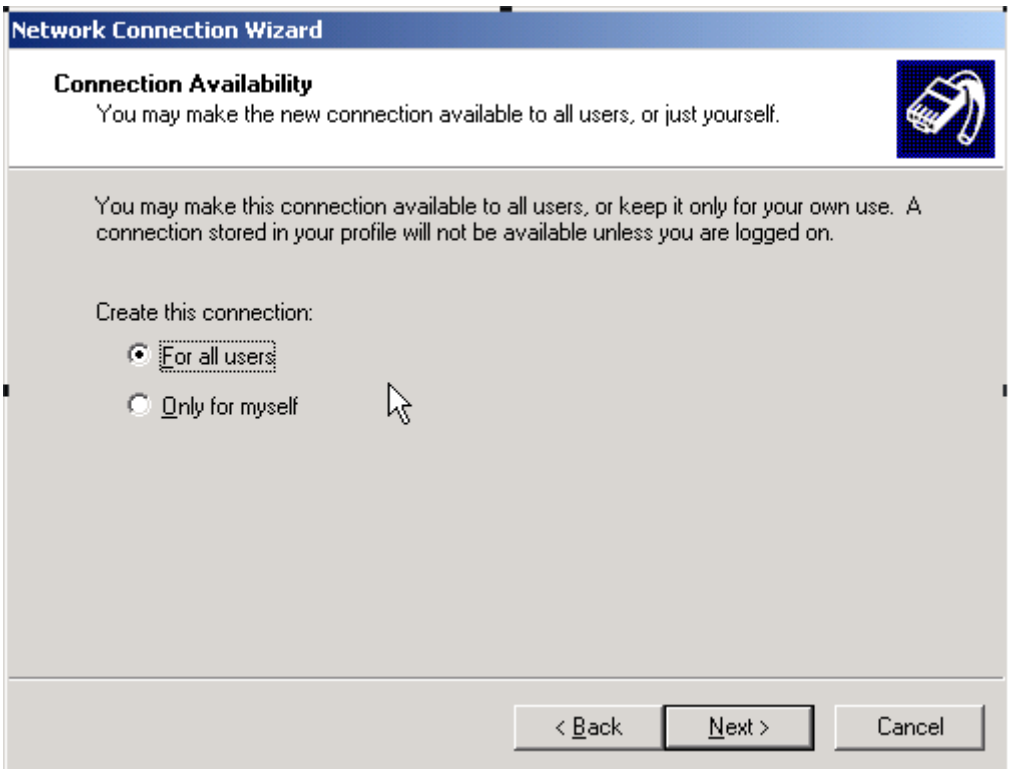
Figure 4-10 Phone Number to Dial Dialog Box



Step 7 Type the MeetingPlace modem number in the phone number field and click **Next**.

Step 8 The Connection Availability dialog box appears as in Figure 4-11. Select **For all users**. Click **Next**.

Figure 4-11 Connection Availability Dialog Box

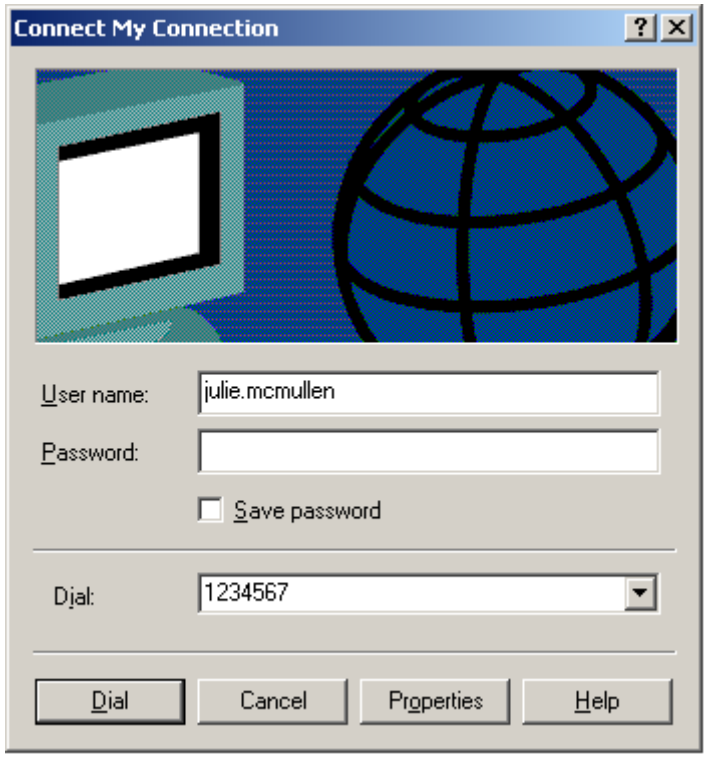


Step 9 The Completing the Network Connection Wizard dialog box appears. Enter the company name in the field labeled "Type the name you want to use for this connection" as in Figure 4-12. Click **Finish**.

Figure 4-12 Completing the Network Connection Wizard Dialog Box

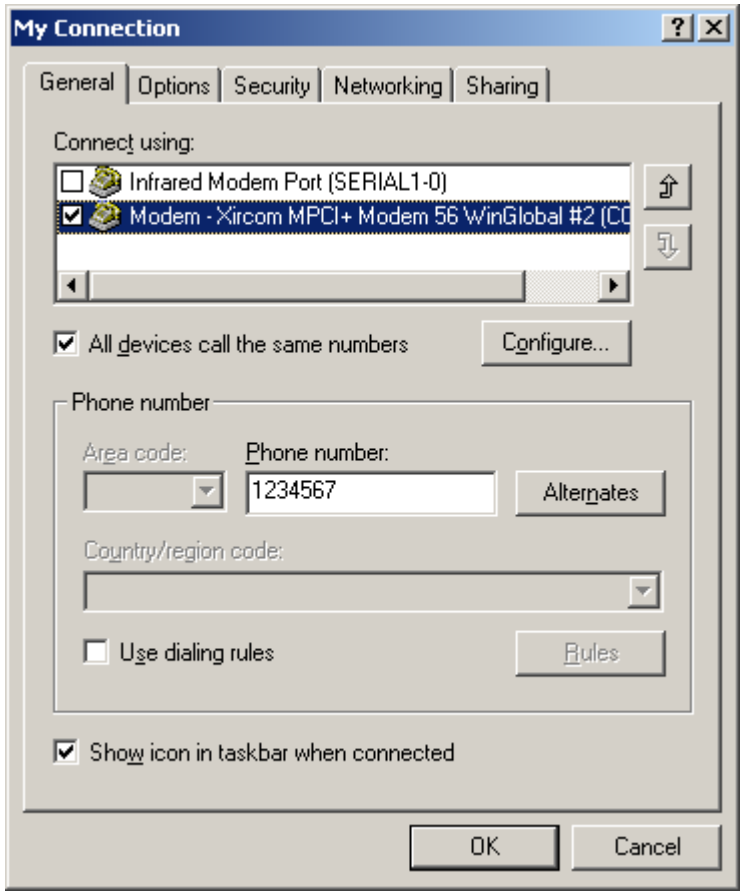
Step 10 The Connection dialog box appears as in Figure 4-13. Click **Properties**.

Figure 4-13 Connection Dialog Box



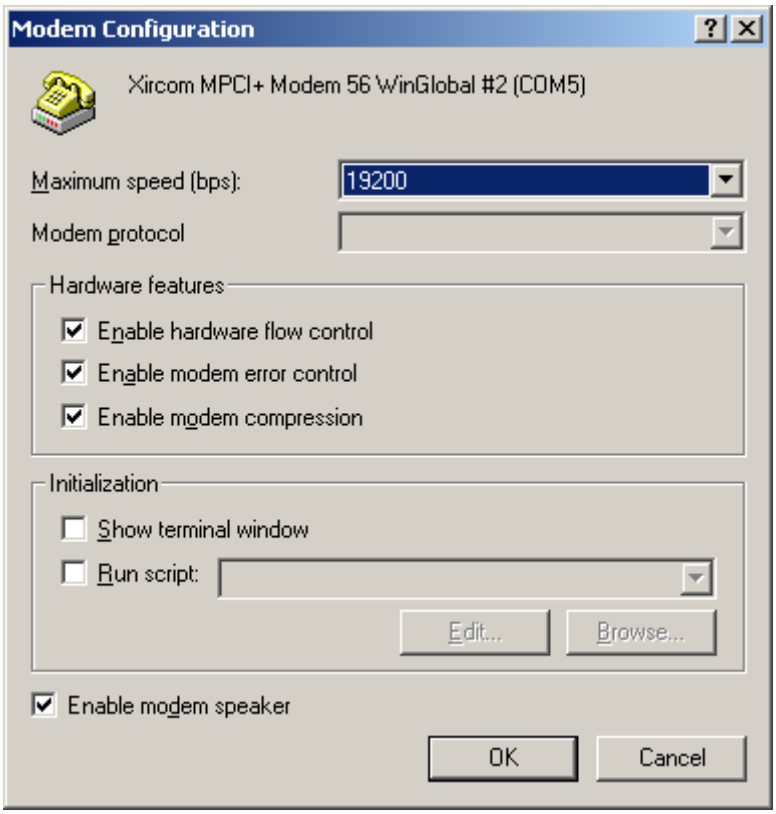
Step 11 The Connection Properties dialog box appears. See Figure 4-14. Select the **General** tab and click **Configure**.

Figure 4-14 Connection Properties Dialog Box



Step 12 The Modem Configuration dialog box appears. Change the maximum speed to 19200 bps as in Figure 4-15. Click **OK.**

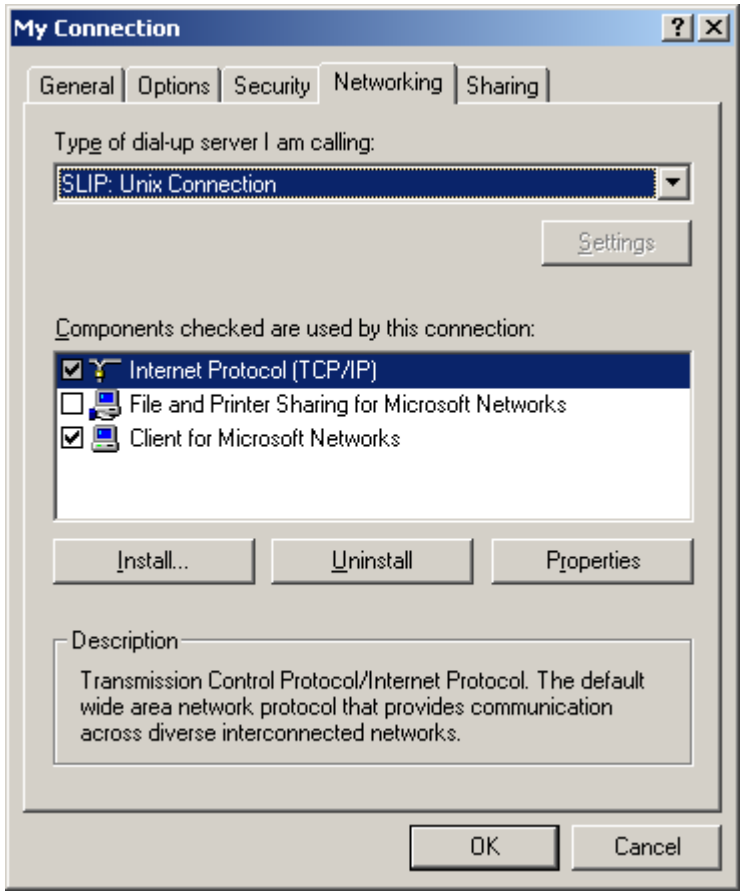
Figure 4-15 Modem Configuration Dialog Box



Step 13 The Connection Properties dialog box appears. Click the **Networking** tab. Figure 4-16 appears.

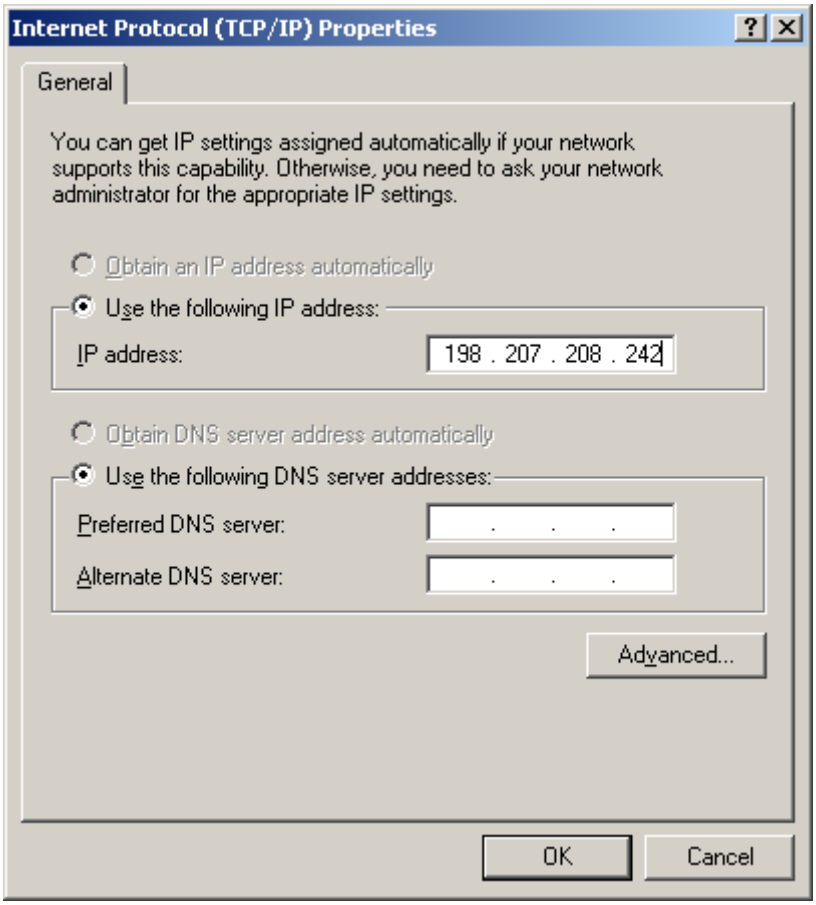
Step 14 Under **Type of dial-up server I am calling**, select “SLIP: Unix Connection”. Under **Components checked are used by this connection:**, highlight “Internet Protocol (TCP/IP)”. Click **Properties**.

Figure 4-16 Networking Tab Dialog Box



Step 15 The Internet Protocol (TCP/IP) Properties dialog box appears as in Figure 4-17. Select **Use the following IP address** and type **198.207.208.242** in the IP address field. Click **OK** to exit the Properties window.

Figure 4-17 Internet Protocol (TCP/IP) Properties Dialog Box



Step 16 Click **OK** to exit the Networking window. Your connection is now complete.

Testing the modem connection

Step 1 Right click on the **My Network Places** icon on your desktop.

Step 2 Select **Properties**. The Network and Dial-up Connections window appears.

Step 3 Double click the connection you just created.

Step 4 Click **Dial**.

This should connect you to the MeetingPlace server. If it does not, double check the steps in "Setting up dial-up networking" section on page 4-7. If you still have problems, contact the Cisco TAC.

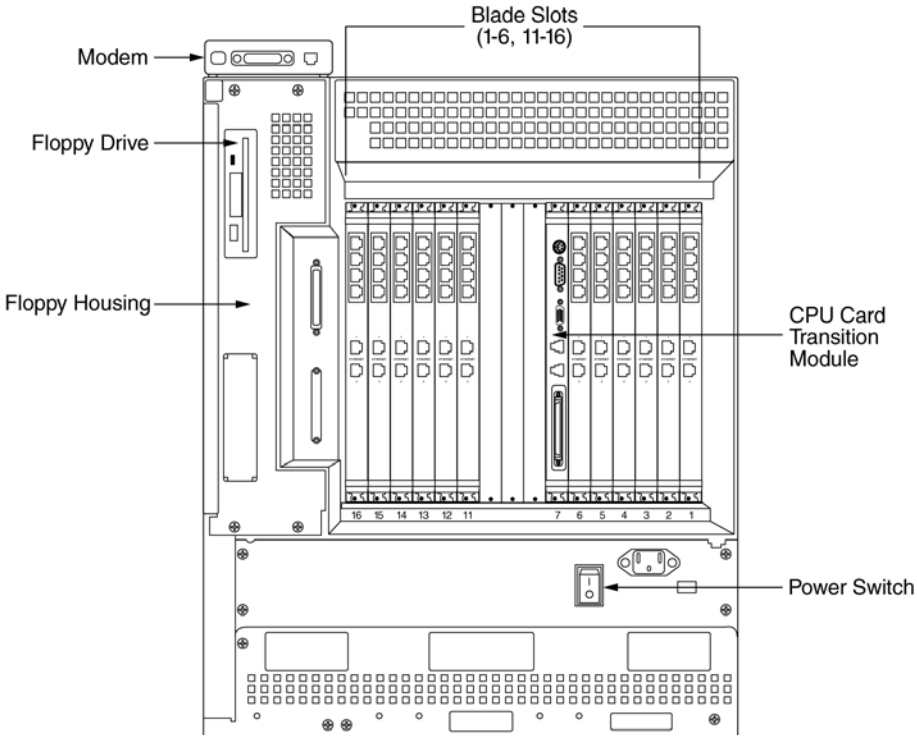
Powering up the server

This section describes how to power up MeetingPlace.

Note The system can take 5-10 minutes to complete initialization. Please take note of the time you power up the system and wait 10 minutes before becoming concerned if it has not come up.

Step 1 Move the 8112 server power switch to the on ("I") position. See Figure 4-18.

Figure 4-18 8112 Server's Power Switch Location



Step 2 Allow up to 10 minutes for the server to initialize. To confirm the server has come up properly, you must connect your laptop to the 8112 server.

If your laptop has not been connected and set up, complete "Connecting your laptop" section on page 4-1 and "Setting up your laptop" section on page 4-3.

If your laptop is already connected and set up, you can verify the server has come up when the laptop displays the line "MeetingPlace is UP".

Note If the line "MeetingPlace is UP" does not appear on the laptop screen:

- Make sure all the cards are securely seated by checking if the blue LED light is on below any of the cards. If the blue light is on, the card or transition module is not seated properly. Refer to "Understanding the 8112 server's LEDs" section on page 2-6 for instructions on removing and installing any of the cards or transition modules.

- Turn the power switch to the off ("O") position.
- Check all connections to make sure they are secure.
- After verifying that all components are secure, repeat the power up procedure. If MeetingPlace does not properly initialize on the second try, contact the Cisco TAC.

Step 3 At the prompt, enter your user name and password. Correct information causes Figure 4-19 to appear. This allows you to enter commands on the Command Line Interface (CLI). For information about CLI commands, refer to Appendix A, "CLI Reference".

Figure 4-19 Logging into the CLI

```
user name: tech
Password:
Last login: Wed Oct 29 11:51:12 from lager
************************************************************
*                      MeetingPlace(tm)                    *
*                by Latitude Communications                *
*                                                          *
*    Copyright (c) 1993-2004 Latitude Communications, Inc. *
*                    All rights reserved.                  *
************************************************************
Conference server 5.2.0   S/N: not set
Wed Oct 29 14:55:03 PST 2003
meetingplace:tech$
```

Configuring the system

This section describes the details for using your laptop to configure the MeetingPlace server. It covers instructions for configuring:

- LAN parameters via the "net" command
- time zone via the "timezone" command
- T1 Smart Blades, Multi Access Blades, and Smart Blades via the "blade" command
- date and time via the "date" command

Configuring the LAN parameters

The LAN parameters identify the MeetingPlace server on the customer's TCP/IP network. The site contact supplies the LAN parameters via the *MeetingPlace Audio Server 5.2 Installation Planning Guide* worksheet 3-3. To configure the LAN parameters, follow this procedure.

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 Type **getether** and press **Enter**. The Ethernet address of the MeetingPlace server appears as in Figure 4-20. (For more information about the "getether" command, see the "getether" section on page A-28.)

Figure 4-20 getether Command

```
meetingplace:tech$ getether
0001af0bc2cd
```

Step 3 Record the Ethernet address for future use.

Step 4 At the tech$ prompt, type **net** and press **Enter**. Figure 4-21 appears. (For more information about the "net" command, see "net" section on page A-38.)

Figure 4-21 net Command Menu

```
meetingplace:tech$ net
 1) View the server & site configuration
 2) Modify the server configuration
 3) Select another server (current unit = #0)
99) Quit
Select:
```

Step 5 Type **2** and press **Enter** to modify the server configuration. Figure 4-22 appears.

Figure 4-22 net Command Modify Menu

```
Select: 2

 1) View the current configuration
 2) Select a different site for this server
 3) Change the host and site names
 4) Change server IP address and Ethernet address
 5) Change site subnet mask or broadcast addr
 6) Change site routing information
 7) Change network time protocol servers
99) Return to the main menu
```

Step 6 Select **3**, **4**, **5**, **6**, and **7** in order and follow the prompts to enter values using the *MeetingPlace Audio Server 5.2 Installation Planning Guide* worksheet 3-3.

See Table 4-2 for the details of each parameter.

Table 4-2 8112 Server Configuration Parameters

Parameter	Explanation
Active	System status, non-editable.
Description	Designates three names: *Host name* — The DNS name tied to the server's IP address. *Host description* — The name of the server as seen in MeetingTime and MeetingPlace Web. It is helpful to use MeetingPlace in this field since it can be different from the TCP/IP name. *Site name* — An arbitrary name for the location of the server.
IP address	Must correspond to the customer's network requirements. See *MeetingPlace Audio Server 5.2 Installation Planning Guide* worksheet 3-3.
Ethernet address	The Media Access Control (MAC) address of the server. It corresponds to the MAC hardware address that uniquely identifies each node of a network. During setup the "getether" command produced this value.
NTP server	This IP address designates the Network Time Protocol (NTP) server on the customer's LAN. It allows MeetingPlace to synchronize its clock with the network time server.
Site subnet mask	A bit mask used to determine what subnet an IP address belongs to. This should be specified by the customer's network administrator. See *MeetingPlace Audio Server 5.2 Installation Planning Guide* worksheet 3-3.
Site broadcast address	Address used to broadcast packets on the LAN segment. See *MeetingPlace Audio Server 5.2 Installation Planning Guide* worksheet 3-3.
Site default gateway	Address of the gateway that accepts and routes information to other networks. See *MeetingPlace Audio Server 5.2 Installation Planning Guide* worksheet 3-3.
Route daemon	Yes or No. Specifies if the MeetingPlace route daemon should be enabled or disabled.

See Figure 4-23 for an example of changing the host and site names.

Figure 4-23 net Command Change Host and Site Names

```
Select: 3
Enter new host name [molson]: molson
Enter new host description [MeetingPlace]: MeetingPlace
Enter new site name [Home Site]: Home Site
 1) View the current configuration
 2) Select a different site for this server
 3) Change the host and site names
 4) Change server IP address and Ethernet address
 5) Change site subnet mask or broadcast addr
 6) Change site routing information
 7) Change network time protocol servers
99) Return to the main menu
```

See Figure 4-24 for an example of changing the IP address and Ethernet address.

Figure 4-24 net Command Change Server IP Address and Ethernet Address

```
Select: 4
Enter new IP address [172.20.21.13]: 172.20.21.13

Please enter the 12-digit Ethernet address (e.g., 0000c0112233).
[0001af0bc2cd]: 0001af0bc2cd

 1) View the current configuration
 2) Select a different site for this server
 3) Change the host and site names
 4) Change server IP address and Ethernet address
 5) Change site subnet mask or broadcast addr
 6) Change site routing information
 7) Change network time protocol servers
99) Return to the main menu
```

See Figure 4-25 for an example of changing the site subnet mask or broadcast address.

Figure 4-25 net Command Change Site Subnet Mask or Broadcast Address

```
Select: 5
Enter new subnet mask [255.255.0.0]: 255.255.0.0

Enter new broadcast address [172.20.255.255]: 172.20.255.255

 1) View the current configuration
 2) Select a different site for this server
 3) Change the host and site names
 4) Change server IP address and Ethernet address
 5) Change site subnet mask or broadcast addr
 6) Change site routing information
 7) Change network time protocol servers
99) Return to the main menu
```

See Figure 4-26 for an example of changing the site routing information.

Figure 4-26 net Command Change Site Routing Information

```
Select: 6

To specify no default gateway, enter "0.0.0.0".
Enter new default gateway address [172.20.1.1]: 172.20.1.1

Enable the route daemon? [no] no

 1) View the current configuration
 2) Select a different site for this server
 3) Change the host and site names
 4) Change server IP address and Ethernet address
 5) Change site subnet mask or broadcast addr
 6) Change site routing information
 7) Change network time protocol servers
99) Return to the main menu
```

See Figure 4-27 for an example of changing the network time protocol servers.

Figure 4-27 net Command Change Network Time Protocol Servers

```
Select: 7

The IP addresses for up to three Network Time Protocol servers
may be entered.
To clear an entry, use the address "0.0.0.0".
NTP server #1 [198.207.208.114]: 198.207.208.114
NTP server #2 [198.207.208.84]: 198.207.208.84
NTP server #3 [0.0.0.0]: 0.0.0.0

 1) View the current configuration
 2) Select a different site for this server
 3) Change the host and site names
 4) Change server IP address and Ethernet address
 5) Change site subnet mask or broadcast addr
 6) Change site routing information
 7) Change network time protocol servers
99) Return to the main menu
```

Step 7 Type **99** and press **Enter** to quit modifying.

Step 8 Type **y** and press **Enter** to commit to the changes you made.

Step 9 Type **1** and press **Enter** from the "net" command menu to view and confirm the new configuration. See Figure 4-28.

Figure 4-28 net Command New Configuration Screen

```
meetingplace:tech$ net
 1) View the server & site configuration
 2) Modify the server configuration
 3) Select another server (current unit = #0)
99) Quit
Select: 1
Current server configuration:
    Unit:                  #0 (molson)
    Active:                YES
    Description:           MeetingPlace
    Kind:                  Conference server
    IP Address:            172.20.21.13
    Ethernet address:      0001af0bc2cd
    NTP servers:           198.207.208.114 198.207.208.84
    Site:                  #0 (Home Site)
    Site subnet mask:      255.255.0.0
    Site broadcast addr:   172.20.255.255
    Site default gateway:  172.20.1.1
    Route daemon:          disabled
 1) View the server & site configuration
 2) Modify the server configuration
 3) Select another server (current unit = #0)
99) Quit
Select:
```

Step 10 Type **99** and press **Enter** to quit the "net" command utility.

Configuring the server's time zone

This section describes how to configure the server's time zone. If the time zone is not correctly set, meetings will occur at the wrong time.

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see "Logging your HyperTerminal session" section on page 4-6.

Step 2 At the tech$ prompt, enter **timezone** and press **Enter**. Figure 4-29 appears. (For more information about the "timezone" command, see "timezone" section on page A-64.)

Figure 4-29 timezone Command Menu

```
meetingplace:tech$ timezone
Please select the region where this server is installed:
  1) Europe
  2) Far East
  3) North America
 99) quit
Select:
```

Step 3 Type the number that applies to the region where the server is located and press **Enter**. Figure 4-30 appears.

Figure 4-30 timezone Command Region Menu

```
Select: 3
Please select the time zone for this server.

The following timezones are available:
  1) America/Anchorage
  2) America/Chicago
  3) America/Denver
  4) America/Edmonton
  5) America/Fort_Wayne
  6) America/Halifax
  7) America/Los_Angeles
  8) America/Montreal
  9) America/New_York
 10) America/Phoenix
 11) America/Vancouver
 12) America/Winnipeg
 13) Pacific/Honolulu
 99) no action
Select:
```

Step 4 Type the number that applies to the server location and press **Enter**. Figure 4-31 is an example of the screen that appears.

Figure 4-31 timezone Command Selection and Confirmation Screen

```
Select: 7

The local time zone (PST) is 480 minutes west of GMT
Daylight savings time policy: US/Canada

Please confirm (y/n):
```

Step 5 Enter **y** and press **Enter** to confirm your selection, or **n** and press **Enter** to abort your selection. The line "DONE" and the tech$ prompt appear.

Configuring blades

This section describes how to configure blades. There are four types of blades:

- T1 Smart Blade
- Multi Access Blade (MA-16)
- Multi Access Blade (MA-4)
- Smart Blade

Refer to Table 4-3 for an explanation of each.

Table 4-3 Blade Types

Blade Type	Explanation
T1 Smart Blade	Provides both PRC and MSC functionality along with necessary trunk interface functionality for digital T1 CAS telephone lines.
Multi Access Blade (MA-16 and MA-4)	Provides the necessary trunk interface card functionality for E1 digital telephony, T1 PRI functionality, and IP-based telephony. The Multi Access Blade supports both Euro ISDN and QSIG telephony protocols, T1 PRI support for North America (United States and Canada), and G.711 and G.729a audio encoding for IP. MA-16: Supports up to 16 spans (up to 480 IP ports) MA-4: Supports up to 4 spans (up to 120 IP ports)
Smart Blade	Provides both PRC and MSC functionality in a single card.

Warning **Mixing protocols is not supported except in combination with IP ports. For example, a system cannot have both T1 and E1 ports configured but it can have T1 (either PRI or CAS) and IP ports or E1 and IP ports. Also, a system cannot have both T1 CAS and T1 PRI ports configured. Refer to Table 4-4**

Table 4-4 Allowed Blade Configurations

Not Allowed	Allowed
T1 CAS and E1	T1 PRI and IP
T1 PRI and E1	E1 and IP
T1 PRI and T1 CAS	T1 CAS and IP

There are five sections that describe how to configure your 8112 server:

- "Configuring a T1 CAS system" section on page 4-27
- "Configuring a T1 PRI system" section on page 4-34
- "Configuring an E1 system" section on page 4-46
- "Configuring a pure IP system" section on page 4-59
- "Examples of mixed system configurations" section on page 4-72

Configuring a T1 CAS system

This section explains how to configure T1 Smart Blades and Smart Blades for a T1 CAS configuration.

Note If this is a mixed T1 CAS/IP configuration, refer to the "Examples of mixed system configurations" section on page 4-72. If this is a pure IP installation, refer to the "Configuring a pure IP system" section on page 4-59. If this is part of a T1 PRI installation, refer to the "Configuring a T1 PRI system" section on page 4-34. If this is part of an E1 installation, refer to the "Configuring an E1 system" section on page 4-46.

Caution The necessary cables should already be attached to the transition modules on the back of the server. If they are not, refer to the "Connecting the system cables" section on page 3-18.

The "blade" command is used to configure all ports. Follow this procedure to configure the necessary T1 Smart Blades and Multi Access Blades (for the IP portion of the configuration). Refer to the examples following this section for more detailed information. For more information about the "blade" command, see the "blade" section on page A-8.

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 At the tech$ prompt, type **blade -t <number of T1 ports>** and press **Enter** for a pure T1 CAS system without any IP configuration

Step 3 Confirm the "blade" command you entered and type **y** and press **Enter**. If you entered the wrong command, type **n** and press **Enter** and then re-enter the correct command.

The system tells you what it is configuring. The tech$ prompt appears when configuration is complete. See Figure 4-32.

Figure 4-32 blade Command — T1 CAS

```
meetingplace:tech$ blade -t <# T1 ports>
This will reset many DB tables, are you sure?  (y/n): y

Configuring "X" T1 ports

Restart the system for changes to take effect
meetingplace:tech$
```

Step 4 Verify your configuration by typing **blade** and pressing **Enter**.

Step 5 Confirm the screen output is correct for your configuration.

Step 6 Type **x** and press **Enter** to exit the "blade" command utility.

Example of a T1 CAS configurations

This section explains how to use the "blade" command when configuring 1152 T1 CAS ports.

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 At the tech$ prompt, type **blade -t 1152** and press **Enter**.

Step 3 Confirm the "blade" command you entered and type **y** and press **Enter**. If you entered the wrong command, type **n** and press **Enter**, then re-enter the correct command.

The server responds by telling you how many ports it is configuring. When the tech$ prompt appears, it is complete. See Figure 4-33.

Figure 4-33 blade Example for 1152 T1 CAS Ports

```
meetingplace:tech$ blade -t 1152
This will reset many DB tables, are you sure?  (y/n): y

Configuring 1152 T1 ports

Restart the system for changes to take effect
meetingplace:tech$
```

Step 4 Verify your configuration by typing **blade** and pressing **Enter**.

Step 5 Confirm the screen output is like Figure 4-34.

Figure 4-34 blade Confirmation for 1152 T1 CAS Ports

```
meetingplace:tech$ blade
Slot  Card    Type    CardId  Ports
 1    CG6000C  T1       0     0-23, 24-47, 48-71, 72-95
 2    CG6000C  T1       1     96-119, 120-143, 144-167, 168-191
 3    CG6000C  T1       2     192-215, 216-239, 240-263, 264-287
 4    CG6000C  T1       3     288-311, 312-335, 336-359, 360-383
 5    CG6000C  T1       4     384-407, 408-431, 432-455, 456-479
 6    CG6000C  T1       5     480-503, 504-527, 528-551, 552-575
 11   CG6000C  T1       6     576-599, 600-623, 624-647, 648-671
 12   CG6000C  T1       7     672-695, 696-719, 720-743, 744-767
 13   CG6000C  T1       8     768-791, 792-815, 816-839, 840-863
 14   CG6000C  T1       9     864-887, 888-911, 912-935, 936-959
 15   CG6000C  T1       10    960-983, 984-1007, 1008-1031, 1032-1055
 16   CG6000C  T1      11    1056-1079, 1080-1103, 1104-1127, 1128-1151

*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program

Enter command:
```

Step 6 Type **x** and press **Enter** to exit the “blade” command utility.

Configuring spans for a T1 CAS system

T1 spans connect to the T1 Smart Blade transition modules in the back of the server.

Note The T1 spans are automatically activated and configured with default settings when the “blade” command is run. Table 4-5 lists the default span configuration.

Check the worksheets in the *MeetingPlace Audio Server 5.2 Installation and Planning Guide* to see if your system is configured this way. If these default settings are accurate for this installation, you do not need to complete this section. If the default settings are not accurate for this installation, complete the steps that follow.

Table 4-5 Default T1 CAS Span Configuration

Parameter	Default	Explanation	Possible Values	X
Activate the DTI span?	y	Specifies if the span is active.	• y = active • n = inactive	
Framing	ESF	Specifies the framing protocol used on this span. Determined by the service provider. *We recommend using ESF only.*	• D4 • ESF	
Zero code suppression	B8ZS	Specifies the zero code suppression for the span. Determined by the service provider. *We recommend using B8ZS only.*	• none • B8ZS • jammed bit	
Timing	external	Specifies if MeetingPlace should get clock timing from the PBX/Central Office or if timing is generated by MeetingPlace. At least one span should always be designated external.	• internal • external (the span is connected to the public network or a trusted system)	
External sync priority	none. The T1 span connected to the T1 Smart Blade in slot 1, line A gets sync priority 1, line B gets 2, etc.	Specifies the priority of the spans that are set for external timing. The system always tries to synchronize from the highest priority span. If the synchronization span goes down, the system automatically switches synchronization to the next highest span. If a higher priority span comes up, the system automatically synchronizes off of it.	• 1-255 (1 is the highest, 255 is the lowest) • never	
Trunk [x]	Numbering is done in order (1, 2, 3, etc.). For example, Trunk [1]:port 0 Trunk [2]:port 1 Trunk [3]:port 2	Specifies which port in the database is assigned to the specific hardware trunk on the card.	• number	

Table 4-5 Default T1 CAS Span Configuration (continued)

Parameter	Default	Explanation	Possible Values	X
Remote loopback to network	n	Specifies if the span should be put into a loopback mode for testing from the remote end.	• y = yes • n = no (normal operation)	
Internal data loopback	n	Specifies if the span should loop back locally for running diagnostics.	• y = yes • n = no (normal operation)	
Port group	0	Specifies the number of the port group.	• 0 (T1 CAS) • 1 (IP) • 2 (E1) • 3 (T1 PRI)	
Active?	y (if you use a blade to configure T1)	Specifies if the port group is active.	• y = yes • n = no	
Card type	T1	Specifies the type of card.	• none • T1 • analog • E1 • IP	
Signaling protocol	wink start	Specifies the signaling protocol.	• loop start • wink start • ground start • clear channel • E1 • IP • protocol table	
Protocol table	0	Specifies the number of the protocol table to copy from.	• number from 0 to 99	
Number of DID digits expected	0	Specifies the number of DID digits.	• number from 0 to 6	

Table 4-5 Default T1 CAS Span Configuration (continued)

Parameter	Default	Explanation	Possible Values	X
Default access type	combined access	Specifies the access type	• Combined access • DID meeting • Profile • MeetingNotes • loop through transfer • EBSApp1004 • EBSApp1005 • EBSApp1007 • EBS Xfer test • NewApp1011 • Choose music • Spanish samples • Goto123123_1015	
Language	English (US)	Specifies which language to use.	• English (US) • English (UK) • no language	
Human assistance?	n	Specifies if human assistance is allowed.	• y = yes • n = no	
Flash transfer?	n	Specifies if this can be flash transferred.	• y = yes • n = no	
Outdial?	y	Specifies if this can be outdialed on.	• y = yes • n = no	

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 At the tech$ prompt, type **span** and press **Enter**. Figure 4-35 appears. For more information about the "span" command, see the "span" section on page A-59.

Figure 4-35 span Command Menu

```
meetingplace:tech$ span
MeetingPlace is up
*****   S P A N   C O N F I G   M E N U   *****
        1)  View DTI span record(s)
        2)  Modify DTI span record
        x)  Exit program
Enter command:
```

Step 3 Type **2** and press **Enter** to modify a span record. Figure 4-36 appears.

Figure 4-36 span Record Selection

```
Enter command: 2
Enter DTI span record number [0..47] : 0
```

Step 4 Type the number of the span record that needs to be modified and press **Enter**. In this example, span record 0 is being configured so type **0** and press **Enter**. The first five lines of Figure 4-36 appear.

Figure 4-37 span Record Configuration

```
Enter command: 2
Enter DTI span record number [0..47] : 0
------------- UNIT 0  SPAN 0  --------------
--- To skip over a field, just press <cr> ---
  Activate the DTI span?         [y] :
  Framing                      [ESF] :
  Zero code suppression [      B8ZS] :
  Timing                  [external] :
  External sync priority     [    1] :
  Trunk [ 1]              [port   0] :
  Trunk [ 2]              [port   1] :
  Trunk [ 3]              [port   2] :
  Trunk [22]              [port  21] :
  Trunk [23]              [port  22] :
  Trunk [24]              [port  23] :
  Remote loopback to network?    [n] :
  Internal data loopback?        [n] :
 Enter command:
```

Step 5 Enter values as indicated by Table 4-5 on page 4-30. Press **Enter** after you enter each value and the next line appears.

If you exceed the number of ports configured by the factory, an error message appears.

Step 6 Press **Enter**. The "span" menu appears as in Figure 4-35 on page 4-33.

Step 7 Type **2** and press **Enter** to configure another span or type **x** and press **Enter** when all spans have been configured.

Note This is the end of the section "Configuring a T1 CAS system". Proceed to the "Configuring the system's date and time" section on page 4-81 to complete configuration.

Configuring a T1 PRI system

This section explains how to configure Multi Access Blades and Smart Blades for a T1 PRI system.

Note If this is part of a T1 PRI/IP mixed configuration, refer to the "Examples of mixed system configurations" section on page 4-72. If this is part of a T1 CAS system, refer to the "Configuring a T1 CAS system" section on page 4-27. If this is part of an E1 system, refer to the "Configuring an E1 system" section on page 4-46. If this is part of a pure IP system, refer to the "Configuring a pure IP system" section on page 4-59.

Caution The necessary cables should already be attached to the transition modules on the back of the server. If they are not, refer to the "Connecting the system cables" section on page 3-18.

The "blade" command is used to configure all ports. Follow this procedure to configure the necessary Multi Access Blades and Smart Blades. Refer to the examples following this section for more detailed information. For more information about the "blade" command, see the "blade" section on page A-8.

In a T1 PRI configuration, the maximum number of ports per span is 23. The maximum number of T1 PRI ports for the 8112 server is 736 because each Multi Access Blade can support up to 16 spans. The 8112 server can have two MA-16 Multi Access Blades for a total of 32 spans. 32 spans x 23 ports each = 736 total ports.

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 At the tech$ prompt, type **blade -p <number of T1 PRI ports>** and press **Enter** for a pure T1 PRI system without any IP configuration

Step 3 Confirm the "blade" command you entered and type **y** and press **Enter**. If you entered the wrong command, type **n** and press **Enter**, then re-enter the correct command.

The system tells you what it is configuring. The tech$ prompt appears when the configuration is complete. See Figure 4-38.

Figure 4-38 blade Command — T1 PRI

```
meetingplace:tech$ blade -p <# T1 PRI ports>
This will reset many DB tables, are you sure?  (y/n): y

Configuring "X" T1 PRI ports

Restart the system for changes to take effect
meetingplace:tech$
```

Step 4 Verify your configuration by typing **blade** and pressing **Enter**.

Step 5 Confirm the screen output is correct for your configuration.

Step 6 Type **x** and press **Enter** to exit the "blade" command utility.

Examples of T1 PRI configuration

The following sections provide configuration instructions for example T1 PRI configurations:

- "736 T1 PRI ports" section on page 4-35
- "368 T1 PRI ports" section on page 4-36

736 T1 PRI ports

This section explains how to use the "blade" command when configuring 736 T1 PRI ports.

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 At the tech$ prompt, type **blade -p 736** and press **Enter**.

Step 3 Confirm the "blade" command you entered and type **y** and press **Enter**. If you entered the wrong command, type **n** and press **Enter**, then re-enter the correct command.

The server responds by telling you how many ports it is configuring. When the tech$ prompt appears, it is complete. See Figure 4-39.

Figure 4-39 blade Example for 736 T1 PRI Ports

```
meetingplace:tech$ blade -p 736
This will reset many DB tables, are you sure?  (y/n): y

Configuring 736 T1 PRI ports

Restart the system for changes to take effect
meetingplace:tech$
```

Step 4 Verify your configuration by typing **blade** and pressing **Enter**.

Step 5 Confirm the screen output is like Figure 4-40.

Figure 4-40 blade Confirmation for 736 T1 PRI Ports

```
meetingplace:tech$ blade
Slot    Card    Type    CardId  Ports
 1      TP1610   T1       0     0-22, 23-45, 46-68, 69-91,
                                92-114, 115-137, 138-160, 161-183
                                184-206, 207-229, 230-252, 253-275,
                                276-298, 299-321, 322-344, 345-367
 2      TP1610   T1       1     377-399, 400-422, 423-445, 446-468,
                                467-489, 490-512, 513-535, 536-558
                                559-581, 582-604, 605-627, 628-650
                                651-673, 674-696, 697-719, 720-736
 3      CG6000C  SB       2
 4      CG6000C  SB       3
 5      CG6000C  SB       4
 6      CG6000C  SB       5
 11     CG6000C  SB       6
 12     CG6000C  SB       7
 13     CG6000C  SB       8
 14     CG6000C  SB       9
 15     no card
 16     no card

*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program
```

Step 6 Type **x** and press **Enter** to exit the "blade" command utility.

368 T1 PRI ports

This section explains how to use the "blade" command when configuring 368 T1 PRI ports.

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 At the tech$ prompt, type **blade -p 368** and press **Enter**.

Step 3 Confirm the "blade" command you entered and type **y** and press **Enter**. If you entered the wrong command, type **n** and press **Enter**, then re-enter the correct command.

The server responds by telling you how many ports it is configuring. When the tech$ prompt appears, it is complete. See Figure 4-41.

Figure 4-41 blade Example for 368 T1 PRI Ports

```
meetingplace:tech$ blade -p 368
This will reset many DB tables, are you sure?  (y/n): y

Configuring 368 T1 PRI ports

Restart the system for changes to take effect
meetingplace:tech$
```

Step 4 Verify your configuration by typing **blade** and pressing **Enter**.

Step 5 Confirm the screen output is like Figure 4-42.

Figure 4-42 blade Confirmation for 368 T1 PRI Ports

```
meetingplace:tech$ blade
Slot    Card    Type    CardId  Ports
 1      TP1610   T1       0     0-22, 23-45, 46-68, 69-91,
                                92-114, 115-137, 138-160, 161-183
                                184-206, 207-229, 230-252, 253-275,
                                276-298, 299-321, 322-344, 345-367
 2      CG6000C  SB       1
 3      CG6000C  SB       2
 4      CG6000C  SB       3
 5      CG6000C  SB       4
 6      no card
 11     no card
 12     no card
 13     no card
 14     no card
 15     no card
 16     no card

*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program
```

Step 6 Type **x** and press **Enter** to exit the “blade” command utility.

Configuring port groups

You can create port groups so that a group of ports can be configured with the same parameters. The instructions on creating and configuring port groups is below.

Warning **If this installation requires NSF codes, refer to Appendix D, "Configuring NSF Codes" before proceeding. If you are unsure if NSF codes are required, refer to Appendix D to confirm.**

Step 1 At the tech$ prompt, type **port** and press **Enter**. Figure 4-43 appears. (For more information about the "port" command, see "port" section on page A-44.)

Figure 4-43 port Command Menu

```
meetingplace:tech$ port
MeetingPlace is up

*****   P O R T / G R O U P   C O N F I G   M E N U   *****

        1)  View port record(s)
        2)  Modify port record
        3)  Copy port records
        4)  View group record(s)
        5)  Modify group record
        x)  Exit program

Enter command:
```

Step 2 Type **5** and press **Enter** to modify the group record. The second line in Figure 4-44 appears.

Figure 4-44 Modifying the Port Group

```
Enter command: 5
Enter port group record number [0..31] : 0

------------     GROUP  0      --------------
--- To skip over a field, just press <cr> ---
  Activate the group?             [y] :  y
  Card type                 [    T1] :  T1
  Signaling          [              ] :  protocol table
  Protocol table                [ 0] :  2
  Number of DID digits          [ 0] :
  Human assistance?              [n] :
  Flash transfer?                [n] :
  Outdial?                       [y] :

Enter command: x
```

Step 3 Type the appropriate port group record number. In this example, it is port group 0, so type **0** and press **Enter**. The rest of Figure 4-44 appears.

Step 4 Type **y** and press **Enter** to activate the port group.

Step 5 Type **T1** and press **Enter** to select the card type. Continue typing and entering the appropriate values for the system configuration.

Step 6 Type **protocol table** and press **Enter** to select signaling.

Step 7 Select the appropriate protocol table number. In this example, it is protocol table 2, so type **2** and press **Enter**. Refer to Table 4-6 for a list of default protocol tables.

Note The protocol table contains the configuration information for the type of signaling used. All T1 PRI systems are shipped from the factory with protocol table 2 set to use the default setting of AT&T PRI protocol, protocol table 3 to use Nortel PRI, and table 4 to use Bell PRI. If this is not correct for your system, it can be changed via the "protparm" command. Refer to the "protparm" section on page A-47 for more information on the "protparm" command.

Note If this is part of an upgrade from a pre-5.1 release, the default protocol tables 3 and 4 will not be correct. To resolve this, use the "protparm" command to delete tables 3 and 4. This restores them to the defaults as listed in Table 4-6.

Step 8 Repeat this procedure if more than one port group is needed.

Step 9 Type **x** and press **Enter** to exit the "port" utility.

Table 4-6 Default Protocol Table Settings — T1 PRI

Protocol Table Number	Default Protocol
2	AT&T PRI
3	Nortel PRI
4	Bell PRI

Assigning ports to port groups

You can assign specific ports to port groups so that all ports in that group have the same parameters.

Step 1 At the tech$ prompt, type **port** and press **Enter**. See Figure 4-45.

Figure 4-45 Assigning Port Record

```
Enter port record number [0..91] : 0

------------- UNIT 0  PORT 0  --------------
--- To skip over a field, just press <cr> ---
  Uses port group              [   2] :
```

Step 2 Type **2** and press **Enter** to modify a port record. The first line in Figure 4-45 appears.

Step 3 Type the port number and press **Enter**. In this example, it is port 0, so type **0** and press **Enter**. The rest of Figure 4-45 appears.

Step 4 Enter the number of the port group and press **Enter**. In this example, it is port group 0, so enter **0** and press **Enter**.

Note If you would like to copy this port record to other ports, refer to the "Copying port records" section on page 4-40.

Step 5 Type **x** and press **Enter** to exit the "port" utility.

Copying port records

Copying port records provides an easy way to copy the port record for one port to as many ports as desired. Follow these steps to do this:

Step 1 If you are not already accessing the "port" command, at the tech$ prompt, type **port** and press **Enter**. See Figure 4-46.

Figure 4-46 Copying Port Records

```
meetingplace:tech$ port
MeetingPlace is up

*****   P O R T / G R O U P   C O N F I G   M E N U   *****

        1)  View port record(s)
        2)  Modify port record
        3)  Copy port records
        4)  View group record(s)
        5)  Modify group record
        x)  Exit program

Enter command: 3
Enter port record number to copy from [0..959] : 0
Enter port(s) to copy to [0-959] : 1-959
Copied to port record(s) 1-959.

Enter command: x
```

Step 2 Type **3** and press **Enter** to copy port records.

Step 3 Enter the port number you want to copy from and press **Enter**, as shown in line 14 of Figure 4-46. In this example, it is port 0, so type **0** and press **Enter**.

Step 4 Enter the port numbers you want to copy to and press **Enter**, as shown in line 15 of Figure 4-46. In this example, all ports are being configured with the same parameters as port 0, so type **1-959** and press **Enter**.

Step 5 The system tells you which ports were copied to, as shown in line 16 of Figure 4-46.

Step 6 Type **x** and press **Enter** to exit the "port" utility.

Configuring T1 spans for a T1 PRI system

T1 spans connect to the Multi Access Blade transition modules in the back of the server.

Note The T1 spans are automatically activated and configured with default settings when the "blade" command is run. Table 4-7 lists the default span configuration.

Check the worksheets in the *MeetingPlace Audio Server 5.2 Installation and Planning Guide* to see if your system is configured this way. If these default settings are accurate for this installation, you do not need to complete this section. If the default settings are not accurate for this installation, complete the steps that follow.

Table 4-7 Default T1 PRI Span Configuration

Parameter	Default	Explanation	Possible Values	X
Activate the DTI span?	y	Specifies if the span is active.	• y = active • n = inactive	
Framing	ESF	Specifies the framing protocol used on this span. Determined by the service provider. *We recommend using ESF only.*	• D4 • ESF	
Zero code suppression	B8ZS	Specifies the zero code suppression for the span. Determined by the service provider. *We recommend using B8ZS only.*	• none • B8ZS • jammed bit	
Timing	external	Specifies if MeetingPlace should get clock timing from the PBX/Central Office or if timing is generated by MeetingPlace. At least one span should always be designated external.	• internal • external (the span is connected to the public network or a trusted system)	
External sync priority	none. The T1 span connected to the T1 Smart Blade in slot 1, line A gets sync priority 1, line B gets 2, etc.	Specifies the priority of the spans that are set for external timing. The system always tries to synchronize from the highest priority span. If the synchronization span goes down, the system automatically switches synchronization to the next highest span. If a higher priority span comes up, the system automatically synchronizes off of it.	• 1-255 (1 is the highest, 255 is the lowest) • never	
Trunk [x]	Numbering is done in order (1, 2, 3, etc.). For example, Trunk [1]:port 0 Trunk [2]:port 1 Trunk [3]:port 2	Specifies which port in the database is assigned to the specific hardware trunk on the card.	• number	

Table 4-7 Default T1 PRI Span Configuration (continued)

Parameter	Default	Explanation	Possible Values	X
Remote loopback to network	n	Specifies if the span should be put into a loopback mode for testing from the remote end.	• y = yes • n = no (normal operation)	
Internal data loopback	n	Specifies if the span should loop back locally for running diagnostics.	• y = yes • n = no (normal operation)	
Port group	3	Specifies the number of the port group.	• 0 (T1 CAS) • 1 (IP) • 2 (E1) • 3 (T1 PRI)	
Active?	y (if you use a blade to configure T1)	Specifies if the port group is active.	• y = yes • n = no	
Card type	T1	Specifies the type of card.	• none • T1 • analog • E1 • IP	
Signaling protocol	wink start	Specifies the signaling protocol.	• loop start • wink start • ground start • clear channel • E1 • IP • protocol table	
Protocol table	0	Specifies the number of the protocol table to copy from.	• number from 0 to 99	
Number of DID digits expected	0	Specifies the number of DID digits.	• number from 0 to 6	

Table 4-7 Default T1 PRI Span Configuration (continued)

Parameter	Default	Explanation	Possible Values	X
Default access type	combined access	Specifies the access type	• Combined access • DID meeting • Profile • MeetingNotes • loop through transfer • EBSApp1004 • EBSApp1005 • EBSApp1007 • EBS Xfer test • NewApp1011 • Choose music • Spanish samples • Goto123123_1015	
Language	English (US)	Specifies which language to use.	• English (US) • English (UK) • no language	
Human assistance?	n	Specifies if human assistance is allowed.	• y = yes • n = no	
Flash transfer?	n	Specifies if this can be flash transferred.	• y = yes • n = no	
Outdial?	y	Specifies if this can be outdialed on.	• y = yes • n = no	

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 At the tech$ prompt, type **e1span** and press **Enter**. Figure 4-47 appears. (For more information about the "e1span" command, see the "e1span" section on page A-22.)

Figure 4-47 e1span Command Menu

```
meetingplace:tech$ e1span
MeetingPlace is up

*****   E 1 S P A N   C O N F I G   M E N U   *****

        1)  View ACTI span record(s)
        2)  Modify ACTI span record
        x)  Exit program

Enter command:
```

Step 3 Type **2** and press **Enter** to modify a span record. Figure 4-48 appears.

Figure 4-48 span Record Selection

```
Enter command: 2
Enter DTI span record number [0..47] : 0
```

Step 4 Type the number of the span record that needs to be modified and press **Enter**. In this example, span record 0 is being configured so type **0** and press **Enter**. The first five lines of Figure 4-49 appear.

Figure 4-49 span Record Configuration

```
Enter command: 2
Enter ACTI span record number [0..47] : 0

-----------  Unit 0  ACTI Span 0  ------------
--- To skip over a field, just press <cr> ---
  Activate the ACTI span?       [y] :
  Timing                 [external] :
  External sync priority    [    1] :
  Framing                 [   CRC4] :
  Zero Code Suppression      [HDB3] :
  Line Build Out (dBm)       [none] :
  Trunk [ 1]             [port   0] :
  Trunk [ 2]             [port   1] :
  Trunk [ 3]             [port   2] :
  Trunk [30]             [port  29] :

Enter command:
```

Step 5 Enter values as indicated by Table 4-7. Press **Enter** after you enter each value and the next line appears.

If you exceed the number of ports configured by the factory, an error message appears.

Step 6 Press **Enter**. The "e1span" menu appears as in Figure 4-47.

Step 7 Type **2** and press **Enter** to configure another span or type **x** and press **Enter** when all spans have been configured.

Note This is the end of the section "Configuring a T1 PRI system". Proceed to the "Configuring the system's date and time" section on page 4-81 to complete configuration.

Configuring an E1 system

This section explains how to configure Multi Access Blades and Smart Blades for an E1 configuration.

Note If this is part of an E1/IP mixed configuration, refer to the "Examples of mixed system configurations" section on page 4-72. If this is part of a T1 PRI installation, refer to the "Configuring a T1 PRI system" section on page 4-34. If this is part of an T1 CAS installation, refer to the "Configuring a T1 CAS system" section on page 4-27. If this is part of a pure IP configuration, refer to the "Configuring a pure IP system" section on page 4-59.

Warning **The necessary cables should already be attached to the transition modules on the back of the server. If they are not, refer to the "Connecting the system cables" section on page 3-18.**

The "blade" command is used to configure all ports. Follow this procedure to configure the necessary Multi Access Blades and Smart Blades. Refer to the examples following this section for more detailed information. For more information about the "blade" command, see the "blade" section on page A-8.

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 At the tech$ prompt, type **blade -e <number of E1 ports>** and press **Enter** for a pure E1 system without any IP configuration. See Figure 4-50.

Figure 4-50 blade Command — E1

```
meetingplace:tech$ blade -e <# E1 ports>
This will reset many DB tables, are you sure?  (y/n): y

Configuring "X" E1 ports

Restart the system for changes to take effect
meetingplace:tech$
```

Step 3 Confirm the "blade" command you entered and type **y** and press **Enter**. If you entered the wrong command, type **n** and press **Enter** and then re-enter the correct command.

The system tells you what it is configuring. The tech$ prompt appears when configuration is complete. See Figure 4-50.

Step 4 Verify your configuration by typing **blade** and pressing **Enter**.

Step 5 Confirm the screen output is correct for your configuration.

Step 6 Type **x** and press **Enter** to exit the "blade" command utility.

Note You can reserve slots for later use by using the "blade" command with the -r option.

Examples of E1 configuration

The following sections provide configuration instructions for example E1 configurations:

- "240 E1 ports" section on page 4-47
- "720 E1 ports" section on page 4-48
- "960 E1 ports" section on page 4-50

240 E1 ports

This section explains how to use the "blade" command when configuring 240 E1 ports.

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 At the tech$ prompt, type **blade -e 240** and press **Enter**.

Step 3 Confirm the "blade" command you entered and type **y** and press **Enter**. If you entered the wrong command, type **n** and press **Enter**, then re-enter the correct command.

The server responds by telling you how many ports it is configuring. When the tech$ prompt appears, it is complete. See Figure 4-51.

Figure 4-51 ***blade Example for 240 E1 Ports***

```
meetingplace:tech$ blade -e 240
This will reset many DB tables, are you sure?  (y/n): y

Configuring 240 E1 ports

Restart the system for changes to take effect
meetingplace:tech$
```

Step 4 Verify your configuration by typing **blade** and pressing **Enter**.

Step 5 Confirm the screen output is like Figure 4-52.

Figure 4-52 blade Confirmation for 240 E1 Ports

```
meetingplace:tech$ blade
Slot    Card    Type    CardId  Ports
 1      TP1610   E1       0     0-29, 30-59, 60-89, 90-119,
                                120-149, 150-179, 180-209, 210-239
 2      CG6000C  SB       0
 3      CG6000C  SB       1
 4      CG6000C  SB       2
 5      no card
 6      no card
 11     no card
 12     no card
 13     no card
 14     no card
 15     no card
 16     no card

*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program
```

Step 6 Type **x** and press **Enter** to exit the "blade" command utility.

720 E1 ports

This section explains how to use the "blade" command when configuring 720 E1 ports.

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 At the tech$ prompt, type **blade -e 720** and press **Enter**.

Step 3 Confirm the "blade" command you entered and type **y** and press **Enter**. If you entered the wrong command, type **n** and press **Enter**, then re-enter the correct command.

The server responds by telling you how many ports it is configuring. When the tech$ prompt appears, it is complete. See Figure 4-53.

Figure 4-53 ***blade Example for 720 E1 Ports***

```
meetingplace:tech$ blade -e 720
This will reset many DB tables, are you sure?  (y/n): y

Configuring 720 E1 ports

Restart the system for changes to take effect
meetingplace:tech$
```

Step 4 Verify your configuration by typing **blade** and pressing **Enter**.

Step 5 Confirm the screen output is like Figure 4-54.

Figure 4-54 blade Confirmation for 720 E1 Ports

```
meetingplace:tech$ blade
Slot    Card    Type    CardId  Ports
 1      TP1610   E1       0     0-29, 30-59, 60-89, 90-119,
                                120-149, 150-179, 180-209, 210-239
                                240-269, 270-299, 300-329, 330-359,
                                360-389, 390-419, 420-449, 450-479
 2      TP1610   E1       1     480-509, 510-539, 540-569, 570-599,
                                600-629, 630-659, 660-689, 690-719
 3      CG6000C  SB       0
 4      CG6000C  SB       1
 5      CG6000C  SB       2
 6      CG6000C  SB       3
 11     CG6000C  SB       4
 12     CG6000C  SB       5
 13     CG6000C  SB       6
 14     CG6000C  SB       7
 15     no card
 16     no card

*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program
```

Step 6 Type **x** and press **Enter** to exit the “blade” command utility.

960 E1 ports

This section explains how to use the "blade" command when configuring 960 E1 ports.

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see "Logging your HyperTerminal session" section on page 4-6.

Step 2 At the tech$ prompt, type **blade -e 960** and press **Enter**.

Step 3 Confirm the "blade" command you entered and type **y** and press **Enter**. If you entered the wrong command, type **n** and press **Enter**, then re-enter the correct command.

The server responds by telling you how many ports it is configuring. When the tech$ prompt appears, it is complete. See Figure 4-55.

Figure 4-55 ***blade Example for 960 E1 Ports***

```
meetingplace:tech$ blade -e 960
This will reset many DB tables, are you sure?  (y/n): y

Configuring 960 E1 ports

Restart the system for changes to take effect
meetingplace:tech$
```

Step 4 Verify your configuration by typing **blade** and pressing **Enter**.

Step 5 Confirm the screen output is like Figure 4-56.

Figure 4-56 blade Confirmation for 960 E1 Ports

```
meetingplace:tech$ blade
Slot    Card    Type    CardId  Ports
 1      TP1610   E1       0     0-29, 30-59, 60-89, 90-119,
                                120-149, 150-179, 180-209, 210-239
                                240-269, 270-299, 300-329, 330-359,
                                360-389, 390-419, 420-449, 450-479
 2      TP1610   E1       1     480-509, 510-539, 540-569, 570-599,
                                600-629, 630-659, 660-689, 690-719
                                720-749, 750-779, 780-809, 810-839,
                                840-869, 870-899, 900-929, 930-959
 3      CG6000C  SB       0
 4      CG6000C  SB       1
 5      CG6000C  SB       2
 6      CG6000C  SB       3
 11     CG6000C  SB       4
 12     CG6000C  SB       5
 13     CG6000C  SB       6
 14     CG6000C  SB       7
 15     CG6000C  SB       8
 16     CG6000C  SB       9

*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program
```

Step 6 Type **x** and press **Enter** to exit the "blade" command utility.

Configuring port groups

You can create port groups so that a group of ports can be configured with the same parameters. The instructions on creating and configuring port groups is below.

Step 1 At the tech$ prompt, type **port** and press **Enter**. Figure 4-57 appears. (For more information about the "port" command, see "port" section on page A-44.)

Figure 4-57 port Command Menu

```
meetingplace:tech$ port
MeetingPlace is up

*****   P O R T / G R O U P   C O N F I G   M E N U   *****

        1)  View port record(s)
        2)  Modify port record
        3)  Copy port records
        4)  View group record(s)
        5)  Modify group record
        x)  Exit program

Enter command:
```

Step 2 Type **5** and press **Enter** to modify the group record. The first line in Figure 4-58 appears.

Figure 4-58 Modifying the Port Group

```
Enter command: 5
Enter port group record number [0..31] : 0

------------     GROUP  0      --------------
--- To skip over a filed, just press <cr> ---
  Activate the group?         :  y
  Card type                   :  E1
  Signaling                   :  protocol table
  Protocol table              :  0
  Number of DID digits        :  0
  Human assistance?           :  n
  Flash transfer?             :  n
  Outdial?                    :  y

Enter command: x
```

Step 3 Type the appropriate port group record number. In this example, it is port group 0, so type **0** and press **Enter**. The rest of Figure 4-58 appears.

Step 4 Type **y** and press **Enter** to activate the port group.

Step 5 Type **E1** and press **Enter** to select the card type. Continue typing and entering the appropriate values for the system configuration.

Step 6 Type **protocol table** and press **Enter** to select signaling.

Step 7 Select the appropriate protocol table number. In this example, it is protocol table 0, so type **0** and press **Enter**. Refer to Table 4-8 for a list of default protocol tables.

Note The protocol table contains the configuration information for the type of signaling used. All E1 systems are shipped from the factory with protocol table 0 set to use the default setting of Euro ISDN protocol and protocol table 1 to use the QSIG protocol. If this is not correct for your system, it can be changed via the "protparm" command. Refer to the "protparm" section on page A-47 for more information on the "protparm" command.

Note If this is part of an upgrade from a pre-5.1 release, the default protocol tables 3 and 4 will not be correct. To resolve this, use the "protparm" command to delete tables 3 and 4. This restores them to the defaults as listed in Table 4-8.

Step 8 Repeat this procedure if more than one port group is needed.

Step 9 Type **x** and press **Enter** to exit the "port" utility.

Table 4-8 Default Protocol Table Settings — E1

Protocol Table Number	Default Protocol
0	Euro ISDN
1	QSIG ECMA

Note There are two QSIG variants: QSIG ECMA and QSIG ETSI. You must be sure to use the same variant that the customer's PBX is set up to use. QSIG ECMA is the default for protocol table 1. If QSIG ETSI is needed, the default protocol must be changed.

Assigning ports to port groups

You can assign specific ports to port groups so that all ports in that group have the same parameters.

Step 1 At the tech$ prompt, type **port** and press **Enter**. Figure 4-57 appears.

Step 2 Type **2** and press **Enter** to modify a port record. The first line in Figure 4-59 appears.

Figure 4-59 Assigning Port Record

```
Enter port record number [0..7] : 0

------------- UNIT 0  PORT 0  --------------
--- To skip over a field, just press <cr> ---
  Uses port group              [   0] :  0
```

Step 3 Type the port number and press **Enter**. In this example, it is port 0, so type **0** and press **Enter**. The rest of Figure 4-59 appears.

Step 4 Enter the number of the port group and press **Enter**. In this example, it is port group 0, so enter **0** and press **Enter**.

Note If you would like to copy this port record to other ports, refer to "Copying port records" section on page 4-54.

Step 5 Type **x** and press **Enter** to exit the "port" utility.

Copying port records

Copying port records provides an easy way to copy the port record for one port to as many ports as desired. Follow these steps to do this:

Step 1 If you are not already accessing the "port" command, at the tech$ prompt, type **port** and press **Enter**. See Figure 4-60.

Figure 4-60 Copying Port Records

```
meetingplace:tech$ port
MeetingPlace is up

*****   P O R T / G R O U P   C O N F I G   M E N U   *****

        1)  View port record(s)
        2)  Modify port record
        3)  Copy port records
        4)  View group record(s)
        5)  Modify group record
        x)  Exit program

Enter command: 3
Enter port record number to copy from [0..959] : 0
Enter port(s) to copy to [0-959] : 1-959
Copied to port record(s) 1-959.

Enter command: x
```

Step 2 Type **3** and press **Enter** to copy port records.

Step 3 Enter the port number you want to copy from and press **Enter**, as shown in line 14 of "" on page <$chapnum54. In this example, it is port 0, so type **0** and press **Enter**.

Step 4 Enter the port numbers you want to copy to and press **Enter**, as shown in line 15 of Figure 4-60. In this example, all ports are being configured with the same parameters as port 0, so type **1-959** and press **Enter**.

Step 5 The system tells you which ports were copied to, as shown in line 16 of Figure 4-60.

Step 6 Type **x** and press **Enter** to exit the "port" utility.

Configuring spans for an E1 system

E1 spans connect to the Multi Access Blade transition modules in the back of the server.

Note The E1 spans are automatically activated and configured with default settings when the "blade" command is run. Table 4-9 lists the default span configuration.

Check the worksheets in the *MeetingPlace Audio Server 5.2 Installation and Planning Guide* to see if your system is configured this way. If these default settings are accurate for this installation, you do not need to complete this section. If the default settings are not accurate for this installation, complete the steps that follow.

Table 4-9 Default E1 Span Configuration

Parameter	Default	Explanation	Possible Values	X
Activate the ACTI span?	y	Specifies if the span is active.	• y = active • n = inactive	
Framing	CRC4	Specifies the framing protocol used on this span. Determined by the service provider. *We recommend using CRC4 only.*	• CRC4 • non-CRC4	
Zero code suppression	HDB3	Specifies the zero code suppression for the span. Determined by the service provider. *We recommend using HDB3 only.*	• HDB3	
Timing	external	Specifies if MeetingPlace should get clock timing from the PBX/Central Office or if timing is generated by MeetingPlace. At least one span should always be designated external.	• internal • external (the span is connected to the public network or a trusted system)	

Table 4-9 Default E1 Span Configuration (continued)

Parameter	Default	Explanation	Possible Values	X
External sync priority	none. The T1 span connected to the T1 Smart Blade in slot 1, line A gets sync priority 1, line B gets 2, etc.	Specifies the priority of the spans that are set for external timing. The system always tries to synchronize from the highest priority span. If the synchronization span goes down, the system automatically switches synchronization to the next highest span. If a higher priority span comes up, the system automatically synchronizes off of it.	• 1-255 (1 is the highest, 255 is the lowest) • never	
Trunk [x]	Numbering is done in order (1, 2, 3, etc.). For example, Trunk [1]:port 0 Trunk [2]:port 1 Trunk [3]:port 2	Specifies which port in the database is assigned to the specific hardware trunk on the card.	• number	
Remote loopback to network	n	Specifies if the span should be put into a loopback mode for testing from the remote end.	• y = yes • n = no (normal operation)	
Internal data loopback	n	Specifies if the span should loop back locally for running diagnostics.	• y = yes • n = no (normal operation)	
Port group	2	Specifies the number of the port group.	• 0 (T1 CAS) • 1 (IP) • 2 (E1) • 3 (T1 PRI)	
Active?	n	Specifies if the port group is active.	• y = yes • n = no	
Card type	E1	Specifies the type of card.	• none • T1 • analog • E1 • IP	

Table 4-9 Default E1 Span Configuration (continued)

Parameter	Default	Explanation	Possible Values	X
Signaling protocol	E1	Specifies the signaling protocol.	• loop start • wink start • ground start • clear channel • E1 • IP • protocol table	
Protocol table	0	Specifies the number of the protocol table to copy from.	• number from 0 to 99	
Number of DID digits expected	0	Specifies the number of DID digits.	• number from 0 to 6	
Default access type	combined access	Specifies the access type	• Combined access • DID meeting • Profile • MeetingNotes • loop through transfer • EBSApp1004 • EBSApp1005 • EBSApp1007 • EBS Xfer test • NewApp1011 • Choose music • Spanish samples • Goto123123_1015	
Language	English (US)	Specifies which language to use.	• English (US) • English (UK) • no language	
Human assistance?	n	Specifies if human assistance is allowed.	• y = yes • n = no	
Flash transfer?	n	Specifies if this can be flash transferred.	• y = yes • n = no	
Outdial?	y	Specifies if this can be outdialed on.	• y = yes • n = no	

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 At the tech$ prompt, type **e1span**. Figure 4-61 appears.

Figure 4-61 e1span Command Menu

```
meetingplace:tech$ e1span
MeetingPlace is up

*****   E 1 S P A N   C O N F I G   M E N U   *****

        1)  View ACTI span record(s)
        2)  Modify ACTI span record
        x)  Exit program

Enter command:
```

Step 3 Type **2** and press **Enter** to modify a span record. Figure 4-62 appears.

Figure 4-62 span Command Record Selection

```
Enter command: 2
Enter ACTI span record number [0..47] : 0
```

Step 4 Type the number of the span record that needs to be modified and press **Enter**. In this example, span record 0 is being configured so type **0** and press **Enter**. The first five lines of Figure 4-63 appear.

Figure 4-63 span Command Record Configuration

```
Enter command: 2
Enter ACTI span record number [0..47] : 0

-----------  Unit 0  ACTI Span 0  ------------
--- To skip over a field, just press <cr> ---
  Activate the ACTI span?       [y] :
  Timing                 [external] :
  External sync priority    [    1] :
  Framing                 [   CRC4] :
  Zero Code Suppression      [HDB3] :
  Line Build Out (dBm)       [none] :
  Trunk [ 1]             [port   0] :
  Trunk [ 2]             [port   1] :
  Trunk [ 3]             [port   2] :
  Trunk [30]             [port  29] :

Enter command:
```

Step 5 Enter values as indicated by Table 4-9. Press **Enter** after you enter each value and the next line appears.

If you exceed the number of ports configured by the factory, an error message appears.

Step 6 Press **Enter**. The "e1span" menu appears as in Figure 4-61.

Step 7 Type **2** and press **Enter** to configure another span or type **x** and press **Enter** when all spans have been configured.

Note This is the end of the section "Configuring an E1 system". Proceed to the "Configuring the system's date and time" section on page 4-81 to complete configuration.

Configuring a pure IP system

Setting up the system

Before configuring the Multi Access Blades in an IP system, customers must know which Quality of Service (QoS) configuration they are using: either the IP Precedence mechanism or the Differentiated Services Code Point (DSCP) mechanism. They then need to provide specific settings for the mechanism. The following sections describe each mechanism and their various settings.

About QoS configuration

For IP configurations, there are two Quality of Service (QoS) mechanisms that can be used: IP Precedence or DSCP. First, determine which mechanism the customer's IP network uses, then determine, with the customer's IT department, the appropriate settings for these values.

About ToS byte

Within the voice packets, the Type of Service (ToS) byte is an 8-bit field in the IP header. It is used for either IP Precedence or DSCP. (Another term for byte is *octet*.) When this byte is used for IP Precedence, three bits are used for the IP Precedence value and four bits are used for the ToS value.

The following shows the bit layout:

7	6	5	4	3	2	1	0
IP precedence			Type of Service				

Note Note the differences in terminology: the ToS *byte* includes all 8 bits; but the ToS *field* is only 4 bits within this byte. The IP Precedence mechanism partitions the ToS byte into an IP Precedence field and a ToS field.

When this byte is used for DSCP, six bits are used for DSCP. The following is the bit layout:

7	6	5	4	3	2	1	0
Differentiated Services Code Point							

Notice that the DSCP field overlaps the fields used for IP Precedence. Therefore, if DSCP values are chosen carefully, then backward compatibility can be achieved if the customer network has a mixture of devices (some using IP Precedence, others using DSCP).

IP Precedence

If you use the traditional IP Precedence QoS mechanism, you must provide two values to be used for MeetingPlace IP configuration:

- IP Precedence value — a value from 0-7. The IP Precedence is used to classify and prioritize types of traffic. Most implementations use an IP Precedence value of 5. Here is a complete list of values:

  0 – routine
  1 – priority
  2 – immediate
  3 – flash
  4 – flash override
  5 – CRITIC/ECP
  6 – internetwork control
  7 – network control

- ToS value — a value from 0-15. The ToS value can determine special handling of packets, such as minimizing delay or maximizing throughput. Unless the customer specifies otherwise, this value is best set to 0.

The following shows an example of how to use the “blade” command to configure an IP Precedence value of 5 and a ToS value of 0. Notice that DSCP is disabled.

Figure 4-64 blade Command with IP Precedence and ToS

```
*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program

Enter command:  2
Enter blade slot [1..16]:  16

  Type                          [IP]:
  Card Type                 [TP1610]:
  Port Group                    [ 1]:
  Number of Ports              [120]:
  1st Port                    [  46]:
  IP address [0]       [172.20.18.30]:
  IP address [1]       [172.20.18.31]:
  Subnet Mask           [255.255.0.0]:
  Default Gateway        [172.20.1.1]:
  Base UDP Port [0]           [ 5000]:
  Base UDP Port [1]           [ 6000]:
  Jitter Buffer Minimum Size   [ 100]:
  Jitter Buffer Optimization     [ 7]:
  IP Precedence                   [0]:  5
  Type of Service (TOS)          [ 0]:  0
  DSCP / DiffServ            [unused]:  unused
  RTCP Interval             [default]:
```

Note This configuration must be done for each Multi Access Blade used for an IP configuration.

DSCP

Differentiated Services Code Point (sometimes called “DiffServ”) is the newer mechanism. It is described in RFC 2474. The DSCP ranges from 0-63. In practice, most implementations use a DSCP value of 40, which corresponds exactly to an IP Precedence value of 5.

The following is an example of how to use the “blade” command to configure a DSCP value of 40.

Figure 4-65 blade Command with DSCP Value

```
*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program

Enter command:  2
Enter blade slot [1..16]:  16

  Type                          [IP]:
  Card Type                 [TP1610]:
  Port Group                    [ 1]:
  Number of Ports              [120]:
  1st Port                    [  46]:
  IP address [0]       [172.20.18.30]:
  IP address [1]       [172.20.18.31]:
  Subnet Mask           [255.255.0.0]:
  Default Gateway        [172.20.1.1]:
  Base UDP Port [0]           [ 5000]:
  Base UDP Port [1]           [ 6000]:
  Jitter Buffer Minimum Size   [ 100]:
  Jitter Buffer Optimization     [ 7]:
  IP Precedence                   [5]:  unused
  Type of Service (TOS)          [ 0]:  unused
  DSCP / DiffServ            [unused]:  40
  RTCP Interval             [default]:
```

Note This configuration must be done for each Multi Access Blade used for an IP configuration.

About jitter buffer settings

The jitter buffer concept is driven by the realities of voice packet networks such as network delay, delay jitter, packet loss, and clock drift. The jitter buffer (also known as a “delay jitter buffer”) enforces an additional packet delay of typically 50-150 additional milliseconds, but it provides the following important benefits:

- Smooths jitter — By delaying all the packets, it is possible to eliminate most effects of delay jitter. That is, for any packets that arrive slightly early or slightly late, the jitter buffer allows the packets to be processed at precise intervals. Any packets that arrive later or earlier than the size of the jitter buffer are discarded, though. Therefore, the jitter buffer should not be set too small. However, the jitter buffer should not be set too large because too much delay can be noticed by participants talking to each other.

- Handles packets out of sequence — In some cases, various delays can cause consecutive packets to be received out of sequence. A jitter buffer provides an opportunity to put these packets back into the proper sequence.
- Handles missing packets — A jitter buffer makes it easier to handle missing (as opposed to just late) packets. When the software determines that the packet is missing, it provides a reasonable approximation for the missing packet. This assumes that the sender enables redundancy support (RFC 2198).
- Handles overruns and underruns — When clocks are not synchronized, there are occasional packet overruns or underruns (depending on whether the far end clock is faster or slower). The jitter buffer allows for a more graceful way of dealing with these.

Jitter buffer configuration

There are two jitter buffer parameters that you can configure:

- Jitter buffer minimum size — The jitter buffer automatically adapts to changing jitter values, but a minimum value needs to be defined. The default value is 100 milliseconds. This is a reasonable value for most installations, but some customer environments may do better with a different value. The "blade" command allows for values from 1-1000 milliseconds.

  A smaller value reduces the noticeable voice delay, but increases the risk of missing packets that degrade voice quality. A smaller value can be considered for customers' IP networks that are:

  - small geographically
  - few hops
  - high bandwidth

  A larger value can provide better voice quality, but the increased delays may become annoying for users. A higher value can be considered for customers' IP networks that are:

  - large geographically
  - many hops
  - potential bandwidth bottlenecks
- Jitter buffer optimization — The jitter buffer optimization factor controls how quickly the jitter buffer can react to network jitter. The "blade" commands allows for optimization factor values from 0-12 and the value defaults to 7.

  At the highest setting, the jitter buffer quickly tracks to the maximal network latencies and stays there, thus minimizing packet error rates but also maximizing delays. At the lowest setting, the jitter buffer increases delay only to compensate for clock drifts and soon decays to its minimal setting again. Mid-range values (such as a default value of 7) provide a reasonable middle ground that is appropriate for most customers.

Example of jitter buffer configuration

4-66 shows how to configure the jitter buffer minimum size to 150 milliseconds and the jitter buffer optimization factor to 9. This example is modifying the blade in slot 16.

Figure 4-66 blade Command Jitter Buffer Configuration

```
*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program

Enter command:  2
Enter blade slot [1..16]:  16

  Type                          [IP]:
  Card Type                 [TP1610]:
  Port Group                    [ 1]:
  Number of Ports              [120]:
  1st Port                    [  46]:
  IP address [0]        [10.10.10.10]:
  Subnet Mask         [255.255.255.0]:
  Default Gateway        [10.10.10.1]:
  Base UDP Port [0]           [ 5000]:
  Base UDP Port [1]           [ 6000]:
  Jitter Buffer Minimum Size   [ 100]: 150
  Jitter Buffer Optimization     [ 7]: 9
  IP Precedence                   [0]:
  Type of Service (TOS)          [ 0]:
  DSCP / DiffServ            [unused]:
  RTCP Interval             [default]:
```

Note This configuration must be done for each Multi Access Blade used for an IP configuration.

Configuring the IP system

This section explains how to configure Multi Access Blades and Smart Blades for a pure IP configuration. If this is part of a T1 CAS system, refer to "Configuring a T1 CAS system" section on page 4-27. If this is part of a T1 PRI system, refer to "Configuring a T1 PRI system" section on page 4-34. If this is part of an E1 system, refer to "Configuring an E1 system" section on page 4-46. If this is part of a mixed system, refer to "Examples of mixed system configurations" section on page 4-72.

The "blade" command is used to configure all ports. Follow the procedure below to configure the necessary Multi Access Blades and Smart Blades. Refer to the examples following this section for more detailed information. For more information about the "blade" command, see the "blade" section on page A-8.

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 At the tech$ prompt, type **blade -i <number of IP ports>** and press **Enter**. This is the command for a pure IP system.

Step 3 Confirm the "blade" command you entered and type **y** and press **Enter**. If you entered the wrong command, type **n** and press **Enter** and then re-enter the correct command.

The system tells you what it is configuring. The tech$ prompt appears when configuration is complete. See Figure 4-67.

Figure 4-67 blade Command — IP

```
meetingplace:tech$ blade -i <# IP ports>
This will reset many DB tables, are you sure?  (y/n): y

Configuring "X" IP ports

Restart the system for changes to take effect
meetingplace:tech$
```

Step 4 Verify your configuration by typing **blade** and pressing **Enter**.

Step 5 Confirm the screen output is correct for your configuration.

Step 6 Type **x** and press **Enter** to exit the "blade" command utility.

Caution Before using the "blade" command to configure an IP system, you must understand the assumptions in Table 4-10. If your installation does not match these assumptions, you must customize the configuration by using the "blade" command's second option that allows you to modify the blade.

Table 4-10 blade Command Assumptions for IP Systems

Number of IP Ports	Assumed Multi-Access Blade Type
1-120	1 MA-4
121-240	2 MA-4s
241-480	1 MA-16
481-600	1 MA-4 and 1 MA-16
601+	2 MA-16s

Step 1 Type **2** and press **Enter** to modify the blade. A prompt for the blade slot to modify appears, as shown in line 8 in Figure 4-68.

Figure 4-68 Completing IP Port Configuration

```
*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program

Enter command:  2
Enter blade slot [1..16]:  16

  Type                              [IP]:
  Card Type                   [   TP1610]:
  Port Group                         [ 1]:
  Number of Ports                   [480]:
  1st Port                         [ 480]:
  IP address [0]                [0.0.0.0]:  10.10.10.10
  IP address [1]                [0.0.0.0]:  10.10.10.11
  Subnet Mask                   [0.0.0.0]:  255.255.255.0
  Default Gateway               [0.0.0.0]:  10.10.10.1
  Base UDP Port [0]               [ 5000]:
  Base UDP Port [1]               [ 6000]:
  Jitter Buffer Minimum Size       [ 100]:
  Jitter Buffer Optimization         [ 7]:
  IP Precedence                       [0]:
  Type of Service (TOS)              [ 0]:
  DSCP / DiffServ                [unused]:
  RTCP Interval                 [default]:
```

Step 2 Type the correct slot number for the blade you want to modify and press **Enter**. In this example, it is slot 16 so type **16** and press **Enter**.

Step 3 Continue pressing **Enter** until you are prompted to enter the IP address, as shown in line 15 of Figure 4-68.

Step 4 Type the correct IP address and press **Enter**. For an MA-4, the system prompts you for one IP address. For an MA-16, the system prompts you for two IP addresses. If you are using less than 240 ports on an MA-16, you can leave the second IP address as 0.0.0.0.

Step 5 Continue pressing **Enter** and verify the default settings are correct for this installation.

If your installation calls for values other than the defaults, make the necessary changes, and continue pressing **Enter** until you see the “blade” command menu.

Step 6 Verify that the IP addresses were changed correctly by typing **1** and pressing **Enter** to view the blade details. When prompted, type the slot number for the blade you want to see.

Step 7 If it is correct, type **x** and press **Enter** to exit the program. If not, repeat the steps above.

Example of a pure IP configuration

This section explains how to use the "blade" command when configuring 960 IP ports.

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 At the tech$ prompt, type **blade -i 960** and press **Enter**.

Step 3 Confirm the "blade" command you entered and type **y** and press **Enter**. If you entered the wrong command, type **n** and press **Enter**, then re-enter the correct command.

The server responds by telling you how many ports it is configuring. When the tech$ prompt appears, it is complete. See Figure 4-69.

Figure 4-69 blade Example for 960 IP Ports

```
meetingplace:tech$ blade -i 960
This will reset many DB tables, are you sure?  (y/n): y

Configuring 960 IP ports

Restart the system for changes to take effect
meetingplace:tech$
```

Step 4 Verify your configuration by typing **blade** and pressing **Enter**.

Step 5 Confirm the screen output is like Figure 4-70.

Figure 4-70 blade Confirmation for 960 IP Ports

```
meetingplace:tech$ blade
Slot    Card    Type    CardId  Ports
 1      CG6000C  SB       0
 2      CG6000C  SB       1
 3      CG6000C  SB       2
 4      CG6000C  SB       3
 5      CG6000C  SB       4
 6      CG6000C  SB       5
 11     CG6000C  SB       6
 12     CG6000C  SB       7
 13     CG6000C  SB       8
 14     CG6000C  SB       9
 15     TP1610   IP       1      480-959 (No IP address)
 16     TP1610   IP       0      0-479 (No IP address)

*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program
```

Step 6 Type **2** and press **Enter** to modify a blade. A prompt for the blade slot to modify appears, as shown in line 8 in Figure 4-71.

Figure 4-71 Setting IP Address for 960 IP Ports

```
*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program

Enter command:  2
Enter blade slot [1..16]:  16

  Type                              [IP]:
  Card Type                  [   TP1610]:
  Port Group                         [ 1]:
  Number of Ports                   [480]:
  1st Port                        [   0]:
  IP address [0]               [0.0.0.0]:  10.10.10.10
  IP address [1]               [0.0.0.0]:  10.10.10.11
  Subnet Mask                  [0.0.0.0]:  255.255.255.0
  Default Gateway              [0.0.0.0]:  10.10.10.1
  Base UDP Port [0]              [ 5000]:
  Base UDP Port [1]              [ 6000]:
  Jitter Buffer Minimum Size     [ 100]:
  Jitter Buffer Optimization       [ 7]:
  IP Precedence                     [0]:
  Type of Service (TOS)            [ 0]:
  DSCP / DiffServ               [unused]:
  RTCP Interval                [default]:
```

Step 7 Type the correct slot number for the blade you want to modify and press **Enter**. In this configuration, it is slot 16 so type **16** and press **Enter**.

Step 8 Continue pressing **Enter** until you are prompted to enter the IP address as in line 15 of Figure 4-71.

Step 9 Enter the correct IP address and continue pressing **Enter** until you are prompted with the "blade" configuration menu.

Step 10 Type **2** and press **Enter** to modify a blade. A prompt for the blade slot to modify appears, as shown in line 8 in Figure 4-71.

Step 11 Type **15** and press **Enter** to select the blade in slot 15.

Note Figure 4-71 shows slot 16 but you have already configured slot 16, so you should select slot 15 now.

Step 12 Continue pressing **Enter** until you are prompted to enter the IP address as in line 15 of Figure 4-71.

Step 13 Enter the correct IP address and continue pressing **Enter** until you are prompted with the "blade" configuration menu.

Step 14 Verify that the IP addresses were changed correctly by typing **1** and pressing **Enter** to view the blade details. When prompted, type the slot number for the blade you want to see.

Step 15 If it is correct, type **x** and press **Enter** to exit the program. If not, repeat the steps above.

Completing IP configuration

This section only needs to be completed if your system is using IP ports.

Step 1 Once the server has finished restarting (about five minutes), proceed with the MeetingPlace IP Gateway installation and configuration. Refer to the *MeetingPlace IP Gateway System Manager's Guide* for instructions.

Step 2 Once the MeetingPlace IP Gateway has been installed and configured, login into the CLI as a technician.

Step 3 At the tech$ prompt, type **restart** and press **Enter**.

Step 4 Type **y** and press **Enter** to confirm that you want to restart the system.

Step 5 Once the server has finished restarting (about five minutes), launch the IP Gateway service running on the MeetingPlace IP Gateway machine. Refer to the *MeetingPlace IP System Manager's Guide* for information on how to launch the service.

Step 6 Log into the CLI as a technician.

Step 7 Type **swstatus** and press **Enter** to verify the software is up. See Figure 4-86 on page 4-83.

Step 8 Type **gwstatus** and press **Enter** to verify the MeetingPlace IP Gateway service is up. See Figure 4-72.

Figure 4-72 gwstatus for IP Gateway

```
meetingplace:tech$ gwstatus
Gateway SIM Status/Tue Oct 28 20:06:24 2003
-----------------------------------------
Remote Units:
 Unit 16 mpgateway         v5.2.0.10      Ok          10/28/03 20:06:10

Gateways:
 Unit 16 WebPub:DataSvc   v4.3.0.100     Ok          10/27/03 18:54:02
 Unit 16 WebPub:MPAgent   v4.3.0.100     Ok          10/27/03 18:53:58
 Unit 16 MPConvert        v4.3.0.100     Ok          10/27/03 18:54:06
 Unit 16 IP Gateway       v5.2.0.7       Ok          10/27/03 18:53:25
 Unit 16 WebPub:Master    v4.3.0.100     Ok          10/27/03 18:53:25
 Unit 16 DataConf:GW      v4.3.0.100     Ok          10/28/03 20:05:48
 Unit 16 DataConf:MCS     v4.3.0.100     Ok          10/28/03 20:05:36
 Unit 16 DataConf:GCC     v4.3.0.100     Ok          10/28/03 20:05:36
```

Step 9 Type **setipcodec** and press **Enter**. The first seven lines of Figure 4-73 appear.

Figure 4-73 setipcodec Command

```
meetingplace:tech$ setipcodec
MeetingPlace is up
*****   I P   C O D E C   C O N F I G   M E N U   *****
        1)  View IP codec configuration
        2)  Modify IP codec configuration
        x)  Exit program
Enter command: 2
Codec Priorities (highest = 1)
------------------------------
  G.711 mu-law                [ 10] :
  G.711 A-law                 [ 11] :
  G.722                    [unused] :
  G.723                    [unused] :
  G.726-16                 [unused] :
  G.726-24                 [unused] :
  G.726-32                 [unused] :
  G.726-40                 [unused] :
  G.728                    [unused] :
  G.729                    [unused] :
  GSM                      [unused] :
  GSM-EFR                  [unused] :
  QCELP                    [unused] :
Codec Attributes
----------------
  G.711 packet size (ms)      [ 20] :
  G.723 frames per packet     [  1] :
  G.723 low rate (5.3 kb/s)?    [y] :
  G.728 frames per packet     [  8] :
  G.729 frames per packet     [  2] :
  G.729A support?               [y] :
  G.729B support?               [y] :
  GSM frames per packet       [  1] :
  GSM-EFR frames per packet   [  1] :
  QCELP frames per packet     [  1] :
Miscellaneous
-------------
  Silence suppression?          [n] :
```

Step 10 Type **2** and press **Enter** to modify the IP codec configuration. The next line in Figure 4-73 appears.

Step 11 Continue pressing **Enter** and enter the appropriate codec priority based on the installation requirements. In this example, G.711 mu-law is given the highest priority and G.711 A-law is given the next highest priority. G.729 is unused. These are the default settings. If other settings are necessary, change them using the "setipcodec" command.

Note If multiple codecs are used, enable and test each one individually and then enable all of them with the correct priority, and test again.

Step 12 Continue pressing **Enter** to accept the default for the remaining settings.

Step 13 Try to place an IP call into the server. If the call is successful, the configuration is complete.

If the call is not successful, run the following commands on the server. (These commands produce logs that give you information about why the call failed.) If you still cannot determine the reason for failure, contact the Cisco TAC. For more information on these commands, refer to Appendix A.

- "errorlog -s info -l" (see the "errorlog" section on page A-24)
- "cptrace" and "cptrace -v" (see the "cptrace" section on page A-13)
- "gwcptrace <unit>" (see the "gwcptrace" section on page A-29)
- "tvportstat -s" and "tvportstat -c" (see the "tvportstat" section on page A-65)

Examples of mixed system configurations

This section provides examples of common mixed system configurations. It does not include the additional steps necessary to complete configuration, such as the span, port, and port group configuration. For that information, refer to the section for the type of ports being configured: the "Configuring a T1 CAS system" section on page 4-27, "Configuring a T1 PRI system" section on page 4-34, "Configuring an E1 system" section on page 4-46, or "Configuring a pure IP system" section on page 4-59.

96 T1 CAS ports, 240 IP ports

This section explains how to use the "blade" command when configuring 96 T1 CAS ports and 240 IP ports.

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 At the tech$ prompt, type **blade -t 96 -i 240** and press **Enter**.

Step 3 Confirm the "blade" command you entered and type **y** and press **Enter**. If you entered the wrong command, type **n** and press **Enter**, then re-enter the correct command.

The server responds by telling you how many ports it is configuring. When the tech$ prompt appears, it is complete. See Figure 4-74.

Figure 4-74 blade Example for 96 T1 CAS and 240 IP Ports

```
meetingplace:tech$ blade -t 96 -i 240
This will reset many DB tables, are you sure?  (y/n): y

Configuring 96 T1 ports
Configuring 240 IP ports

Restart the system for changes to take effect
meetinplace:tech$
```

Step 4 Verify your configuration by typing **blade** and pressing **Enter**.

Step 5 Confirm the screen output is like Figure 4-75.

Figure 4-75 blade Confirmation for 96 T1 CAS and 240 IP Ports

```
meetingplace:tech$ blade
Slot  Card     Type    CardId  Ports
 1    CG6000C  T1       0     0-23, 24-47, 48-71, 72-95
 2    CG6000C  SB       1
 3    CG6000C  SB       2
 4    CG6000C  SB       3
 5    no card
 6    no card
 11   no card
 12   no card
 13   no card
 14   no card
 15   TP1610-4 IP       1     216-335 (No IP address)
 16   TP1610-4 IP       0     96-215 (No IP address)

*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program

Enter command:
```

Step 6 Type **2** and press **Enter** to modify a blade. A prompt for the blade slot to modify appears, as shown in line 8 in Figure 4-76.

Figure 4-76 Setting IP Address for 96 T1 CAS and 240 IP Ports

```
*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program

Enter command:  2
Enter blade slot [1..16]:  16

  Type                          [IP]:
  Card Type                [TP1610-4]:
  Port Group                     [ 1]:
  Number of Ports               [120]:
  1st Port                     [  96]:
  IP address [0]            [0.0.0.0]:  10.10.10.10
  Subnet Mask               [0.0.0.0]:  255.255.255.0
  Default Gateway           [0.0.0.0]:  10.10.10.1
  Base UDP Port [0]           [ 5000]:
  Jitter Buffer Minimum Size   [ 100]:
  Jitter Buffer Optimization     [ 7]:
  IP Precedence                   [0]:
  Type of Service (TOS)          [ 0]:
  DSCP / DiffServ            [unused]:
  RTCP Interval             [default]:
```

Step 7 Type the correct slot number for the blade you want to modify and press **Enter**. In this configuration, it is slot 16 so type **16** and press **Enter**.

Step 8 Continue pressing **Enter** until you are prompted to enter the IP address as in line 15 of Figure 4-76.

Step 9 Enter the correct IP address and continue pressing **Enter** until you are prompted with the "blade" configuration menu.

Step 10 Type **2** and press **Enter** to modify a blade. A prompt for the blade slot to modify appears, as shown in line 8 in Figure 4-76.

Step 11 Type the correct slot number for the blade you want to modify and press **Enter**. In this configuration, it is slot 15 so type **15** and press **Enter**.

Note Figure 4-76 shows slot 16 but you have already configured slot 16, so you should select slot 15 now.

Step 12 Continue pressing **Enter** until you are prompted to enter the IP address as in line 15 of Figure 4-76.

Step 13 Enter the correct IP address and continue pressing **Enter** until you are prompted with the "blade" configuration menu.

Step 14 Verify that the IP addresses were changed correctly by typing **1** and pressing **Enter** to view the blade details. When prompted, type the slot number for the blade you want to see.

Step 15 If it is correct, type **x** and press **Enter** to exit the program. If not, repeat the steps above.

23 T1 PRI ports, 120 IP ports

This section explains how to use the "blade" command when configuring 23 T1 PRI ports and 120 IP ports.

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 At the tech$ prompt, type **blade -p 23 -i 120** and press **Enter**.

Step 3 Confirm the "blade" command you entered and type **y** and press **Enter**. If you entered the wrong command, type **n** and press **Enter**, then re-enter the correct command.

The server responds by telling you how many ports it is configuring. When the tech$ prompt appears, it is complete. See Figure 4-77.

Figure 4-77 blade Example for 23 T1 PRI and 120 IP Ports

```
meetingplace:tech$ blade -p 23 -i 120
This will reset many DB tables, are you sure?  (y/n): y

Configuring 23 T1 PRI ports
Configuring 120 IP ports

Restart the system for changes to take effect
meetinplace:tech$
```

Step 4 Verify your configuration by typing **blade** and pressing **Enter**.

Step 5 Confirm the screen output is like Figure 4-78.

Figure 4-78 blade Confirmation for 23 T1 PRI and 120 IP Ports

```
meetingplace:tech$ blade
Slot    Card    Type    CardId  Ports
 1      TP1610-4 T1       0     0-22, none, none, none
 2      CG6000C  SB       0
 3      CG6000C  SB       1
 4      no card
 5      no card
 6      no card
 11     no card
 12     no card
 13     no card
 14     no card
 15     no card
 16     TP1610-4 IP       1   23-142 (No IP address)

*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program
```

Step 6 Type **2** and press **Enter** to modify a blade. A prompt for the blade slot to modify appears, as shown in line 8 in Figure 4-79 appears.

Figure 4-79 Setting IP Address for 23 T1 PRI and 120 IP Ports

```
*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program

Enter command:  2
Enter blade slot [1..16]:  16

  Type                              [IP]:
  Card Type                  [   TP1610]:
  Port Group                         [ 1]:
  Number of Ports                   [480]:
  1st Port                        [ 480]:
  IP address [0]                [0.0.0.0]:  10.10.10.10
  IP address [1]                [0.0.0.0]:  10.10.10.11
  Subnet Mask                   [0.0.0.0]:  255.255.255.0
  Default Gateway               [0.0.0.0]:  10.10.10.1
  Base UDP Port [0]               [ 5000]:
  Base UDP Port [1]               [ 6000]:
  Jitter Buffer Minimum Size       [ 100]:
  Jitter Buffer Optimization         [ 7]:
  IP Precedence                       [0]:
  Type of Service (TOS)              [ 0]:
  DSCP / DiffServ                [unused]:
  RTCP Interval                 [default]:
```

Step 7 Type the correct slot number for the blade you want to modify and press **Enter**. In this configuration, it is slot 16 so type **16** and press **Enter**.

Step 8 Continue pressing **Enter** until you are prompted to enter the IP address as in line 15 of Figure 4-79.

Step 9 Enter the correct IP address and continue pressing **Enter** until you are prompted with the “blade” configuration menu.

Step 10 Verify that the IP address was changed correctly by typing **1** and pressing **Enter** to view the blade details. When prompted, type the slot number for the blade you want to see.

Step 11 If it is correct, type **x** and press **Enter** to exit the program. If not, repeat the steps above.

480 E1 ports and 480 IP ports

This section explains how to use the "blade" command when configuring 480 E1 ports and 480 IP ports.

Step 1 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 At the tech$ prompt, type **blade -e 480 -i 480** and press **Enter**.

Step 3 Confirm the "blade" command you entered and type **y** and press **Enter**. If you entered the wrong command, type **n** and press **Enter**, then re-enter the correct command.

The server responds by telling you how many ports it is configuring. When the tech$ prompt appears, it is complete. See Figure 4-80.

Figure 4-80 blade Example for 480 E1 Ports and 480 IP Ports

```
meetingplace:tech$ blade -e 480 -i 480
This will reset many DB tables, are you sure?  (y/n): y

Configuring 480 E1 ports
Configuring 480 IP ports

Restart the system for changes to take effect
meetingplace:tech$
```

Step 4 Verify your configuration by typing **blade** and pressing **Enter**.

Step 5 Confirm the screen output is like Figure 4-81.

Figure 4-81 blade Confirmation for 480 E1 and 480 IP Ports

```
meetingplace:tech$ blade
Slot    Card    Type    CardId  Ports
 1      TP1610   E1       0     0-29, 30-59, 60-89, 90-119,
                                120-149, 150-179, 180-209, 210-239
                                240-269, 270-299, 300-329, 330-359,
                                360-389, 390-419, 420-449, 450-479
 2      CG6000C  SB       0
 3      CG6000C  SB       1
 4      CG6000C  SB       2
 5      CG6000C  SB       3
 6      CG6000C  SB       4
 11     CG6000C  SB       5
 12     CG6000C  SB       6
 13     CG6000C  SB       7
 14     CG6000C  SB       8
 15     CG6000C  SB       9
 16     TP1610   IP       1     480-959 (No IP address)

*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program
```

Step 6 Type **2** and press **Enter** to modify a blade. A prompt for the blade slot to modify appears, as shown in line 8 in Figure 4-82 appears.

Step 7 Type the correct slot number for the blade you want to modify and press **Enter**. In this configuration, it is slot 16 so type **16** and press **Enter**.

Figure 4-82 Setting IP Address for 480 E1 and 480 IP Ports

```
*****   B L A D E   C O N F I G   M E N U   *****

        1)  View blade details
        2)  Modify blade
        x)  Exit program

Enter command:  2
Enter blade slot [1..16]:  16

  Type                          [IP]:
  Card Type               [   TP1610]:
  Port Group                     [ 1]:
  Number of Ports               [480]:
  1st Port                     [ 480]:
  IP address [0]            [0.0.0.0]:  10.10.10.10
  IP address [1]            [0.0.0.0]:  10.10.10.11
  Subnet Mask               [0.0.0.0]:  255.255.255.0
  Default Gateway           [0.0.0.0]:  10.10.10.1
  Base UDP Port [0]           [ 5000]:
  Base UDP Port [1]           [ 6000]:
  Jitter Buffer Minimum Size   [ 100]:
  Jitter Buffer Optimization     [ 7]:
  IP Precedence                   [0]:
  Type of Service (TOS)          [ 0]:
  DSCP / DiffServ            [unused]:
  RTCP Interval             [default]:
```

Step 8 Continue pressing **Enter** until you are prompted to enter the IP address, as shown in line 15 of Figure 4-82.

Step 9 Enter the correct IP address and continue pressing **Enter** until you are prompted with the “blade” configuration menu.

Step 10 Type **2** and press **Enter** to modify a blade. A prompt for the blade slot to modify appears, as shown in line 8 in Figure 4-82.

Step 11 If it is correct, type **x** and press **Enter** to exit the program. If not, repeat the steps above.

Configuring the system's date and time

To configure the system's date and time, the application software must be down. The "date" command is used to set any portion of the date and time without specifying the higher parameters. For example, you can set the hour without setting the day of the month, but you must specify the minutes when setting the hour.

Caution The server's time zone must be set before setting the server's date and time. If this has not been done yet, complete the "Configuring the server's time zone" section on page 4-24 before proceeding.

Set the server's date and time by following this procedure:

Step 1 Shut down the software by typing **down** and pressing **Enter**. (For more information about the "down" command, see the "down" section on page A-19.)

Step 2 Type **y** and press **Enter** to verify that you want to shut down the system. The third and fourth lines in Figure 4-83 appear.

Figure 4-83 down Command

```
meetingplace:tech$ down
Are you sure (y/n)? y
Checking to see if the system is loaded...OK
System DOWN procedure has been initiated.
The system is DOWN.
meetingplace:tech$
```

Step 3 Wait about one minute and the fifth and sixth lines of Figure 4-83 appear.

Step 4 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see "Logging your HyperTerminal session" section on page 4-6.

Step 5 Type **date** and press **Enter**. The display shows the current date, time, and abbreviated time zone as shown on the second line of Figure 4-84.

Figure 4-84 date Command

```
meetingplace:tech$ date
Wed Oct 29 15:07:32 PST 2003
meetingplace:tech$ date 0310291508
Wed Oct 29 15:08:00 PST 2003
```

Step 6 Type **date** followed by a space and then type a date or time in any of the following formats:

- yyyymmddhhmm — year, month, day, hour, minute
- yymmddhhmm — year, month, day, hour, minute
- mmddhhmm — month, day, hour, minute
- hhmm — hour, minute

Press **Enter**. Refer to the third line in Figure 4-84.

The display shows the new date and time as in the last line of Figure 4-84.

The month, day, hour, and minute values are all two digits, with a zero prefix for values less than 10. For the year, you can either use all four digits of the year (for example, "1998") or just the last two digits (for example, "02" for the year 2002). The hour is in 24-hour format (00-23). You can append seconds to any format by adding a period and two digits (for example ".34" means 34 seconds).

Step 7 Finalize the configuration by typing **restart** and pressing **Enter**. Refer to the first line in Figure 4-85. (For more information about the "restart" command, see the "restart" section on page A-51.)

Figure 4-85 restart Command

```
meetingplace:tech$ restart
Are you sure (y/n)? y
Enabling system activation.
Checking to see if the system is loaded...
The System Integrity Manager is not running.
```

Step 8 Type **y** and press **Enter** to verify you want to restart the system. The third, fourth, and fifth lines in "Figure 4-85restart Command" section on page 4-82 appear.

Step 9 Wait five to ten minutes and verify the system has come up by entering **swstatus** and pressing **Enter**. (For more information about the "swstatus" command, see "swstatus" section on page A-63.)

Once all of the software modules have a status of "UP", as in Figure 4-86, move on to the next step.

Figure 4-86 swstatus Command

```
meetingplace:tech$ swstatus
Conference server 5.2.0   S/N: M00002    Latitude Comm.
System status: Operating
System mode: Up
Temperature: 30
Power supply: OK

MODULE NAME          STATUS     VERSION
SIM                  UP         "11/14/02 20:08 MPBUILD-rel520"
LSH                  UP         "11/14/02 18:53 MPBUILD-rel520"
SNMPD                UP         "11/14/02 20:33 MPBUILD-rel520"
DBQSERVER            UP         "11/14/02 19:13 MPBUILD-rel520"
DBSERVER             UP         "11/14/02 19:13 MPBUILD-rel520"
POSERVER             UP         "11/14/02 19:43 MPBUILD-rel520"
CPSERVER             UP         "11/14/02 19:40 MPBUILD-rel520"
CONFSCHED            UP         "11/14/02 19:58 MPBUILD-rel520"
WSSERVER             UP         "11/14/02 20:09 MPBUILD-rel520"
VOICESERVER          UP         "11/14/02 20:28 MPBUILD-rel520"
GWSIMMGR             UP         "11/14/02 20:41 MPBUILD-rel520"

UNIT SITE  STATUS    RUN LEVEL  UNIT KIND   LAST ATTACH
  10    0  OK        UP         GATEWAY     11/23/02 04:38:08
  11    0  OK        UP         GATEWAY     11/23/02 04:37:38
  12    0  OK        UP         GATEWAY     11/25/02 12:25:26
  13    0  OK        UP         GATEWAY     11/21/02 19:41:28
  14    0  OK        UP         GATEWAY     11/23/02 04:37:19
```

Verifying the configuration

Use Table 4-11 as a checklist to verify all configuration steps have been completed before proceeding.

Table 4-11 Configuration Checklist

X	Command	Description
	net	Set the network parameters for the server.
	timezone	Set the server's time zone.
	blade	Configure Smart Blades present in the system.
	date	Set the server's date and time.
	restart	Restart the server.

Configuring reservationless meetings (optional)

Reservationless meetings are disabled by default. If you would like to enable reservationless meetings, you need to do so via the "mtgmode" command. For details on the "mtgmode" command, refer to the "mtgmode" section on page A-37.

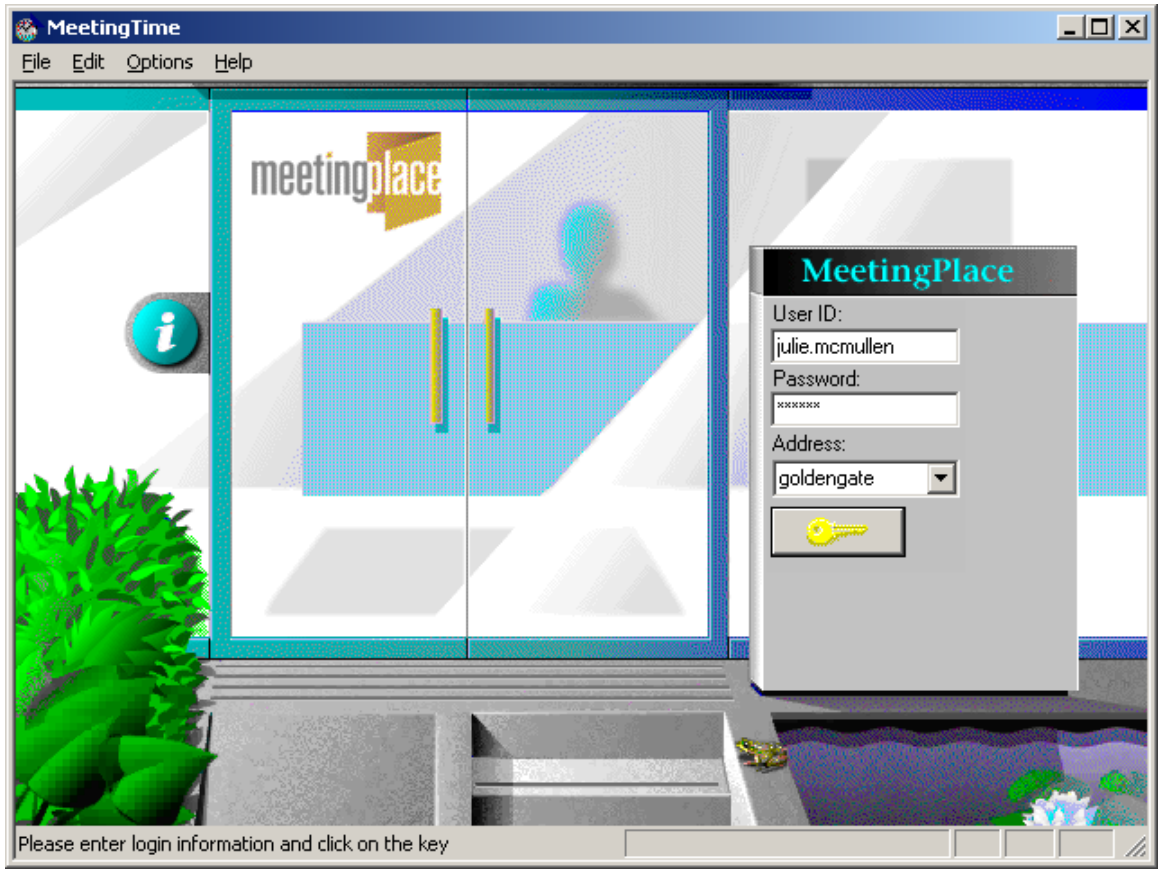
Using MeetingTime to configure ports

After a system restart, the LAN connection becomes active. Locate the MeetingTime media kit that was included in the system box. Install MeetingTime on the System Manager's PC. To install MeetingTime, follow the directions included in the media kit.

This section describes how to use MeetingTime to complete system configuration. The *MeetingPlace Audio Server 5.2 System Manager's Guide* contains complete information about MeetingTime. For these procedures, you need worksheets 4-5, 4-6, and 4-7 from the *MeetingPlace Audio Server 5.2 Installation Planning Guide*. This procedure consists of transferring information from the worksheets to the MeetingTime screens.

Step 1 Double click the MeetingTime icon. Figure 4-87 appears.

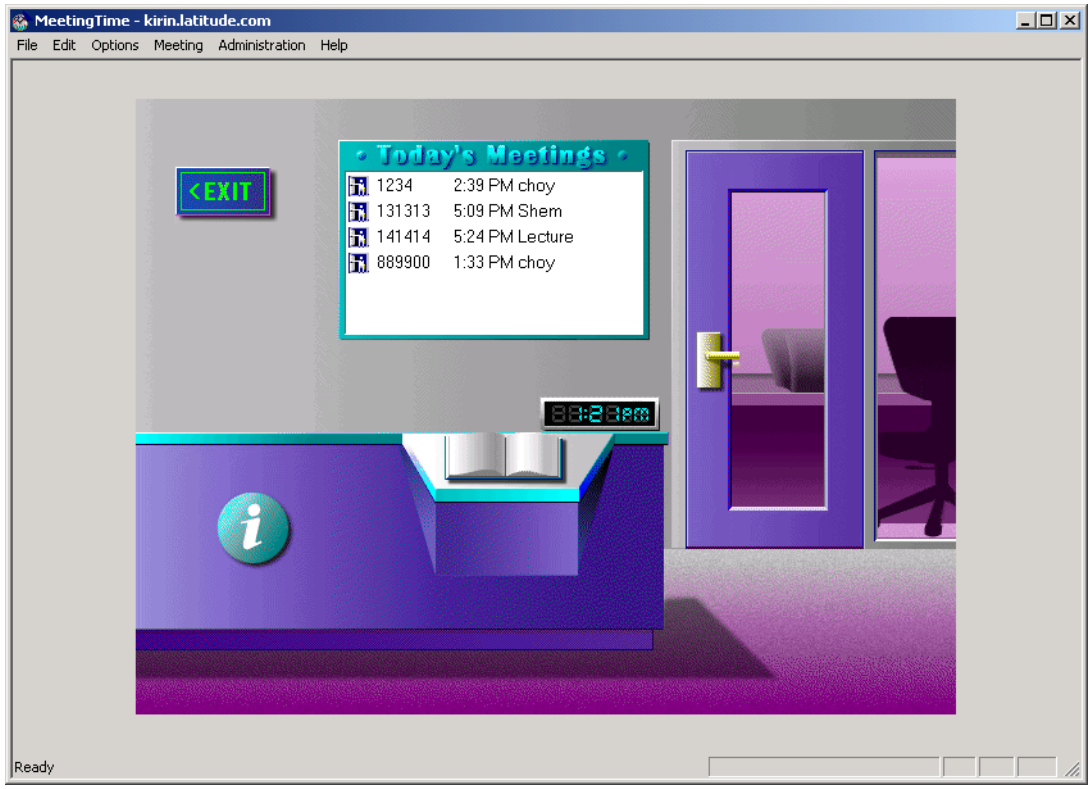
Figure 4-87 MeetingTime Login Dialog Box



Step 2 Enter your case sensitive user ID, your password, and the address or host name of the MeetingPlace server. If you do not know your password, contact the Cisco TAC.

Step 3 Click the door key icon. The MeetingPlace lobby appears. See Figure 4-88.

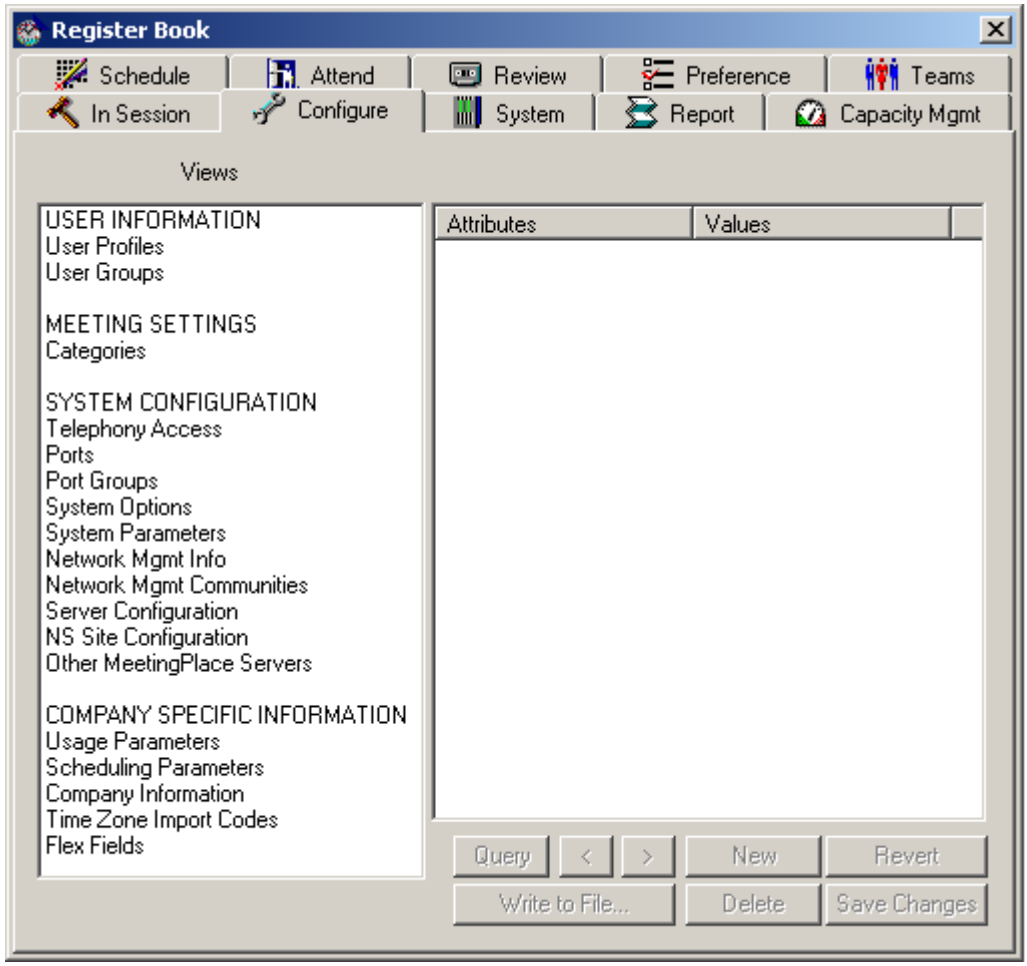
Figure 4-88 MeetingTime Lobby Dialog Box



Step 4 Click the register book on the receptionist's desk, under the receptionist's hand.

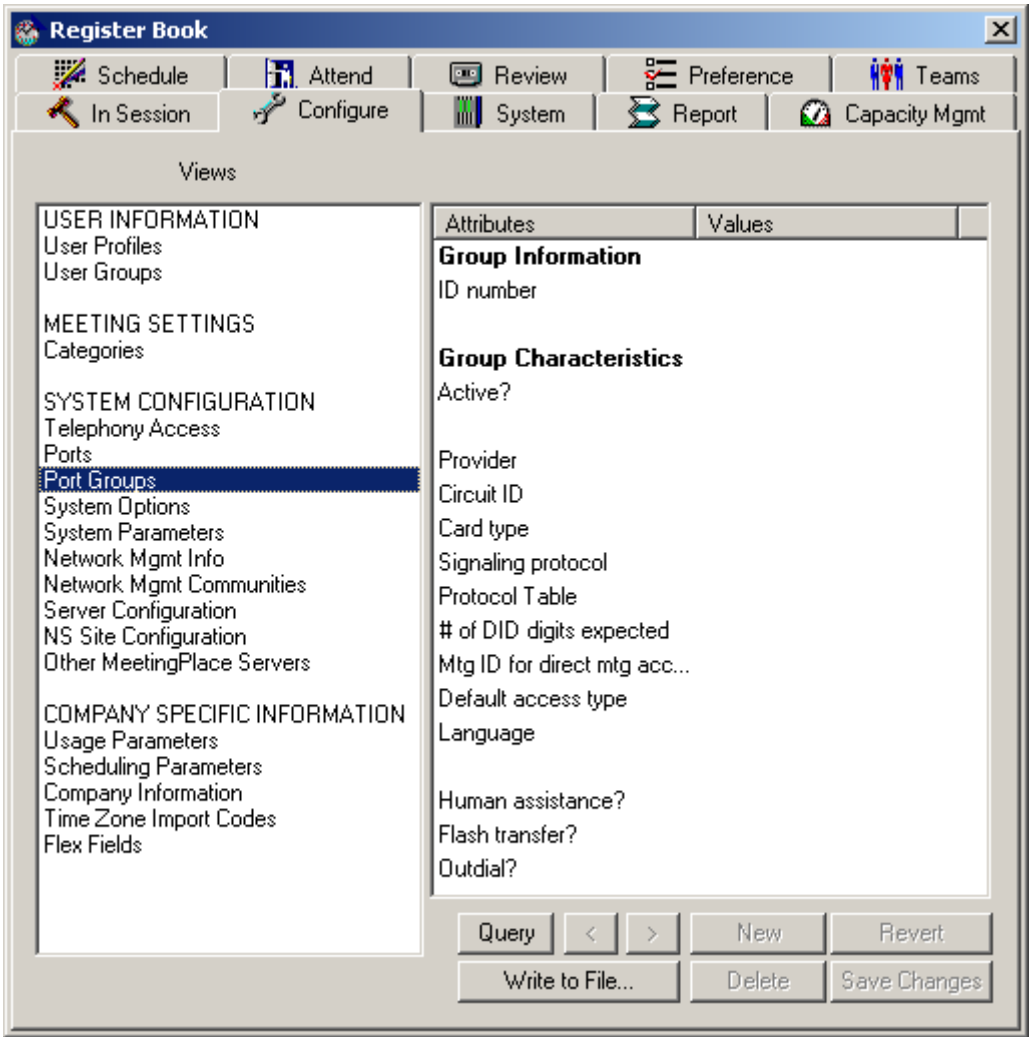
Step 5 Click the **Configure** tab. MeetingTime Configure Tab Dialog Box appears.

Figure 4-89 MeetingTime Configure Tab Dialog Box



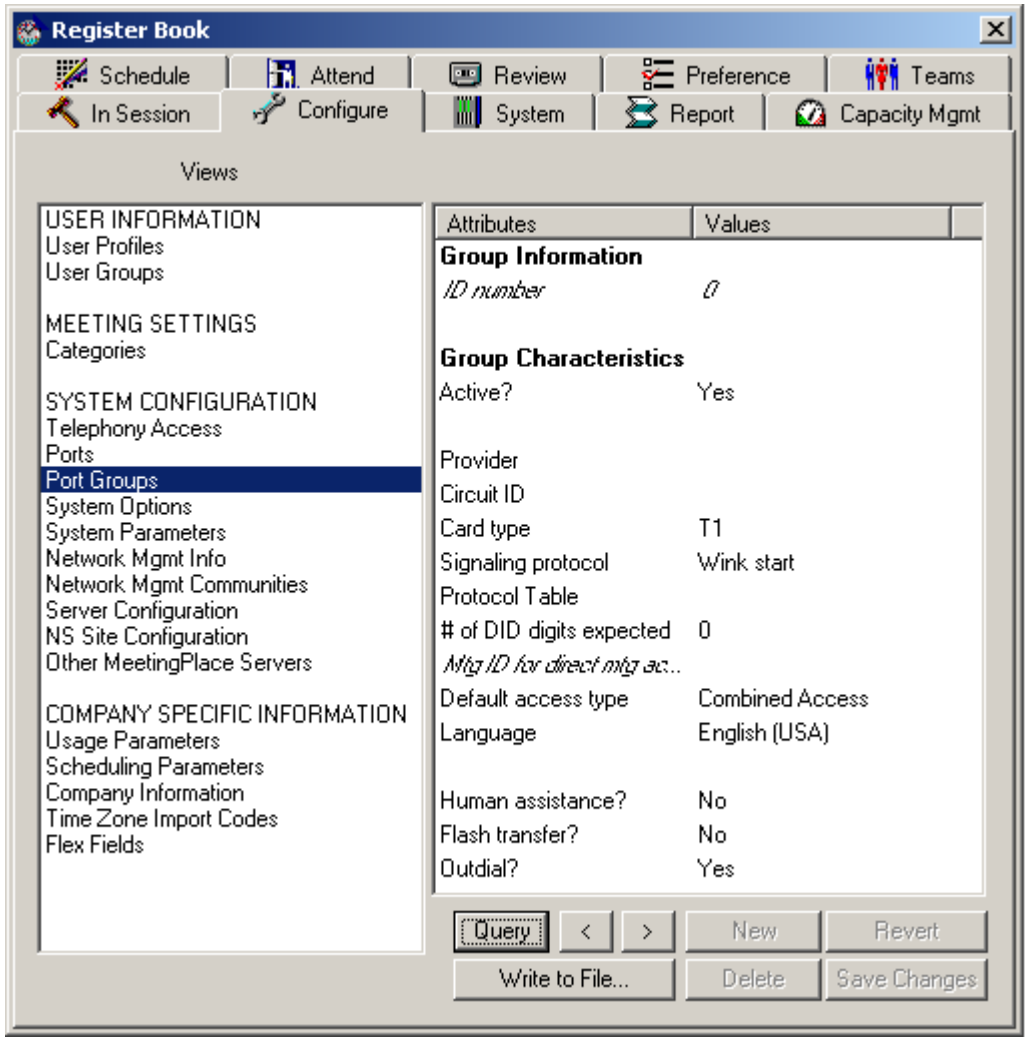
Step 6 Under **Views** on the left side, select **Port Groups**. The attributes for port group 0 (ID number 0) appear without values. See Figure 4-90.

Figure 4-90 MeetingTime Port Groups Attributes Dialog Box



Step 7 Click **Query**. The values for port group 0 appear. See Figure 4-91.

Figure 4-91 MeetingTime Port Groups Attributes and Values Dialog Box



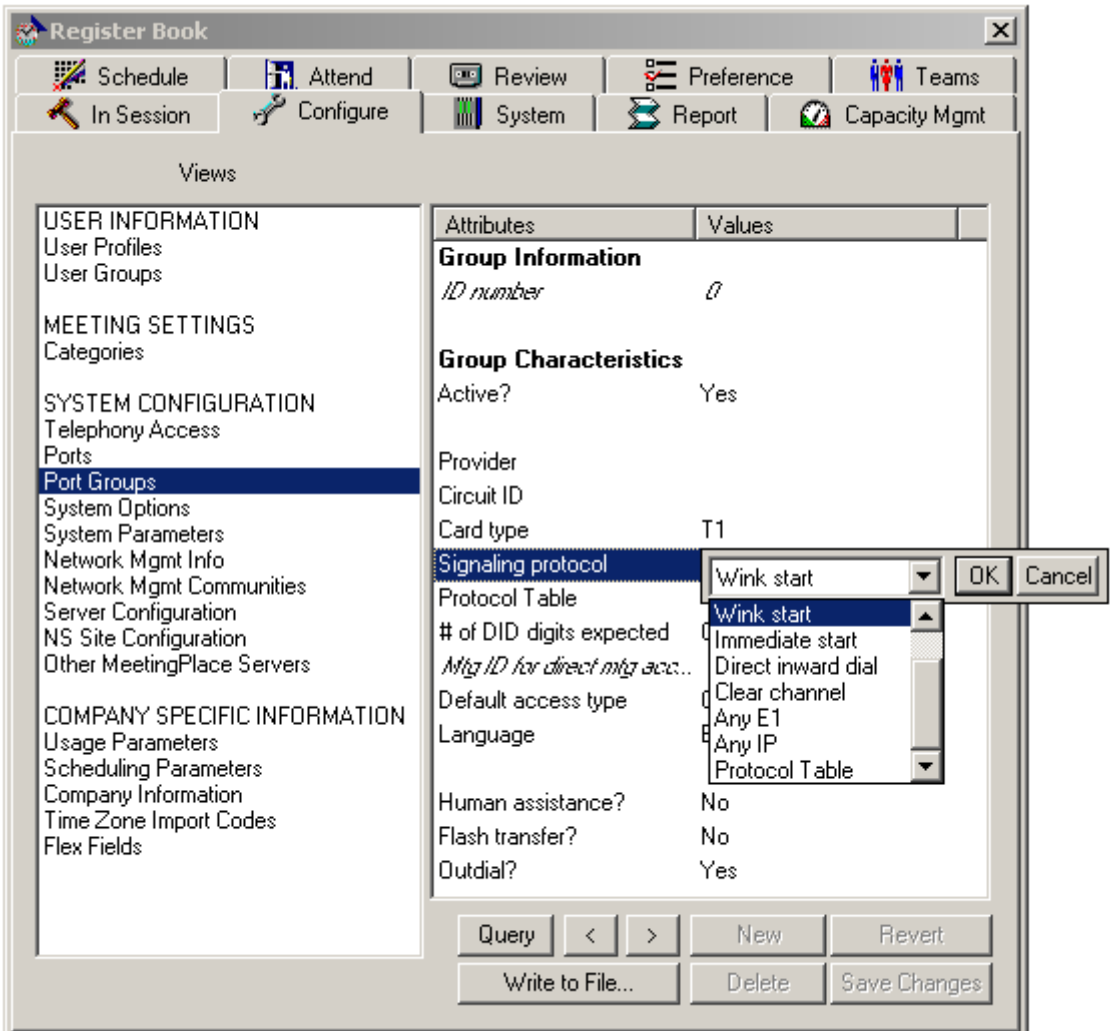
Step 8 Change the attributes by doing the following:

a. Click the value. Not all values can change. If the value can change, an editable field appears containing the current value just clicked.

b. Enter a new value or select one from the drop-down menu.

c. Click **OK**. The field disappears and the new value appears. See Figure 4-92.

Figure 4-92 Changing an Attribute's Value Dialog Box

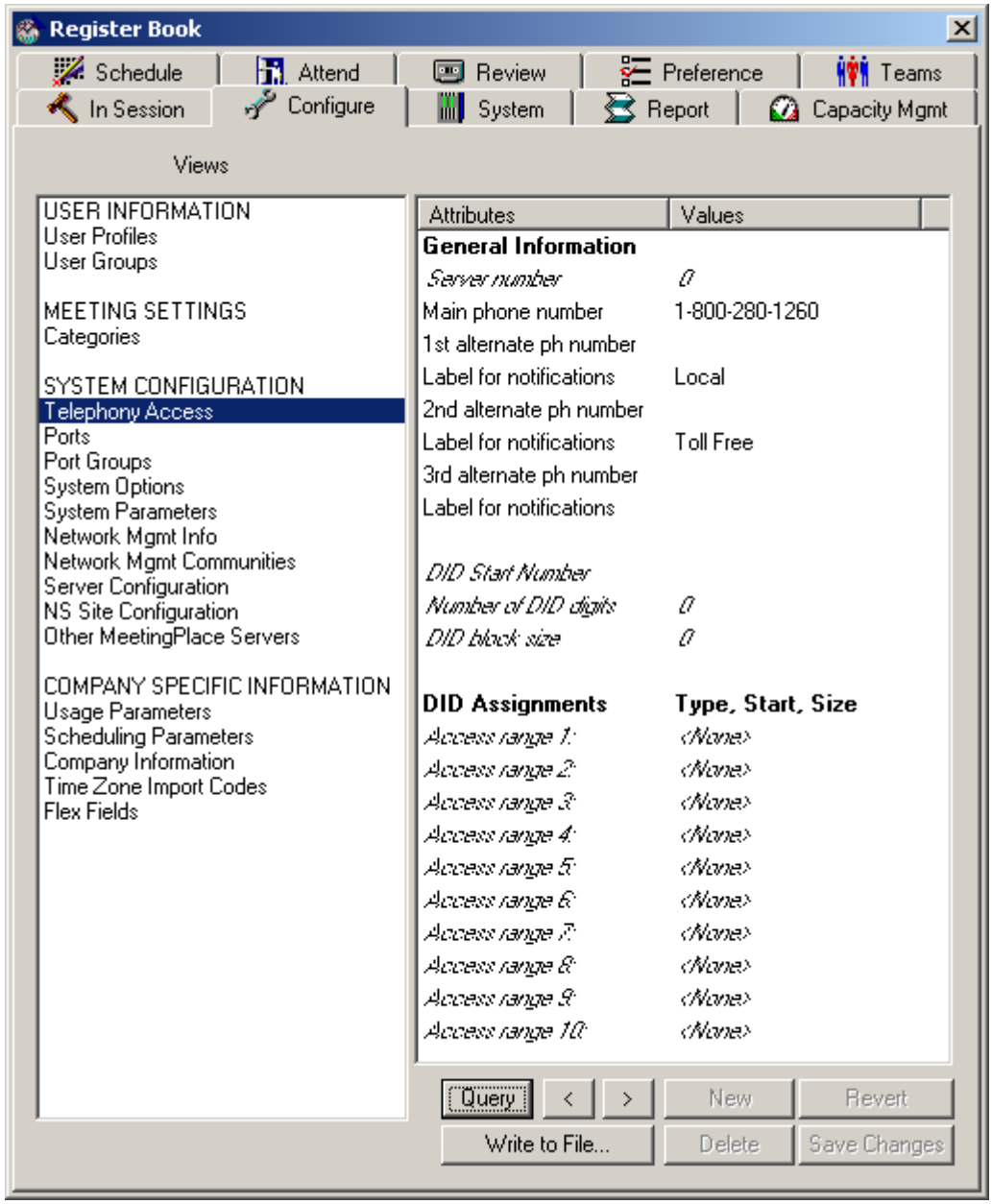


Step 9 Make changes to the attributes for port group 0 based on the information in worksheet 4-7 in the *MeetingPlace Audio Server 5.2 Installation Planning Guide*.

Step 10 Under **Views**, select **Telephony Access**. Attributes for telephony access appear on the right.

Step 11 Click **Query**. Values appear. See Figure 4-93.

Figure 4-93 MeetingTime Telephony Access Dialog Box

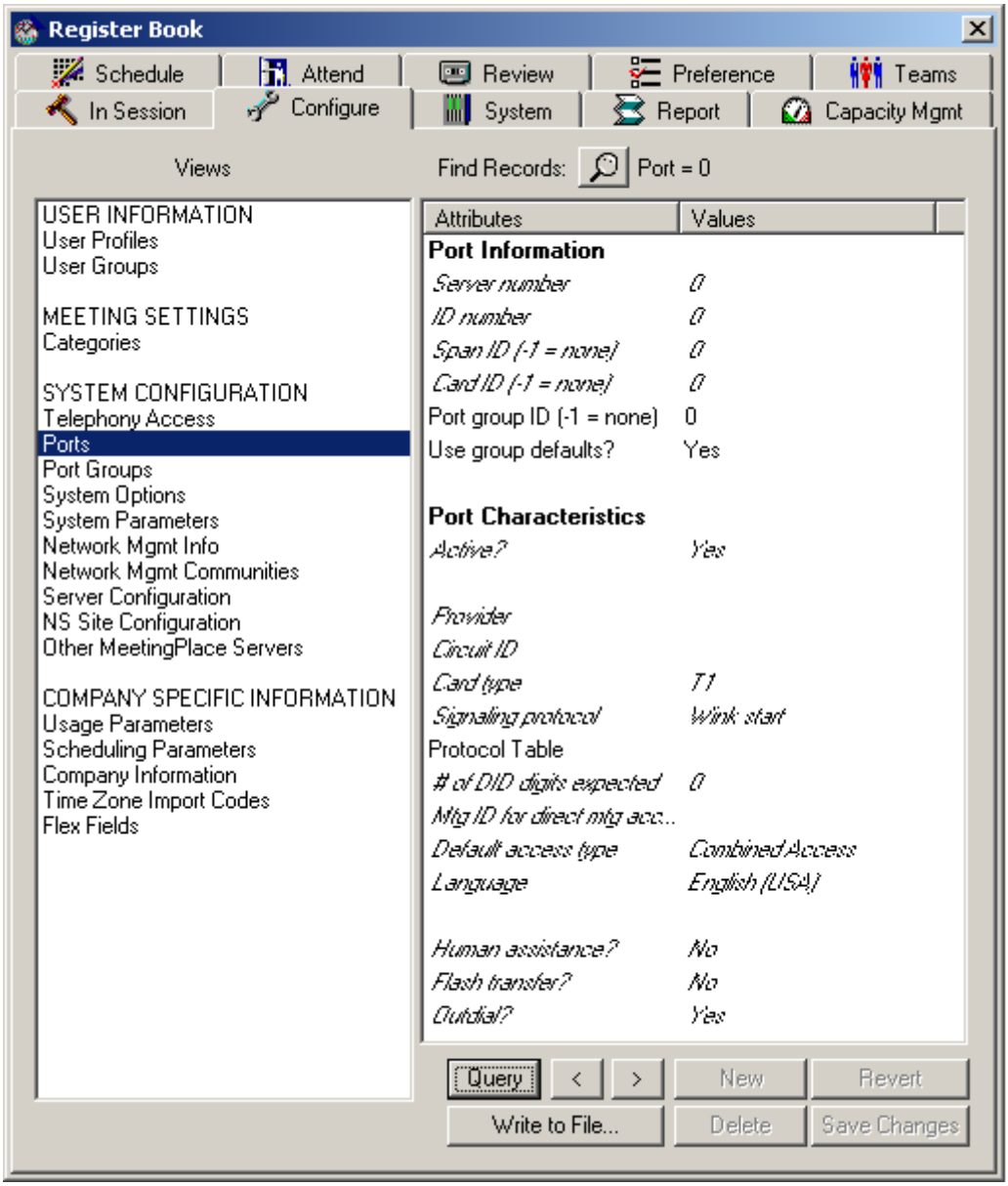


Step 12 Using the technique described in Step 8, make changes to the telephony access attributes based on the information in worksheet 4-5 in the *MeetingPlace Audio Server 5.2 Installation Planning Guide*.

Step 13 Under **Views**, select **Ports**. Attributes for ports appear on the right.

Step 14 Click **Query**. Values appear. See Figure 4-94.

Figure 4-94 MeetingTime Ports Dialog Box

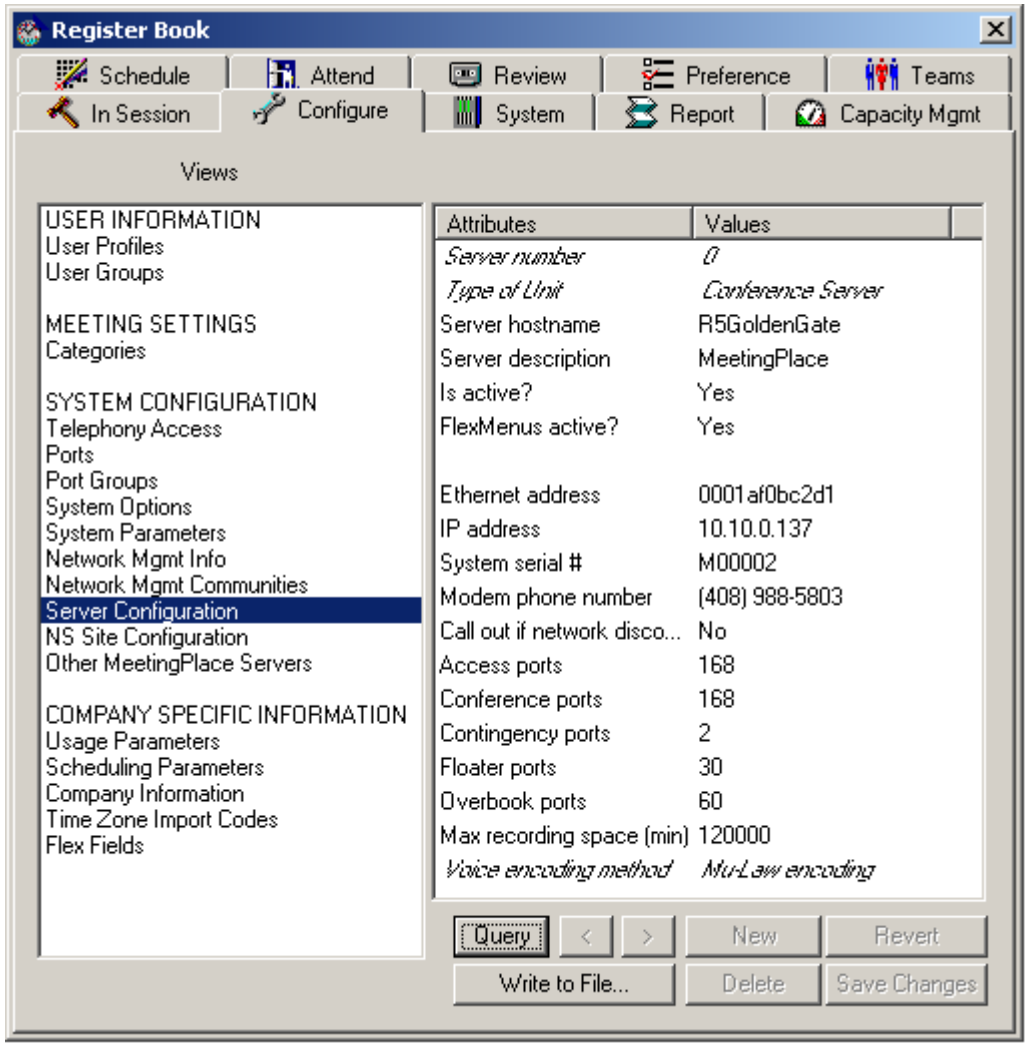


Step 15 Using the technique described in Step 8, make changes to the ports attributes based on the information in worksheet 4-6 in the *MeetingPlace Audio Server 5.2 Installation Planning Guide*.

Step 16 Under **Views**, select **Server Configuration**. Attributes for server configuration appear on the right.

Step 17 Click **Query**. Values appear. See Figure 4-95.

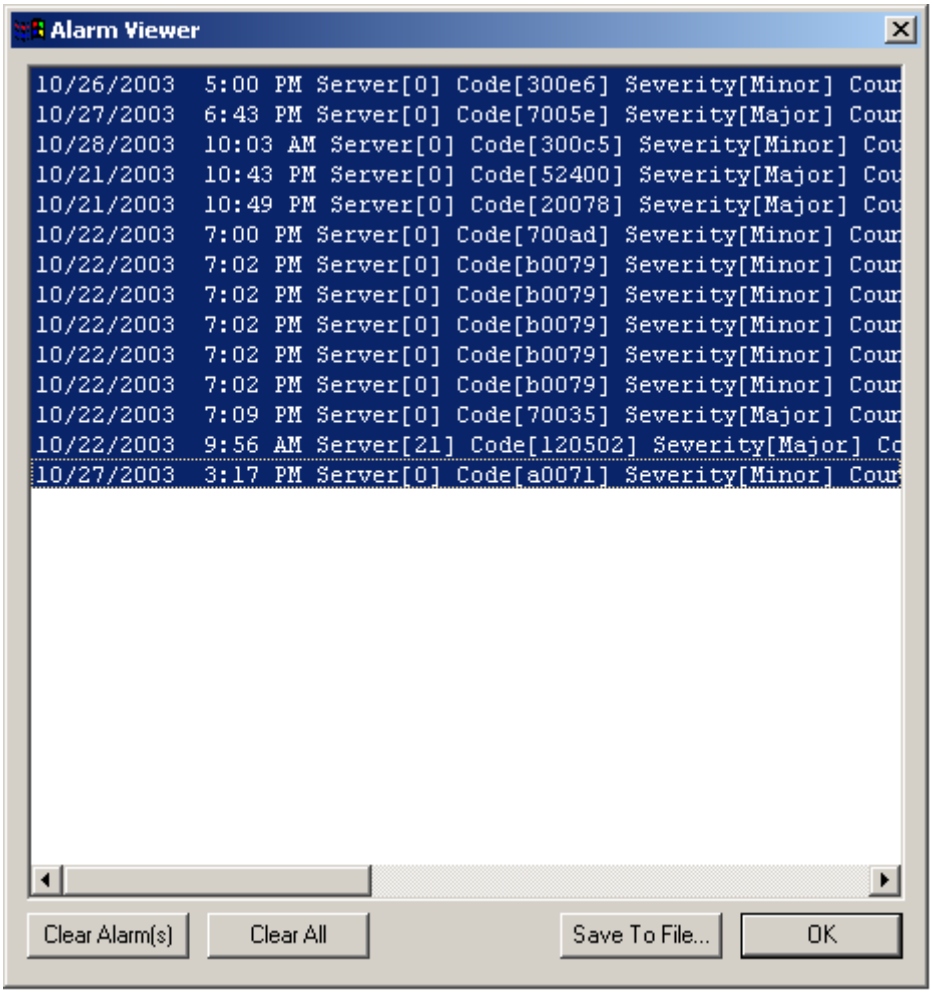
Figure 4-95 MeetingTime Server Configuration Dialog Box



Step 18 Using the technique described in Step 8, make changes to the server configuration attributes.

Step 19 Check the alarm table by selecting the **System** tab, **Alarm Tables**, and click **Execute**. See Figure 4-96.

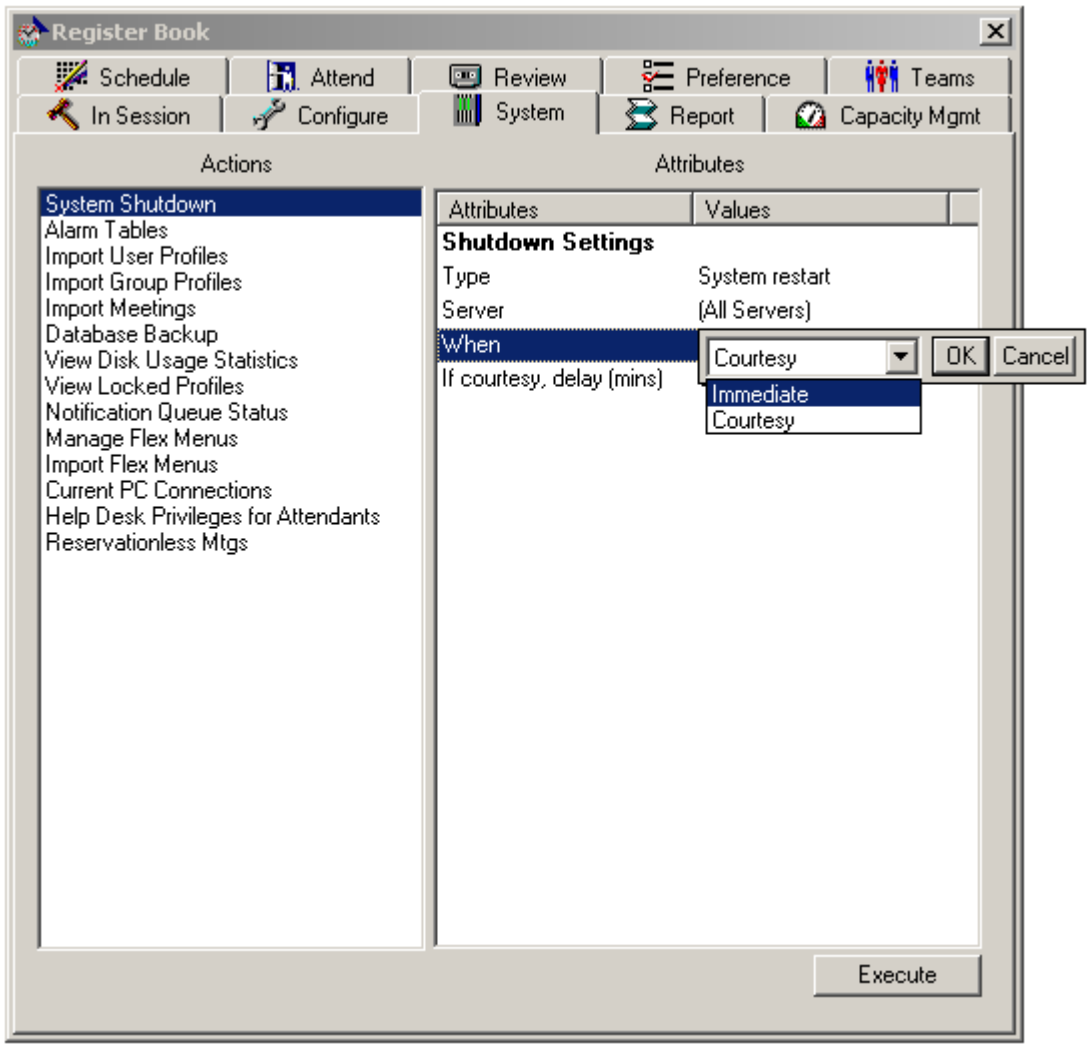
Figure 4-96 MeetingTime Alarm Tables Dialog Box



Step 20 Clear the alarm table by highlighting all the alarms and clicking **Clear Alarm(s)**.

Step 21 Under the **System** tab, select **System Shutdown**. Set attributes to “System restart”, “All Servers”, and “Immediate” and click **Execute** to reboot MeetingPlace. See Figure 4-97.

Figure 4-97 MeetingTime System Shutdown Dialog Box



Testing the installation

After MeetingPlace has restarted (about five minutes), use the following procedure to verify MeetingPlace installation. This section describes how to test the following:

- T1 telephony. Refer to the "Testing T1 telephony" section on page 4-96.
- E1 telephony. Refer to the "Testing E1 telephony" section on page 4-99.
- scheduling. Refer to the "Testing scheduling" section on page 4-101.
- conferencing. Refer to the "Testing conferencing" section on page 4-102.
- network latency. Refer to the "Testing network latency" section on page 4-103.

Testing T1 telephony

To test T1 telephony connectivity, test both inbound and outbound calls.

Testing inbound calls

To verify inbound calls, you must have a means for directly selecting each of the trunks connected to MeetingPlace. Most PBX's and Central Office trunks either:

- use circular hunting, which accesses each port in turn.
- allow each trunk to be selected with a special dialing sequence.

When the PBX uses circular hunting

Step 1 Access the CLI. If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 Type **spanstat <span number> -ab** and press **Enter**. For information about the "spanstat" command, see the "spanstat" section on page A-61. For <span number>, start with span 0 and check each port before moving onto span 1 and other active spans.

Step 3 Dial the system access number.

Step 4 Look at the "spanstat" command output to monitor which port receives the call. For example, in Figure 4-98, span 0, port 1 received the call.

Figure 4-98 spanstat -ab Command — T1

```
meetingplace:tech$ spanstat 0 -ab
    Span 0 (Card 0 Trunk 0) is up

 1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24
TR TR TR TR TR TR TR TR TR TR TR TR TR TR TR TR TR TR TR TR TR TR TR TR
33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Step 5 When you hear the prompt, "Welcome to MeetingPlace", press **2**. The system replies with, "Enter your profile number". This verifies a full two way connection between the PBX/Central Office.

Step 6 Repeatedly, dial the system access number until each port is tested.

Note Type **spanstat help** and press **Enter** to determine the character code definitions and sequences for the various types of connections.

When the PBX does not use circular hunting

Step 1 Ask the PBX administrator for the dialing sequence that controls which port picks up the call.

Step 2 For each port, press **2** and listen for the "Enter your profile number" prompt. This ensures a full two-way connection between the PBX/Central Office.

Step 3 We recommend that PBX/Telco hunt from highest port to lowest port.

Testing outbound calls

If MeetingPlace is connected to a PBX, it is necessary to test outbound calls placed to extensions on the PBX as well as calls placed to the public network. A call should be made on each port. Outbound calls should be tested on PSTN connections as well.

Step 1 Access the CLI. If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 Type **activity** and press **Enter**. Figure 4-99 appears. For more information about the "activity" command, refer to "activity" section on page A-4.

Figure 4-99 activity Command Menu

```
meetingplace:tech$ activity
VUI Configuration: 1152 Sessions, 1200 Confs

 ***    VUI INTERNAL STATUS  UTILITY    ***

DebugMenu:
 1) Quick Status of all Ports            4) Make Test Call
 2) Verbose Status of Port Range         5) Show All Confs
 3) Display complete Port Information    0) Quit
Enter the Command   (0 -- 100):
```

Step 3 To make a test call, type **4** and press **Enter**. A prompt appears as in Figure 4-100 requesting a destination telephone number.

Figure 4-100 activity Command — Make a Test Call

```
meetingplace:tech$ activity
VUI Configuration: 1152 Sessions, 1200 Confs

 ***    VUI INTERNAL STATUS  UTILITY    ***

DebugMenu:
 1) Quick Status of all Ports            4) Make Test Call
 2) Verbose Status of Port Range         5) Show All Confs
 3) Display complete Port Information    0) Quit
Enter the Command   (0 -- 100): 4
You entered 4.
Enter destination for your call:
```

Step 4 Enter the extension of a nearby telephone as the destination phone number to be dialed. A prompt asks if you want specific ports.

Step 5 Enter **t** and press **Enter** for true. A prompt asks if you want to specify a range of ports.

Step 6 Enter **t** and press **Enter** for true. A prompt asks for the starting port number.

Step 7 Enter the lowest number and press **Enter**. A prompt asks for the ending port number.

Step 8 Enter a port number 10 or 20 ports above the starting port number and press **Enter**. A prompt asks if the system should do the test calls in groups.

Step 9 Enter **f** and press **Enter**. A prompt asks for the delay between calls.

Step 10 Enter the desired delay and press **Enter**. If all is correct, the telephone rings.

Step 11 Answer the phone and listen to voice quality. Press 1 and hang up. The telnet display reports the testing of that port is okay. The telephone is called from the next port.

Step 12 Repeat the last step until all the ports in the specified group are tested.

Step 13 Repeat this procedure using the seven digit number (you may need to add a “9” along with the seven digits if connected to a PBX) to place a call to the public network.

Step 14 Enter **0** and press **Enter** to exit the “activity” command.

Troubleshooting telephony configuration

To troubleshoot the telephony testing, follow these steps.

Step 1 Check that the worksheet information was correctly entered into MeetingTime.

Step 2 Check all the physical connections to the system.

Step 3 Check that no LEDs are in a bad state. Refer to the “Understanding the 8112 server’s LEDs” section on page 2-6 for an explanation of the LEDs.

Step 4 If you made any changes to the MeetingTime configuration, access the CLI and type **restart** and press **Enter**.

Step 5 After the system comes back up, repeat the testing procedures.

If these actions do not correct the problem, contact the Cisco TAC.

Testing E1 telephony

To test E1 telephony connectivity, test both inbound and outbound calls.

Testing inbound calls

To verify inbound calls, you must have a means for directly selecting each of the trunks connected to MeetingPlace. Most PBX's and Central Office trunks either:

- use circular hunting, which accesses each port in turn.
- allow each trunk to be selected with a special dialing sequence.

When the PBX uses circular hunting

Step 1 Access the CLI. If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 Type **spanstat <span number> -all** and press **Enter**. For <span number>, start with span 0 and check each port before moving onto span 1 and other active spans.

Step 3 Dial the system access number.

Step 4 Look at the "spanstat" command output to monitor which port receives the call. For example, in Figure 4-101, span 0, port 1 received the call.

Figure 4-101 spanstat -all Command — E1

```
meetingplace:tech$ spanstat 0 -all
    E1 Span 0 (ETI 0 Line A) is up

 1 2 3 4 5  6 7 8 9 0   1 2 3 4 5  6 7 8 9 0   1 2 3 4 5  6 7 8 9 0
                    10                     20                     30
ii........ ..........  .......... ..........  .......... ..........
```

Step 5 When you hear the prompt, "Welcome to MeetingPlace", press **2**. The system replies with, "Enter your profile number". This verifies a full two way connection between the PBX/Central Office.

Step 6 Repeatedly, dial the system access number until each port is tested.

Note Type **spanstat help** and press **Enter** to determine the character code definitions and sequences for the various types of connections.

When the PBX does not use circular hunting

Step 1 Ask the PBX administrator for the dialing sequence that controls which port picks up the call.

Step 2 For each port, press **2** and listen for the "Enter your profile number" prompt. This ensures a full two-way connection between the PBX/Central Office.

Step 3 We recommend that PBX/Telco hunt from highest port to lowest port.

Testing outbound calls

If MeetingPlace is connected to a PBX, you must test outbound calls placed to extensions on the PBX as well as calls placed to the public network. A call should be made on each port. Outbound calls should be tested on PSTN connections, as well.

Step 1 Access the CLI. If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 2 Type **activity** and press **Enter**. Figure 4-99 appears.

Step 3 To make a test call, enter **4**. A prompt appears as in Figure 4-100 requesting a destination telephone number.

Step 4 Enter the extension of a nearby telephone as the destination phone number to be dialed. A prompt asks if you want specific ports.

Step 5 Enter **t** and press **Enter** for true. A prompt asks if you want to specify a range of ports.

Step 6 Enter **t** and press **Enter** for true. A prompt asks for the starting port number.

Step 7 Enter the lowest number and press **Enter**. A prompt asks for the ending port number.

Step 8 Enter a port number 10 or 20 ports above the starting port number and press **Enter**. A prompt asks if the system should do the test calls in groups.

Step 9 Enter **f** and press **Enter**. A prompt asks for the delay between calls.

Step 10 Enter the desired delay and press **Enter**. If all is correct, the telephone rings.

Step 11 Answer the phone and listen to voice quality. Press 1 and hang up. The telnet display reports the testing of that port is OK. The telephone is called from the next port.

Step 12 Repeat the last step until all the ports in the specified group are tested.

Step 13 Repeat this procedure using a seven digit number (you may need to add a "9" along with the seven digits if connected to a PBX) to place a call to the public network.

Step 14 Enter **0** and press **Enter** to exit the "activity" command.

Troubleshooting telephony configuration

To troubleshoot the telephony testing, follow these steps.

Step 1 Check that the worksheet information was correctly entered into MeetingTime.

Step 2 Check all the physical connections to the system.

Step 3 Check that no LEDs are in a bad state. Refer to the "Understanding the 8112 server's LEDs" section on page 2-6 for an explanation of the LEDs.

Step 4 If you made any changes to the MeetingTime configuration, access the CLI and type **restart** and press **Enter**.

Step 5 After the system comes back up, repeat the testing procedures.

If these actions do not correct the problem, contact the Cisco TAC.

Testing scheduling

Beyond basic telephony functionality, verify that users can schedule new meetings. When testing scheduling capability, use the technician profile that shipped with the system.

Testing voice interface

Step 1 Verify that you can schedule immediate meetings via the phone interface.

Step 2 Verify you can attend that scheduled meeting.

Step 3 Verify that you can schedule a future meeting via the phone interface.

Testing MeetingTime

Verify you can schedule a meeting via MeetingTime.

Testing MeetingPlace Web

If MeetingPlace Web has been installed, verify that meetings can be scheduled via this interface.

Testing MeetingPlace for Microsoft Outlook and MeetingPlace for Lotus Notes

If MeetingPlace for Microsoft Outlook or MeetingPlace for Lotus Notes is installed, verify that meetings can be scheduled using these interfaces.

Testing notifications

If the MeetingPlace notification option is enabled, verify you can receive notifications when meetings are scheduled.

Testing conferencing

Verify conferencing functionality by scheduling and attending meetings.

Testing recorded meetings

If the system is configured for recordings, follow this procedure. If it is not, proceed to the next section, "Testing non-recorded meetings, ad hoc recording" section on page 4-102.

Step 1 Schedule a recorded meeting.

Step 2 Verify that the meeting is indeed recorded and retrievable after the meeting.

Testing non-recorded meetings, ad hoc recording

If the system is configured for recordings, follow this procedure. If it is not, proceed to the next section, "Testing web conferencing" section on page 4-102.

Step 1 Schedule a meeting without recording.

Step 2 Attend the meeting and activate the recording by pressing #61.

Step 3 Verify that the meeting is indeed recorded and that it is retrievable after the meeting.

Testing web conferencing

If web conferencing is installed, refer to the *Web Conferencing System Manager's Guide* to perform a functional check.

Testing network latency

To test for network latency, follow this procedure.

Step 1 Access the CLI and type **ping -s 1000 <IP address of another machine on the network>** and then press **Enter**.

Step 2 Once you have received several reply messages, type **<Ctrl> C**.

If there is no reply, the MeetingPlace server cannot make a network connection to the machine you specified. Verify the IP address and consult the internal networking contacts.

Step 3 Verify there is 0% packet loss. See Figure 4-102.

Figure 4-102 Testing Network Latency

```
meetingplace:tech$ ping -s 1000 172.20.19.25
--- Type <CTRL-C> to stop ---
PING 172.20.19.25 (172.20.19.25): 1000 data bytes
1008 bytes from 172.20.19.25: icmp_seq=0 ttl=255 time=2.897 ms
1008 bytes from 172.20.19.25: icmp_seq=1 ttl=255 time=2.584 ms
1008 bytes from 172.20.19.25: icmp_seq=2 ttl=255 time=2.587 ms
1008 bytes from 172.20.19.25: icmp_seq=3 ttl=255 time=2.578 ms
1008 bytes from 172.20.19.25: icmp_seq=4 ttl=255 time=2.615 ms
1008 bytes from 172.20.19.25: icmp_seq=5 ttl=255 time=2.582 ms
1008 bytes from 172.20.19.25: icmp_seq=6 ttl=255 time=2.577 ms
1008 bytes from 172.20.19.25: icmp_seq=7 ttl=255 time=2.586 ms
^C
--- 172.20.19.25 ping statistics ---
8 packets transmitted, 8 packets received, 0% packet loss
round-trip min/avg/max = 2.571/2.603/2.897 ms
```

Repairing and Maintaining the 8112 Server

This chapter provides instructions on repairing and maintaining the MeetingPlace Audio Server 5.2 for the 8112 server. It covers the replacement procedures for the field-replaceable units (FRUs) listed in Table 5-1 and the regular maintenance required.

Table 5-1 Field-replaceable Units

FRU	Section and Page
Disk drive	"Replacing a disk drive" section on page 5-7
CD-ROM drive	"Replacing the CD-ROM drive" section on page 5-10
Power supply unit	"Replacing a power supply unit" section on page 5-11
Power supply unit fan filter	"Replacing a power supply unit fan filter" section on page 5-14
floppy drive	"Replacing the floppy drive" section on page 5-16
CPU	"Replacing the CPU" section on page 5-20
Hot swap controller	"Replacing the hot swap controller" section on page 5-26
T1 Smart Blade and Smart Blades	"Replacing T1 Smart Blades or Smart Blades" section on page 5-29
Multi Access Blade	"Replacing a Multi Access Blade" section on page 5-32
Modem	"Replacing the modem" section on page 5-33

Note The Travan NS20 tape drive is no longer used by the 8112 server. When the 8112 server was upgraded, the tape drive was replaced by a CD-ROM drive. If you need instructions on how to remove the Travan NS20 tape drive, refer to the *MeetingPlace Audio Server 5.2 Upgrade and Installation Document*. For instructions on installing a CD-ROM drive, see the "Installing the new CD-ROM drive" section on page 5-10.

The majority of repair procedures require the following sequence of activities:

1. Schedule the repair. Refer to the "Scheduling the repair" section on page 5-2.
2. Prepare for the repair, including the following steps:
   - Verify no user activity. Refer to the "Verifying no user activity" section on page 5-3.
   - Back up the database. Refer to the "Backing up the database" section on page 5-4.
   - Power down MeetingPlace. Refer to the "Powering down MeetingPlace" section on page 5-5.
3. Perform and test the repair. Refer to the following sections:
   - "Replacing a disk drive" section on page 5-7
   - "Replacing the CD-ROM drive" section on page 5-10
   - "Replacing a power supply unit" section on page 5-11
   - "Replacing a power supply unit fan filter" section on page 5-14
   - "Replacing the floppy drive" section on page 5-16
   - "Replacing the CPU" section on page 5-20
   - "Replacing the hot swap controller" section on page 5-26
   - "Replacing T1 Smart Blades or Smart Blades" section on page 5-29
   - "Replacing a Multi Access Blade" section on page 5-32
   - "Replacing the modem" section on page 5-33
4. Power up MeetingPlace. Refer to the "Powering up the server" section on page 4-17.

Scheduling the repair

Before going to the customer site, arrange with the customer site contact for a no-meeting period for the amount of time the repair requires.

Preparing for the repair

This section explains the steps that need to be performed prior to replacing any of the FRUs mentioned in this chapter.

Step 1 Inspect the piece of new hardware to verify no damage occurred in transit.

Step 2 Verify your toolkit contains the correct tools for the repair. Refer to Appendix B, "Required Toolkit" for a list of required tools.

Note If you are replacing any of the power supply units or power supply fan filters, you do not need to complete the rest of this section. Go directly to the "Replacing a power supply unit" section on page 5-11 and "Replacing a power supply unit fan filter" section on page 5-14.

Verifying no user activity

This section explains how to verify there is no user activity on the system before shutting it down for the repair.

Step 1 If not already connected, access the command line interface (CLI) by following the procedures in the "Connecting your laptop" section on page 4-1 and "Setting up your laptop" section on page 4-3.

Note CLI commands are case sensitive. For CLI command information, refer to Appendix A, "CLI Reference".

Step 2 Log in as technician. The tech$ prompt appears.

Step 3 Start logging your terminal session. For information on logging, see "Logging your HyperTerminal session" section on page 4-6.

Step 4 Verify there is no user activity by typing **activity** and pressing **Enter**. A menu appears as in Figure 5-1.

Figure 5-1 activity Command Menu

```
meetingplace:tech$ activity
VUI Configuration: 1152 Sessions, 1200 Confs

 ***    VUI INTERNAL STATUS  UTILITY    ***

DebugMenu:
 1) Quick Status of all Ports            4) Make Test Call
 2) Verbose Status of Port Range         5) Show All Confs
 3) Display complete Port Information    0) Quit
Enter the Command   (0 -- 100):
```

Step 5 Type **1** and press **Enter** to see a quick status of all ports. Figure 5-2 appears. Dashes indicate an inactive port, "CO" indicates the port is in a conference, and "PR" indicates the port is in a user profile.

Figure 5-2 Verifying No User Activity

```
Enter the Command   (0 -- 100): 1
You entered 1.

Port Ap : Port Ap : Port Ap : Port Ap : Port Ap : Port Ap : Port Ap :
   0 -- :   18 -- :   36 -- :   54 -- :   72 -- :   90 -- :  108 -- :
   1 -- :   19 -- :   37 -- :   55 -- :   73 -- :   91 -- :  109 -- :
   2 -- :   20 -- :   38 -- :   56 -- :   74 -- :   92 -- :  110 -- :
   3 -- :   21 -- :   39 -- :   57 -- :   75 -- :   93 -- :  111 -- :
   4 -- :   22 -- :   40 -- :   58 -- :   76 -- :   94 -- :  112 -- :
   5 -- :   23 -- :   41 -- :   59 -- :   77 -- :   95 -- :  113 -- :
   6 -- :   24 -- :   42 -- :   60 -- :   78 -- :   96 -- :  114 -- :
   7 -- :   25 -- :   43 -- :   61 -- :   79 -- :   97 -- :  115 -- :
   8 -- :   26 -- :   44 -- :   62 -- :   80 -- :   98 -- :  116 -- :
   9 -- :   27 -- :   45 -- :   63 -- :   81 -- :   99 -- :  117 -- :
  10 -- :   28 -- :   46 -- :   64 -- :   82 -- :  100 -- :  118 -- :
  11 -- :   29 -- :   47 -- :   65 -- :   83 -- :  101 -- :  119 -- :
  12 -- :   30 -- :   48 -- :   66 -- :   84 -- :  102 -- :  120 -- :
  13 -- :   31 -- :   49 -- :   67 -- :   85 -- :  103 -- :  121 -- :
  14 -- :   32 -- :   50 -- :   68 -- :   86 -- :  104 -- :  122 -- :
  15 -- :   33 -- :   51 -- :   69 -- :   87 -- :  105 -- :  123 -- :
  16 -- :   34 -- :   52 -- :   70 -- :   88 -- :  106 -- :  124 -- :
  17 -- :   35 -- :   53 -- :   71 -- :   89 -- :  107 -- :  125 -- :
Hit l for legend, q for quit, ENTER for next page:
```

Step 6 Scan the list of ports. Type **l** and press **Enter** to see the legend or press **Enter** to go to the next page. Continue until you have seen all the ports. If there is anything but dashes, explain to the site contact that some ports are currently in use and ask if it is alright to move forward with the repair.

Even though the site contact should have scheduled meetings to book all ports for the repair, users may be dialing in to schedule meetings or to listen to meeting recordings.

Step 7 When all the ports have been shown, the "activity" command menu appears again. Type **0** and **Enter** to exit the "activity" command menu. The tech$ prompt appears.

Step 8 Use MeetingTime to verify that the only meetings scheduled for the time required to perform the repair belong to the site contact.

Backing up the database

The backup mechanism has changed in this version of the MeetingPlace Audio Server. It is now done through the MeetingPlace Backup Gateway. For information on how to install, configure, and use the backup mechanism, refer to the *MeetingPlace Backup Gateway System Manager's Guide*.

Powering down MeetingPlace

Follow this procedure to power down MeetingPlace *before* turning the power switch to the off ("O") position.

Step 1 If not already connected, access the CLI by following the procedures in the "Connecting your laptop" section on page 4-1 and "Setting up your laptop" section on page 4-3.

Step 2 Log in as technician. The tech$ prompt appears.

Step 3 Type **halt** and press **Enter**.

Step 4 The second line in Figure 5-3 appears. Type **y** and press **Enter** to confirm that you do want to power down the system.

Figure 5-3 halt Command

```
meetingplace:tech$ halt
Are you sure (y/n)? y
NMI ioctl: Argument invalid/improper
Checking to see if the system is loaded...OK
System DOWN procedure has been initiated.

System HALT sequence has been initiated.
Please do not kill power until you see the "LynxOS is down" message.
meetingplace:tech$ The MeetingPlace software is DOWN
---> Halting the system

**** LynxOS is down ****
```

Step 5 The rest of Figure 5-3 appears. Wait for the "`**** LynxOS is down ****`" message to appear as shown in the last line of Figure 5-3.

Step 6 Turn the power switch on the back of the server to the off ("O") position. See Figure 5-4.

Figure 5-4 Components on the Back of the 8112 Server

Step 7 Remove the power cable from the back of the server. See Figure 5-5.

Figure 5-5 8112 Server's Power Cable

Replacing a disk drive

This section describes how to replace a disk drive on the 8112 server. There are two disk drives and one common spare. The replacement procedure is the same for both.

Warning **DO NOT touch the disk drive key unless the server is completely shut down and powered off.**

Removing an old disk drive

Step 1 Verify that all of the steps in the "Preparing for the repair" section on page 5-2 have been completed.

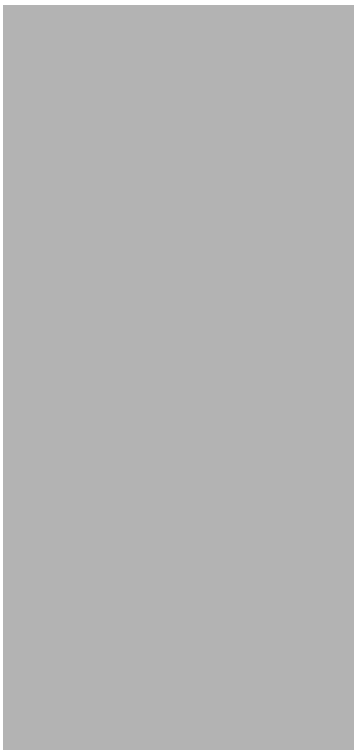
Step 2 Identify which disk drive you are replacing. See Figure 5-6.

Figure 5-6 8112 Server's Hardware Components

Step 3 Push in the disk drive's keyswitch and turn the key counter-clockwise for a quarter of a turn. Turning the keyswitch unlatches the disk drive and carrier from the bay.

Step 4 Pull the disk drive straight out of the bay. See the "Figure 5-7Removing a Disk Drive" section on page 5-9.

Figure 5-7 Removing a Disk Drive



Installing a new disk drive

Step 1 Ensure the system is powered down. If you are installing a new disk drive immediately after removing an old one, the system should still be powered down. Otherwise, follow the steps in "Preparing for the repair" section on page 5-2.

Step 2 Slide the new disk drive straight into the empty drive bay. You hear a click when it is completely in.

Step 3 Secure the disk drive by pushing the keyswitch in and turning it clockwise for a quarter of a turn. This latches the disk drive and carrier into the frame.

Step 4 Attach the power cable to the back of the server.

Step 5 Power up the server. Refer to "Powering up the server" section on page 4-17.

Step 6 Test that the disk drive is correctly installed. See the "Testing the installation" section on page 4-95 for more information.

Replacing the CD-ROM drive

This section describes how to replace a CD-ROM drive.

Warning **Handling the CD-ROM drive can result in static damage. Use an anti-static wrist strap, static-dissipating work surface, and anti-static bags when handling and storing it.**

Removing the old CD-ROM drive

Step 1 Verify that all of the steps in the "Preparing for the repair" section on page 5-2 have been completed.

Step 2 Identify where the CD-ROM drive is located. It is always in the front of the server. See the "Figure 5-68112 Server's Hardware Components" section on page 5-8.

Step 3 Loosen the four captive screws in the corners of the drive bay housing in the *front* of the 8112 server. See the "Figure 5-68112 Server's Hardware Components" section on page 5-8.

Step 4 Loosen the four captive screws in the corners of the floppy drive housing in the *back* of the 8112 server. See Figure 5-4.

Step 5 Pull the floppy drive housing partially out of the back of the chassis.

Step 6 From the back of the 8112 server, remove the IDE cable from the server's inner connector and remove the power cables from the CD-ROM drive.

Step 7 From the front of the 8112 server, slide the CD-ROM drive out.

Installing the new CD-ROM drive

Step 1 Loosen the four captive screws in the corners of the drive bay housing in the *front* of the 8112 server. See Figure 5-6.

Step 2 Loosen the four captive screws in the corners of the floppy drive housing in the *back* of the 8112 server. See Figure 5-4.

Step 3 Pull the floppy drive housing partially out of the back of the chassis.

Step 4 Locate the IDE cable and attach it to the back of the CD-ROM drive. Be sure to attach it the correct way.

Step 5 Thread the free end of the IDE cable through the empty CD-ROM drive slot from the front of the server towards the back.

Step 6 Attach the power cable to the back of the CD-ROM drive.

Step 7 From the front of the 8112 server, gently slide in the CD-ROM drive as far as it can go.

Step 8 From the back of the 8112 server, pull the CD-ROM drive towards you as far as possible. Plug the CD-ROM drive's IDE cable into the server's inner connector and plug the free end of the power cable into the server.

Step 9 Tighten the four captive screws in the corners of the floppy drive housing in the *back* of the 8112 server.

Step 10 Tighten the four captive screws in the corners of the floppy drive housing in the *back* of the 8112 server.

Step 11 Power up the server. Refer to the "Powering up the server" section on page 4-17.

Step 12 Test that the CD-ROM drive is correctly installed. See the "Testing the installation" section on page 4-95 for more information.

Replacing a power supply unit

This section describes how to replace a power supply unit. The power supply unit consists of the power supply and the power supply's fan. This power supply unit is considered one single FRU. These components should not be removed or replaced separately. The only exception is that the power supply unit fan *filter* can be removed separately. See "Replacing a power supply unit fan filter" section on page 5-14 for more information on the power supply unit fan filter.

Removing an old power supply unit

Note The 8112 server has three power supply units. You can remove any one of the power supply units without shutting down the server or affecting performance.

To replace two or three power supply units at once, you must power down the 8112 server. Refer to the "Powering down MeetingPlace" section on page 5-5.

Step 1 Verify there is no user activity and back up the database. Refer to "Verifying no user activity" section on page 5-3 and "Backing up the database" section on page 5-4.

Step 2 Identify which power supply unit you are replacing. See Figure 5-6.

Step 3 Using a screwdriver, loosen the two captive screws located at the bottom of the power supply sled to be removed. See Figure 5-8.

Warning **Do not touch any of the exposed leads, terminals, or components. Hazardous voltages, capable of causing death, may be present in this product.**

Figure 5-8 Power Supply Unit Captive Screws

Step 4 Using the handle on the front of the power supply unit sled, pull the power supply unit sled slowly straight out of the chassis. Support the sled from the bottom and lift the back edge of it over the front lip of the chassis. See Figure 5-9.

Figure 5-9 Removing a Power Supply Unit

Installing a new power supply unit

Warning **Do not touch any of the exposed leads, terminals, or components. Hazardous voltages, capable of causing death, may be present in this product.**

Step 1 Slowly slide the power supply unit sled into the chassis. Guides on the chassis and rails on the power supply unit sled assist in properly aligning the power supply unit sled during insertion.

Note The power supply unit sled should be inserted with a single, steady motion. Bouncing the power supply unit sled during insertion may cause an alarm condition in the system.

Step 2 Tighten the two captive screws located at the bottom front of the power supply unit. See Figure 5-8.

Note If you are replacing more than one power supply unit, follow the above procedure for each power supply unit. Once they have all been replaced, attach the power cable to the back of the server and power up the server. Refer to the "Powering up the server" section on page 4-17.

Step 3 Test that the power supply unit is correctly installed. See "Testing the installation" section on page 4-95 for more information.

Replacing a power supply unit fan filter

This section describes how to replace the power supply unit fan filter.

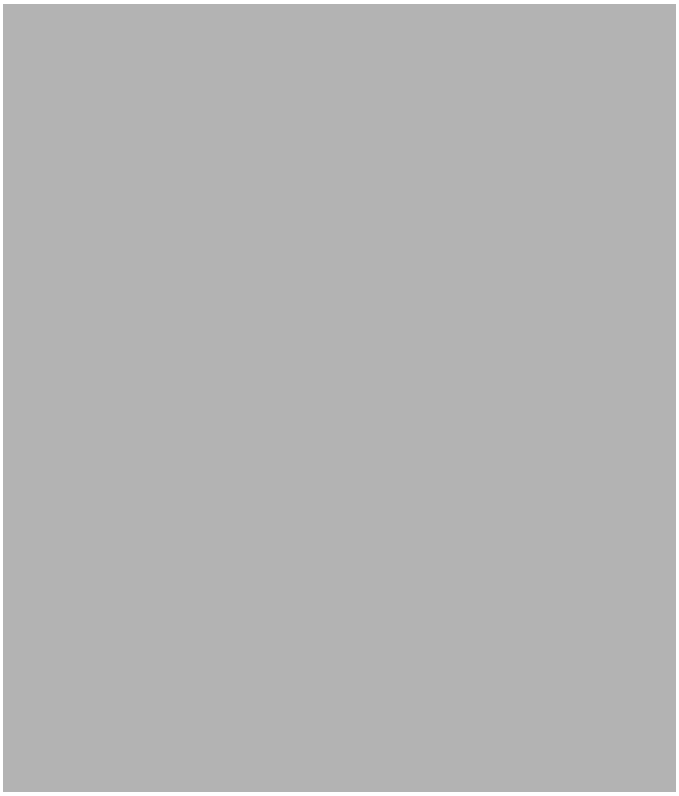
Removing an old power supply unit fan filter

Step 1 Verify there is no user activity and back up the database. Refer to the "Verifying no user activity" section on page 5-3 and "Backing up the database" section on page 5-4.

Warning **Do not touch any of the exposed leads, terminals, or components. Hazardous voltages, capable of causing death, may be present in this product.**

Step 2 Pull out the top edge of the filter frame by using the metal tab in the top left corner of the filter. See Figure 5-10.

Figure 5-10 Power Supply Unit Fan Filter



Step 3 Pull the fan filter's frame up at a slight angle to remove it, sliding it in between the power supply unit and the power supply unit handle.

Step 4 Remove the power supply unit fan filter from its frame.

Installing a new power supply unit fan filter

Step 1 Slide the new power supply unit fan filter into the power supply unit fan filter frame.

Step 2 Place the new power supply unit fan filter frame between the power supply unit and the power supply unit handle.

Note The correct orientation is when the metal tab on the new power supply unit fan filter frame is in the top left corner. See Figure 5-10.

Step 3 Gently push the new power supply unit fan filter frame into place. There is no lock position, just make sure the new power supply unit fan filter frame stays in place. You do not need to use much force.

Step 4 Attach the power cable to the back of the server.

Step 5 Power up the server. Refer to the "Powering up the server" section on page 4-17.

Testing the power supply unit fan filter

Step 1 If not already connected, access the CLI by following the procedures in the "Connecting your laptop" section on page 4-1 and "Setting up your laptop" section on page 4-3.

Step 2 Login as a technician. The tech$ prompt appears.

Step 3 Turn on terminal logging. For information on logging, see "Logging your HyperTerminal session" section on page 4-6.

Step 4 Type **hwconfig** and press **Enter**. Figure 5-11 appears.

Figure 5-11 hwconfig Command

```
meetingplace:tech$ hwconfig
Cabinet:                Motorola CPX8216T
Bus architecture:       CompactPCI
Processor card:         CPV5370 S/N=5129443
    Processor:          Pentium III, Model 8, 700 MHz
    Memory:             512MB
    Temperature:        31C
    Voltages:           3.32V, 5.02V, 12.06V
Power Supplies:
    PS1:                OK, fan is OK
    PS2:                OK, fan is OK
    PS3:                OK, fan is OK
SCSI Adapter:           NCR 810
    DISK 1:             36000MB (SEAGATE  ST336704LW       REV=0004)
    DISK 2:             36000MB (SEAGATE  ST336704LW       REV=0004)
    Solid State Disk:   IMPERIAL "MG-35/400 ULTRA" S/N=0128 REV=B403
                        Battery: usage = 307 days, charge is OK
Ethernet:               Intel 8225x PCI 10/100 (0001af03c05e)
Modem:                  Absent or unrecognized
Smart Blades:
    Slot 16:            NMS CG6000C S/N=20363257 REV=5894-B2 MSC0 PRC0
    Slot 15:            NMS CG6000C S/N=20363261 REV=5894-B2 MSC1 PRC1
```

Step 5 Verify the output for the power supply units and their fans is like lines 9-12 in Figure 5-11.

Note The floppy drive and CD-ROM drive do not show up in the “hwconfig” command output even when they are installed and running.

Replacing the floppy drive

This section describes how to replace a floppy drive.

Note The floppy drive is housed in the back of the server. The floppy drive housing must be removed from the server before replacing the actual floppy drive.

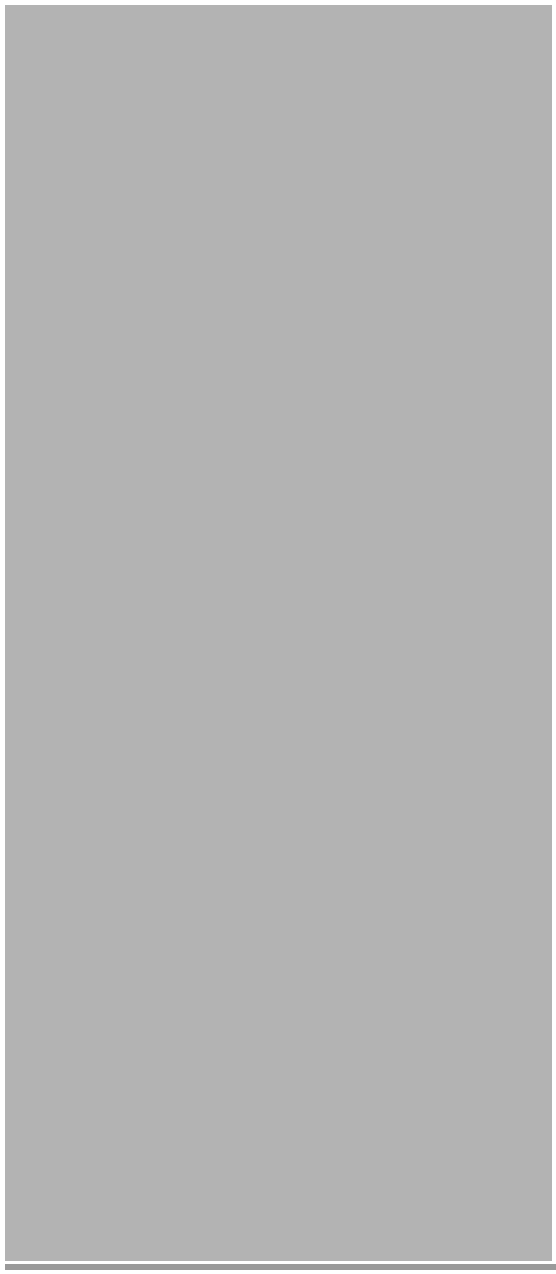
Removing the floppy drive housing

Step 1 Verify all steps in the section the "Preparing for the repair" section on page 5-2 have been completed.

Step 2 Loosen the four captive screws in the corners of the floppy drive housing. See Figure 5-4.

Step 3 Pull the floppy drive housing straight out of the chassis. See Figure 5-12.

Figure 5-12 Floppy Drive Housing



Removing the floppy drive

Step 1 Remove the ribbon and power cables from the floppy drive. See Figure 5-13. Note the orientation of the floppy drive cables so you can replace them in the same position.

Figure 5-13 Floppy Drive Cables

Step 2 Loosen the captive screws holding the floppy drive to the floppy drive housing and pull the drive free. See Figure 5-14.

Figure 5-14 Floppy Drive Screws

Installing the new floppy drive

Step 1 Insert the floppy drive into the floppy housing.

Step 2 Fasten the floppy drive to the floppy housing with the captive screws. See Figure 5-14.

Step 3 Connect the non-keyed end of the floppy drive ribbon cable to the connector on the back of the floppy drive. Be sure to align the cable correctly. See Figure 5-13.

Step 4 Connect the other end of the floppy drive ribbon cable (the keyed end) to the power connector on the back of the drive.

Installing the floppy housing

Step 1 Slide the floppy housing straight into the chassis and secure it with the four captive screws in the corners of the housing. See Figure 5-12.

Step 2 Attach the power cable to the back of the server.

Step 3 Power up the server. Refer to the "Powering up the server" section on page 4-17.

Testing the floppy drive

Step 1 If not already connected, access the CLI by following the procedures in the "Connecting your laptop" section on page 4-1 and "Setting up your laptop" section on page 4-3.

Step 2 Login as a technician. The tech$ prompt appears.

Step 3 Turn on terminal logging. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 4 Type **hwconfig** and press **Enter**. Figure 5-11 appears.

Step 5 Verify that the "Diskette drive" entry shows that a floppy is present as in Line 19 in Figure 5-11.

Step 6 Test that the floppy drive is correctly installed. See the "Testing the installation" section on page 4-95 for more information.

Replacing the CPU

The section describes how to replace the CPU card (located on the front of the server) and the CPU transition module (located in the back of the server).

Warning **Handling the CPU card can result in static damage. Use an anti-static wrist strap, static-dissipating work surface, and anti-static bags when handling and storing the card.**

Note Any time the CPU card is replaced, you need new license keys for the MeetingPlace server. If you do not have these, contact the Cisco TAC before proceeding.

Note The CPU card always goes into slot 7 in the front of the server. It also has a transition module in the slot 7 in the back of the server. Whenever the CPU card is replaced, this transition module must also be replaced.

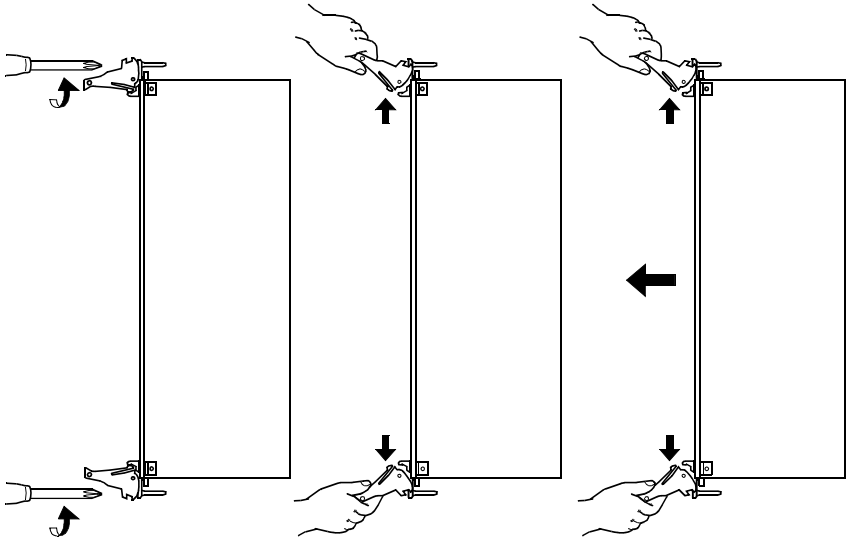
Removing the old CPU card

Step 1 Verify all steps in the "Preparing for the repair" section on page 5-2 have been completed.

Step 2 Locate the CPU card in slot 7 in the front of the server. See Figure 5-6.

Step 3 With a screwdriver, loosen the CPU card's captive screws at the top and bottom of the panel. See Figure 5-15.

Figure 5-15 Removing the CPU Card and Transition Module



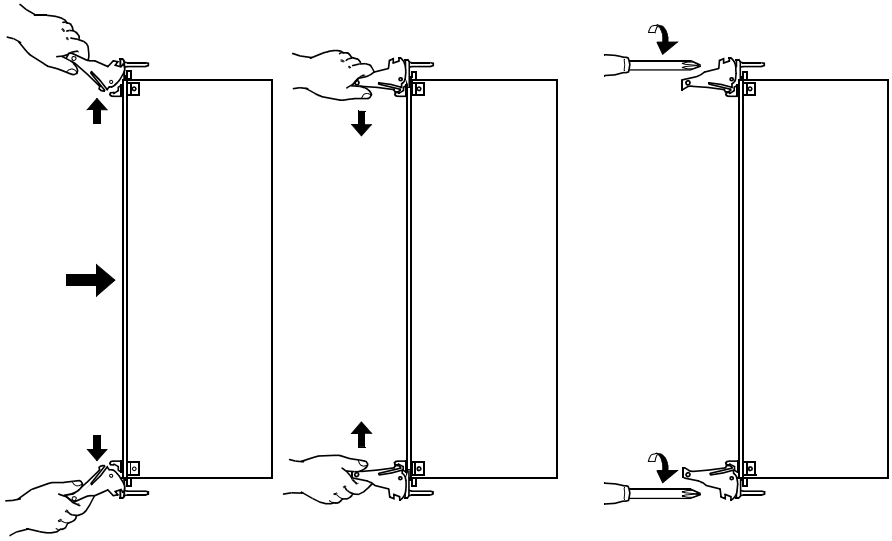
Step 4 Press the ejector levers outward. This partially unseats the CPU card from the backplane connectors. See Figure 5-15.

Step 5 Pull the CPU card out from the chassis by pressing the ejector levers outward and pulling the CPU card out. See Figure 5-15.

Installing the new CPU card

Step 1 Press the ejector levers outward. See Figure 5-16.

Figure 5-16 Installing the CPU Card and Transition Module



Step 2 Holding the CPU card by the ejector levers, partially insert the CPU card into the slot, about half way.

Step 3 Verify that the CPU card is properly seated in the guides on the top and bottom. If not, remove the CPU card and try again.

Step 4 Pushing gently and firmly on the CPU card's face plate, slide the CPU card into the slot until you encounter significant resistance. At this point, the ejector levers should be in contact with the chassis rails so they grab when pushed inward.

Step 5 Use the ejector levers to lock the CPU card in the slot by pushing the ejector levers toward one another until they are in the locked position. See Figure 5-16.

Step 6 Secure the CPU card by tightening the captive screws on the right and left sides of the panel. See Figure 5-16.

Step 7 Verify that any empty slots have covers on them.

Warning **An empty slot that is uncovered can result in a destructive hardware failure.**

Step 8 Attach the power cable to the back of the server.

Step 9 Power up the server. Refer to the "Powering up the server" section on page 4-17.

Removing the old CPU transition module

Step 1 Verify all steps in the "Preparing for the repair" section on page 5-2 have been completed.

Step 2 Locate the CPU transition module in slot 7 in the back of the server.

Step 3 With a screwdriver, loosen the CPU transition module's captive screws at the top and bottom of the panel. See Figure 5-15.

Step 4 Press the ejector levers outward. This partially unseats the CPU transition module from the backplane connectors. See Figure 5-15.

Step 5 Pull the CPU transition module from the chassis by pressing the ejector levers outward and pulling the CPU transition module out. See Figure 5-15.

Installing the new CPU transition module

Step 1 Press the ejector levers outward. See Figure 5-16.

Step 2 Holding the CPU transition module by the ejector levers, partially insert the CPU transition module into the slot, about half way.

Step 3 Verify that the CPU transition module is properly seated in the guides on the top and bottom. If not, remove the CPU transition module and try again.

Step 4 Pushing gently and firmly on the CPU transition module's face plate, slide the CPU transition module into the slot until you encounter significant resistance. At this point, the ejector levers should be in contact with the chassis rails so they grab when pushed inward.

Step 5 Use the ejector levers to seat the CPU transition module in the slot by closing the ejector levers toward one another until they are in the locked position. See Figure 5-16.

Step 6 Secure the CPU transition module by tightening the captive screws at the top and bottom of the panel. See Figure 5-16.

Step 7 Verify that any empty slots have covers on them.

Warning **An empty slot that is uncovered can result in a destructive hardware failure.**

Step 8 Attach the power cable to the back of the server.

Step 9 Power up the server. Refer to the "Powering up the server" section on page 4-17.

Verifying the CPU card and transition module are properly seated

Step 1 Verify the CPU card's ejector levers are locked. If the LED on the bottom of the CPU card is blue, the CPU card is not locked. If the CPU card is not locked, reseat it.

Step 2 Verify the CPU transition module's levers are locked. If the LED on the bottom of the CPU card is blue, the CPU transition module is not locked. If the CPU transition module is not locked, reseat it.

Verifying the server's date and time

After replacing the CPU card or transition module, verify the server's date and time are correct.

Step 1 If not already connected, access the CLI by following the procedures in the "Connecting your laptop" section on page 4-1 and "Setting up your laptop" section on page 4-3.

Step 2 Login as a technician. The tech$ prompt appears.

Step 3 At the tech$ prompt, type **date** and press **Enter**. If the date and time are correct, go to the next step.

If the date and time are not correct, change them by following the procedure in the "Configuring the system" section on page 4-18.

Step 4 Test the installation by following the procedure in the "Testing the installation" section on page 4-95.

Checking the multi-server meeting configuration

After the CPU card or transition module has been replaced, you must check the system's multi-server meeting configuration.

Step 1 Log into MeetingTime as technician.

Step 2 Click the **Configure** tab and select **Other MeetingPlace Servers**.

Step 3 Click **Query**. See Figure 5-17.

Figure 5-17 MeetingTime Configure Tab Dialog Box

Step 4 If you see other MeetingPlace servers listed, you must update those servers with this server's new Ethernet address.

For all the servers you see listed under **Other MeetingPlace Servers**, you need to do the following:

a. Log into the server via MeetingTime.

b. Go to the **Configure** tab and select **Other MeetingPlace Servers**.

c. Click **Query** and continue clicking the forward arrow until you see the MeetingPlace server for which you just replaced the CPU card and transition module.

d. Change the Ethernet address to match the new CPU card and transition module and click **Save Changes**.

e. Exit MeetingTime.

Replacing the hot swap controller

This section provides instructions on how to replace a hot swap controller. The hot swap contoller is located in slot 10.

Warning **Handling the hot swap controller can result in static damage. Use an anti-static wrist strap, static-dissipating work surface, and anti-static bags when handling and storing the card.**

Note The hot swap controller card always goes into slot 10 in the front of the server. It also has a transition module in the slot 10 in the back of the server. Whenever the hot swap controller card is replaced, this transition module must also be replaced.

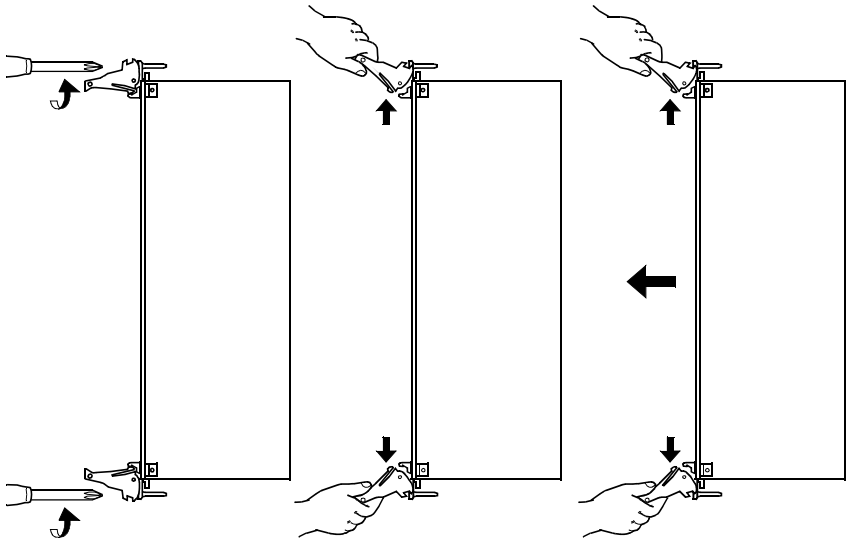
Removing the old hot swap controller card

Step 1 Verify all steps in the "Preparing for the repair" section on page 5-2 have been completed.

Step 2 Locate the hot swap controller card in slot 10 in the front of the server. See Figure 5-6.

Step 3 With a screwdriver, loosen the hot swap controller card's captive screws at the top and bottom of the panel. See Figure 5-19.

Figure 5-18 Removing the Hot Swap Controller Card and Transition Module



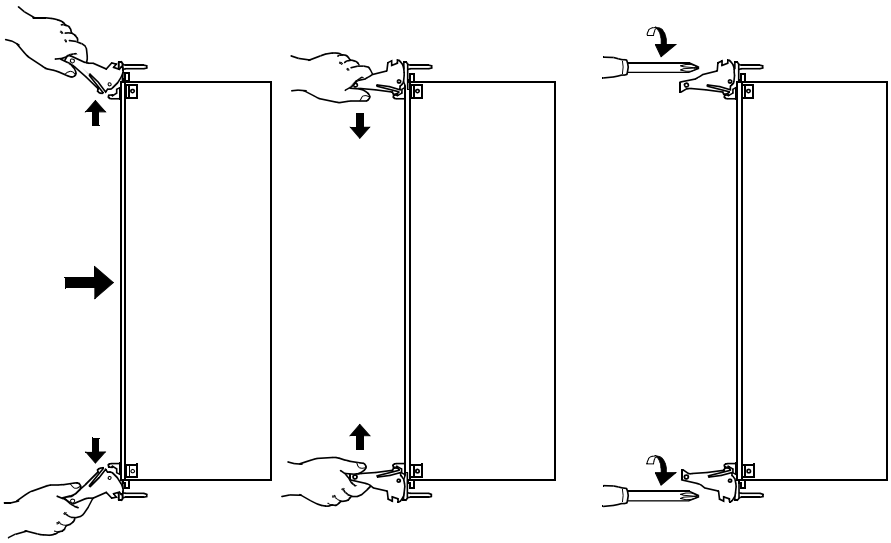
Step 4 Press the ejector levers outward. This partially unseats the hot swap controller card from the backplane connectors. See Figure 5-19.

Step 5 Pull the hot swap controller card from the chassis by pressing the ejector levers outward and pulling the CPU transition module out. See Figure 5-19.

Installing the new hot swap controller card

Step 1 Press the ejector levers outward. See Figure 5-16.

Figure 5-19 Installing the Hot Swap Controller Card and Transition Module



Step 2 Holding the hot swap controller card by the ejector levers, partially insert the hot swap controller card into the slot, about half way.

Step 3 Verify that the hot swap controller card is properly seated in the guides on the top and bottom. If not, remove the hot swap controller card and try again.

Step 4 Pushing gently and firmly on the hot swap controller card's face plate, slide the hot swap controller card into the slot until you encounter significant resistance. At this point, the ejector levers should be in contact with the chassis rails so they grab when pushed inward.

Step 5 Use the ejector levers to seat the hot swap controller card in the slot by closing the ejector levers toward one another until they are in the locked position. See Figure 5-19.

Step 6 Secure the hot swap controller card by tightening the captive screws at the top and bottom of the panel. See Figure 5-19.

Removing the old hot swap controller transition module

Step 1 Locate the hot swap controller transition module in slot 10 in the back of the server.

Step 2 Loosen the hot swap controller transition module's two captive screws at the top and bottom of the panel. See Figure 5-18.

Step 3 Press the ejector levers outward. This partially unseats the hot swap controller transition module from the backplane connectors. See Figure 5-18.

Step 4 Pull the hot swap controller transition module from the chassis by pressing the ejector levers outward and pulling the hot swap controller transition module out. See Figure 5-18.

Installing the new hot swap controller transition module

Step 1 Press the ejector levers outward. See Figure 5-19.

Step 2 Holding the hot swap controller transition module by the levers, partially insert it into the slot, about half way.

Step 3 Verify that the hot swap controller transition module is properly seated in the guides, top and bottom. If not, remove it and try again.

Step 4 Pushing gently and firmly on the hot swap controller transition module's face plate, slide it into the slot until you encounter significant resistance. At this point, the levers should be in contact with the chassis rails so they will grab when pushed inward.

Step 5 Use the ejector levers to seat the hot swap controller transition module in the slot by closing the levers toward one another until they are in the horizontal locked position. See Figure 5-19.

Step 6 Secure the hot swap controller transition module by tightening the captive screws at the top and bottom of the panel. See Figure 5-19.

Step 7 Verify that any empty slots have covers on them.

Warning **An empty slot that is uncovered can result in a destructive hardware failure.**

Step 8 Attach the power cable to the back of the server.

Step 9 Power up the server. Refer to the "Powering up the server" section on page 4-17.

Testing the hot swap controller

Step 1 Verify the hot swap controller card's ejector levers are locked. If the LED on the bottom of the hot swap controller card is blue, the hot swap controller card is not locked. If the hot swap controller card is not locked, reseat it.

Step 2 Verify the hot swap controller transition module's levers are locked. If the LED on the bottom of the hot swap controller card is blue, the hot swap controller transition module is not locked. If the hot swap controller transition module is not locked, reseat it.

Step 3 Test the installation by following the procedure in the "Testing the installation" section on page 4-95.

Replacing T1 Smart Blades or Smart Blades

This section provides instructions on how to replace a T1 Smart Blade or a Smart Blade card and transition module. The procedure for a T1 Smart Blade and a Smart Blade is the same.

Note "T1 Smart Blade" and "Smart Blade" are two different components with different functions, even though their names are similar.

Note Each T1 Smart Blade and Smart Blade card has a transition module in the same slot in the back of the server. Whenever a T1 Smart Blade or Smart Blade card is replaced, its corresponding transition module must also be replaced.

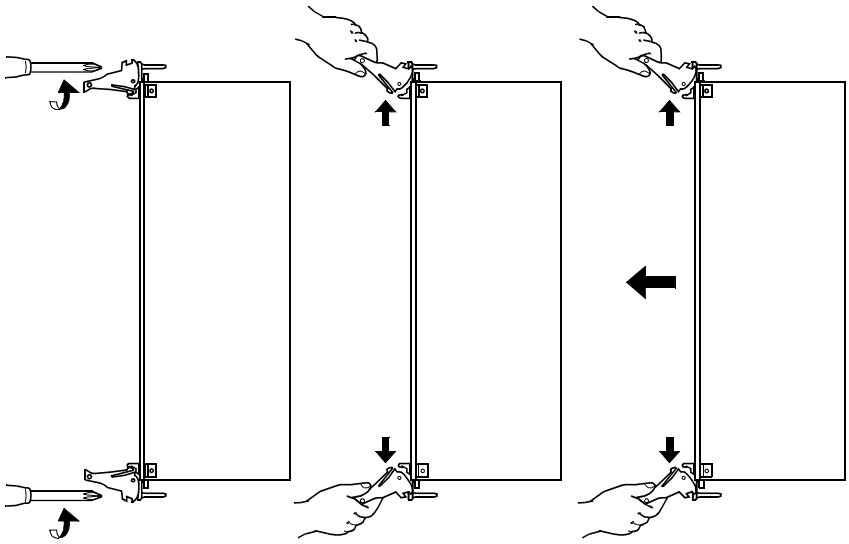
Warning **Handling these cards can result in static damage. Use an anti-static wrist strap, static-dissipating work surface, and anti-static bags when handling and storing these cards.**

Removing an old T1 Smart Blade or Smart Blade card

Step 1 Verify all steps in the section the "Preparing for the repair" section on page 5-2 have been completed.

Step 2 Verify which T1 Smart Blade or Smart Blade card needs replacing and loosen that card's two captive screws on the top and bottom of the panel. See Figure 5-20.

Figure 5-20 Removing a T1 Smart Blade Card and Transition Module



Step 3 Press the ejector levers outward. This partially unseats the T1 Smart Blade or Smart Blade card from the backplane connectors. See Figure 5-20.

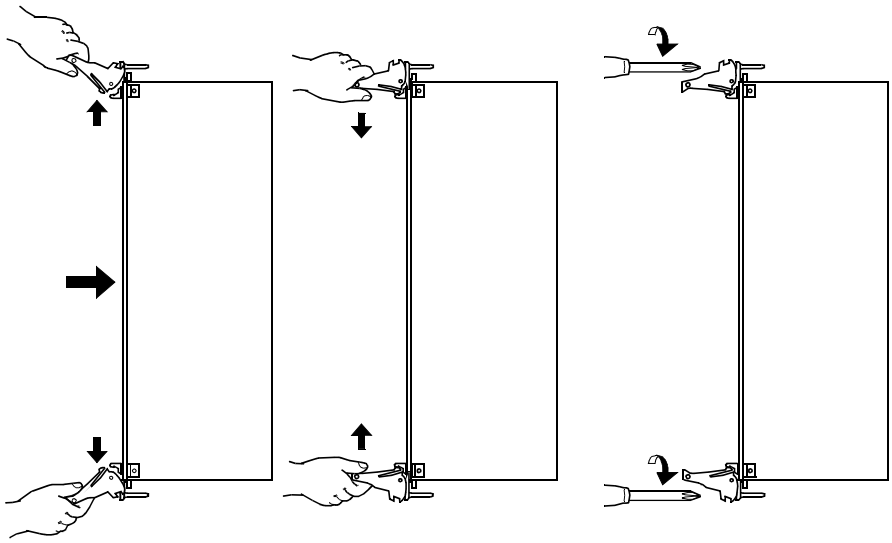
Step 4 Pull the T1 Smart Blade or Smart Blade card from the chassis by pressing the ejector levers outward and pulling the card out. See Figure 5-20.

Installing a new T1 Smart Blade or Smart Blade card

Step 1 Ensure that the system is powered down. If you are installing a new T1 Smart Blade or Smart Blade card immediately after removing an old one, the system should still be powered down. Otherwise, follow the steps in the "Preparing for the repair" section on page 5-2.

Step 2 Press the ejector levers outward. See Figure 5-21.

Figure 5-21 Installing a T1 Smart Blade Card and Transition Module



Step 3 Holding the T1 Smart Blade or Smart Blade card by the levers, partially insert the card into the slot, about half way.

Step 4 Verify that the T1 Smart Blade or Smart Blade card is properly seated in the guides, top and bottom. If not, remove the card and try again.

Step 5 Pushing gently and firmly on the T1 Smart Blade or Smart Blade card's face plate, slide the card into the slot until you encounter significant resistance. At this point, the levers should be in contact with the chassis rails so they will grab when pushed inward.

Step 6 Use the ejector levers to seat the T1 Smart Blade or Smart Blade card in the slot by closing the levers toward one another until they are in the horizontal locked position. See Figure 5-21.

Step 7 Secure the T1 Smart Blade or Smart Blade card by tightening the captive screws at the top and bottom of the panel. See Figure 5-21.

Removing an old T1 Smart Blade or Smart Blade transition module

Step 1 Locate the T1 Smart Blade or Smart Blade card's corresponding transition module in the back of the server.

Step 2 Loosen the T1 Smart Blade or Smart Blade transition module's two captive screws at the top and bottom of the panel. See Figure 5-20.

Step 3 Press the ejector levers outward. This partially unseats the T1 Smart Blade or Smart Blade transition module from the backplane connectors. See Figure 5-20.

Step 4 Pull the T1 Smart Blade or Smart Blade transition module from the chassis by pressing the ejector levers outward and pulling the transition module out. See Figure 5-20.

Installing a new T1 Smart Blade or Smart Blade transition module

Step 1 Ensure that the system is powered down. If you are installing a new T1 Smart Blade or Smart Blade transition module immediately after removing an old one, the system should still be powered down. Otherwise, follow the steps in the "Preparing for the repair" section on page 5-2.

Step 2 Press the ejector levers outward. See Figure 5-21.

Step 3 Holding the T1 Smart Blade or Smart Blade transition module by the levers, partially insert the transition module into the slot, about half way.

Step 4 Verify that the T1 Smart Blade or Smart Blade transition module is properly seated in the guides on the top and bottom. If not, remove the transition module and try again.

Step 5 Pushing gently and firmly on the T1 Smart Blade or Smart Blade transition module's face plate, slide the transition module into the slot until you encounter significant resistance. At this point, the levers should be in contact with the chassis rails so they will grab when pushed inward.

Step 6 Use the ejector levers to seat the T1 Smart Blade or Smart Blade transition module in the slot by closing the levers toward one another until they are in the horizontal locked position. See Figure 5-21.

Step 7 Secure the T1 Smart Blade or Smart Blade transition module by tightening the captive screws on the top and bottom of the panel. See Figure 5-21.

Step 8 Verify that any empty slots have covers on them.

Warning **An empty slot that is uncovered can result in a destructive hardware failure.**

Step 9 Attach the power cable to the back of the server.

Step 10 Power up the server. Refer to the "Powering up the server" section on page 4-17.

Testing a T1 Smart Blade or Smart Blade card and transition module

Step 1 Verify the T1 Smart Blade or Smart Blade card's ejector levers are locked. If the LED on the bottom of the card is blue, the card is not locked. If the card is not locked, see the "Powering down MeetingPlace" section on page 5-5 and reseat the card.

Step 2 Verify the T1 Smart Blade or Smart Blade transition module's ejector levers are locked. If the LED on the bottom of the T1 Smart Blade or Smart Blade card is blue, the transition module is not locked. If the transition module is not locked, see the "Powering down MeetingPlace" section on page 5-5 and reseat the transition module.

Step 3 Test the installation by following the procedure in the "Testing the installation" section on page 4-95.

Replacing a Multi Access Blade

This section provides instructions on how to replace a Multi Access Blade's card and transition module.

Warning **Handling these cards can result in static damage. Use an anti-static wrist strap, static-dissipating work surface, and anti-static bags when handling and storing these cards.**

Note Each Multi Access Blade card has a transition module in the same slot in the back of the server. Whenever a Multi Access Blade card is replaced, its corresponding transition module must also be replaced.

Removing an old Multi Access Blade card

Step 1 Verify all steps in the "Preparing for the repair" section on page 5-2 have been completed.

Step 2 Verify which Multi Access Blade card needs replacing. Locate the two red plastic latches on the top and bottom of the card within each black plastic handle.

Step 3 Press on both red latches and release them.

Step 4 Lift both of the black plastic handles to unseat the Multi Access Blade card.

Step 5 Gently pull the Multi Access Blade card out of the chassis.

Installing a new Multi Access Blade card

Step 1 Ensure that the system is powered down. If you are installing a new Multi Access Blade card immediately after removing an old one, the system should still be powered down. Otherwise, follow the steps in the "Preparing for the repair" section on page 5-2.

Step 2 Verify which slot number the new Multi Access Blade card is going into.

Step 3 Gently insert the Multi Access Blade card horizontally into the server's slot. As the card is inserted, the black plastic handles on the left and right of the card's front panel must engage with the chassis. When the card is firmly mounted into the correct position inside the chassis, the red plastic latches within each handle self-lock.

Step 4 Verify the black handles are in their locked position.

Removing an old Multi Access Blade transition module

Step 1 Verify all steps in the "Preparing for the repair" section on page 5-2 have been completed.

Step 2 Verify which Multi Access Blade transition module needs replacing. Locate the two red plastic latches on the top and bottom of the transition module within each black plastic handle.

Step 3 Press on both red latches and release them.

Step 4 Lift both black plastic handles to unseat the Multi Access Blade transition module.

Step 5 Gently pull the Multi Access Blade transition module out of the chassis.

Installing a new Multi Access Blade transition module

Step 1 Ensure that the system is powered down. If you are installing a new transition module immediately after removing an old one, the system should still be powered down. Otherwise, follow the steps in the "Preparing for the repair" section on page 5-2.

Step 2 Verify which slot number the new Multi Access Blade transition module is going into.

Step 3 Gently insert the Multi Access Blade transition module into the server's slot. As the transition module is inserted, the black plastic handles on the top and bottom of the transition module's panel must engage with the chassis. When the transition module is firmly mounted into the correct position inside the chassis, the red plastic latches within each handle self-lock.

Step 4 Verify the black handles are in their locked position.

Replacing the modem

This section provides instructions on how to replace the modem.

Note The modem is external and can be placed in the most safe and convenient place according to the rack arrangement. The location of the modem should be in a place where the cables are protected and cannot be pulled out of place.

For E1 and T1 PRI systems only, the modem sits inside the breakout box.

Removing the old modem

Step 1 Verify all steps in the "Preparing for the repair" section on page 5-2 have been completed.

Step 2 Turn the modem's power switch to the off position. The modem's power switch is on the side of the modem.

Step 3 Disconnect the modem cable from the COM 2 port on the CPU transition module. See the "Step 4Disconnect the RJ-11 connector from its source." section on page 5-34.

Figure 5-22 CPU Transition Module

Step 4 Disconnect the RJ-11 connector from its source.

Step 5 Disconnect the modem's power cable from the power outlet.

Step 6 Remove the modem and all of its cables from the location.

Installing the new modem

Refer to the "Installing and connecting the modem" section on page 3-40 for directions on how to install and connect the modem for both T1 CAS and T1 PRI/E1 systems.

Regular maintenance

This section explains the regular maintenance needed to keep the 8112 server up and running.

Replacing the power supply unit fan filter

The filter in the power supply unit fan needs to be replaced on a regular basis. The frequency of the replacement depends on how much dust is in the air. On average, the filter should be replaced once a year. To replace the power supply unit fan filter, refer to the "Replacing a power supply unit fan filter" section on page 5-14.

In addition, if any of the following alarms are seen, immediately check the power supply unit fan and its filter:

- 0x70034 (MAJOR) Temperature out of range
- 0x700BB (MINOR) Power supply fan N is failing
- 0x700C6 (MINOR) Power supply N cooling failure

Enabling server disk capacity monitoring (optional)

MeetingPlace Audio Server 5.2 provides the ability to monitor disk use. It raises an alarm when it reaches or exceeds a specified use threshold. To enable disk capacity monitoring, follow this procedure.

Step 1 If not already connected, access the CLI by following the procedures in the "Connecting your laptop" section on page 4-1 and "Setting up your laptop" section on page 4-3.

Step 2 Login as a technician. The tech$ prompt appears.

Step 3 Turn on terminal logging. For information on logging, see "Logging your HyperTerminal session" section on page 4-6.

Step 4 Type **configdiskcap** and press **Enter**. Figure 5-23 appears.

Figure 5-23 Using configdiskcap to Enable Disk Capacity Monitoring

```
meetingplace:tech$ configdiskcap
++++++++++++++++++++++++++++++++++
Disk Capacity Monitor Configuration
++++++++++++++++++++++++++++++++++
Capacity values are utilization percentage thresholds.
A major alarm will be raised if a threshold is exceeded.

Select a file system threshold to modify when prompted.

Values must be between 60 and 99; a capacity
of 0 disables checking for that file system.

   CAP% FILESYSTEM
   ==== ==========
1) 0    /
2) 0    /lat/db
3) 0    /tmp
4) 0    /lat/fs.1
5) 0    /lat/fs.2
6) 0    /lat/fs.3

Select an item to modify, s to save and exit,
or q to quit without saving:
```

Step 5 Type the number of the file whose use threshold capacity you want to modify and press **Enter**. In the example in Figure 5-24, we want to modify the use threshold capacity for the /lat/db file (file 2), so type **2** and press **Enter**.

Figure 5-24 Changing File System Capacity

```
Select an item to modify, s to save and exit,
or q to quit without saving: 2
enter new value for /lat/db: 95

   CAP% FILESYSTEM
   ==== ==========
1) 0    /
2) 95   /lat/db
3) 0    /tmp
4) 0    /lat/fs.1
5) 0    /lat/fs.2
6) 0    /lat/fs.3

Select an item to modify, s to save and exit,
or q to quit without saving: s
```

Step 6 Enter the new use threshold value for this file. In this example, we want to have the use threshold capacity be 95 percent, so type **95** and press **Enter**.

Step 7 Enter **s** and press **Enter** to save your changes and exit the "configdiskcap" command.

Troubleshooting

This chapter contains the following troubleshooting topics:

- system does not answer (see the "System does not answer" section on page 6-1)
- cannot outdial (see "Cannot outdial" section on page 6-7)
- LAN connectivity (see the "LAN connectivity" section on page 6-9)
- general (see the "General" section on page 6-10)

For details on troubleshooting the various MeetingPlace gateways, refer to the specific gateway's system manager's guide.

System does not answer

Troubleshooting this problem differs for the T1, E1, and IP ports.

T1 ports that do not answer

The troubleshooting technique for T1 CAS and T1 PRI is the same. Follow the procedure below for both types of configuration.

Step 1 Verify that the span is up using the "spanstat" command. See the "spanstat" section on page A-61 for more information. If the T1 trunks show no alarms:

a. Use "spanstat -ab" to verify that calls are being presented to the system. The AB bits change state when a caller dials into the system.

b. The PBX/Telco routing may not be set up correctly or trunks may be in a lockout state.

Step 2 Look for errors on the span using the "spanstat -s" command.

Step 3 Verify correct cabling (frequently reversed):

- pin 1 — MP Receive (tip), pin 2 — MP Receive (ring)
- pin 4 — MP Send (tip), pin 5 — MP Send (ring)

Step 4 Verify the configuration with the "span" command. See the "span" section on page A-59 for more information.

Step 5 Check the framing (ESF vs. D4) and coding (B8ZS vs. jammed bit).

E1 ports that do not answer

For E1 ports that do not answer, follow this procedure:

Step 1 Verify that the span is up using the "spanstat" command. See the "spanstat" section on page A-61 for more information. If the E1 trunks show no alarms:

a. The PBX/Telco routing may not be set up correctly or trunks may be in a lockout state.

b. Use "spanstat <span number> -all" to verify that calls are being presented to the system. The call state changes when a caller dials into the system.

A proper incoming call should follow the sequence:

– "ds" (incoming call) => "ii" (call active) => ".." (port idle)

A proper outgoing call should follow the sequence:

– "sd" (outgoing call) => "oo" (call active) => ".." (port idle)

Note If a "ds" => ".." or "sd" => ".." transition occurs quickly, this indicates that the near-end or far-end, respectively, is rejecting the call. Verify that the port is active on the MeetingPlace side (near-end) and the ISDN service is activated on the far-end. Contact the Cisco TAC for information on determining the ISDN cause code for the call rejection.

Note If a port stays in any of these states for more than ten seconds, this indicates a possible protocol problem where one side is not clearing down the telephone call all of the way ("do", "di", "od", "id"). If this is the case, contact the Cisco TAC to determine if ISDN messages are being lost.

Step 2 Look for errors on the span using the "spanstat -s" command.

Step 3 Verify correct cabling (frequently reversed):

pin 1 — MP Receive (tip), pin 2 — MP Receive (ring)
pin 4 — MP Send (tip), pin 5 — MP Send (ring)

Step 4 Verify the configuration with the "e1span" command. See the "e1span" section on page A-22 for more information.

Step 5 Check the framing and coding using the "protparm" and "e1span" commands. See the "protparm" section on page A-47 for more information.

Check the port group's protocol table

Verify that the port group for any troubled port references the correct protocol table for the ISDN protocol being interfaced to.

Step 1 At the tech$ prompt, type **port** and press **Enter**. The "port" command menu in Figure 6-1 appears.

Figure 6-1 port Command Menu

```
meetingplace:tech$ port

*****   P O R T / G R O U P   C O N F I G   M E N U   *****

        1)  View port record(s)
        2)  Modify port record
        3)  Copy port records
        4)  View group record(s)
        5)  Modify group record
        x)  Exit program

Enter command: 4
```

Step 2 Type **4** and press **Enter** to view the port group record. The second line in Figure 6-2 appears.

Figure 6-2 View Port Group

```
Enter command: 4
Enter port group record number [0..31, <cr> for all] : 0

------------     GROUP  0      --------------
  Activate the group?         :  y
  Card type                   :  E1
  Signaling                   :  Euro ISDN
  Protocol table              :  50
  Number of DID digits        :  0
  Human assistance?           :  n
  Flash transfer?             :  n
  Outdial?                    :  y

Enter command: x
```

Step 3 Type the appropriate port group number and press **Enter**. In this example, it is 0, so type **0** and press **Enter**. The rest of Figure 6-2 appears.

Step 4 Take note of the protocol table number. In this example, it is protocol table 50.

Step 5 Type **x** and press **Enter** to exit the "port" command utility.

Step 6 Type **protparm** and press **Enter**. Figure 6-3 appears.

Figure 6-3 protparm Command Menu

```
meetingplace:tech$ protparm

*****   P R O T P A R M   C O N F I G   M E N U   *****

        1)  View protocol parameter table(s)
        2)  Modify protocol parameter table
        3)  Copy protocol table
        4)  Delete protocol table(s)
        x)  Exit program

Enter command: 1
```

Step 7 Type **1** and press **Enter** to view the protocol parameter table. The second line in Figure 6-4 appears.

Figure 6-4 Protocol Table Menu

```
Enter command: 1
Enter protocol table number [0..99, <cr> for all] : 50

*****   V I E W   M E N U   *****

   1)  View entire table
   2)  View general information
   3)  View incoming called party number processing (DDI)
   4)  View incoming calling party number processing (CLI)
   5)  View outgoing calling party information
   6)  View outgoing called party type of number (TON)
   7)  View outgoing called party numbering plan (NPI)
   8)  View outgoing private number definition
   9)  View outgoing local number definition
   a)  View outgoing long distance number definition
   b)  View outgoing international number definition
   c)  View outgoing Network Specific Facilities (NSF) codes
   d)  View outgoing NSF Carrier Identification Code (CIC)
   x)  Exit to main menu

Enter list command [table 50]: 2
```

•

Step 8 Type the appropriate protocol table number found in Figure 6-2 and press **Enter**. In this example, it is 50, so type **50** and press **Enter**. The rest of Figure 6-4 appears.

Step 9 Type **2** and press **Enter** to view general information. A screen similar to Figure 6-5 appears.

Figure 6-5 Protocol Table Parameters

```
Enter list command [table 50]: 2

----------------- PROTOCOL TABLE  50 -----------
  Activate the table?             :  y
  Description                     : Euro-ISDN generic table for Europe
  Protocol                        :  Euro ISDN
  CAS signaling table filename    :  (none)
  Default clearing cause          :  16 (normal clearing)
  B-channel negotiation           :  exclusive
  Protocol side                   :  user

Enter list command [table 50]: 0
```

Step 10 Verify the protocol table has the correct parameters set. If it does not, change it as necessary by going to the main "protparm" utility menu (by typing **x** and pressing **Enter**) and selecting the modify protocol parameter table option (by typing **2** and pressing **Enter**).

Note Protocol tables 0-49 are read-only and cannot be modified. If you need to make changes to one of these tables, you need to copy one of the read-only tables and then modify your copy.

Step 11 Type **x** and press **Enter** to exit the "protparm" utility.

IP ports that do not answer

For IP ports that do not answer (for example, the caller hears a busy or fast busy sound), follow the procedure below. For information on troubleshooting problems with the MeetingPlace IP Gateway, refer to the *MeetingPlace IP Gateway System Manager's Guide*.

Things to check on the MeetingPlace Audio Server

Step 1 Make sure the server has IP ports configured and active using the "blade" and "portstat" commands.

Step 2 Log into the CLI and at the tech$ prompt, type **tvportstat -all** and press **Enter**.

Step 3 Monitor the output of this command while you make a test call. Verify the incoming call is seen by the server.

Step 4 Type **cptrace -T 5** and press **Enter**.

Step 5 Monitor the output of this command while you make another test call. Verify the incoming call is seen by the server.

Step 6 Type **errorlog -s info -l** and press **Enter**. Scroll through the log by typing **f** and check for warnings and alarms, especially those that happen in the cpiphandler.cc file. To exit out of this command, type **q**.

Step 7 Type **gwstatus** and press **Enter** to verify that the Gateway SIM and IP Gateway services have a status of "Ok".

Things to check on the MeetingPlace IP Gateway

Step 1 At the tech$ prompt, type **gwstatus** and press **Enter** to verify that the Gateway SIM and IP Gateway services have a status of "Ok".

Step 2 Verify that the MeetingPlace IP Gateway configuration has the appropriate call control enabled (either H.323 or SIP).

Step 3 Open the Gateway SIM eventlog and make a test call.

Step 4 While looking at the Gateway SIM eventlog, verify the test call is received by the MeetingPlace IP Gateway and that the IP server is returning a response code of 0 such as:

Step 5 MP Resp. Msg=3 CPerr=0 SeqNum=0x16

Step 6 Verify that no softphones such as Microsoft NetMeeting are running on the IP Gateway.

Step 7 If MeetingPlace Web is on the same machine, be sure that MeetingPlace Web and the MeetingPlace IP Gateway are assigned to different IP addresses.

Things to check on the Cisco Call Manager

Step 1 Verify an H.323 gateway has been created for the IP Gateway and that a route pattern has been assigned to the IP Gateway.

Step 2 Verify the Cisco Call Manager server can "ping" the MeetingPlace IP Gateway and vice versa.

IP calls connect but no audio is heard

Follow this procedure when the IP call connects but no audio is heard.

Things to check on the MeetingPlace Audio Server

Step 1 Verify the subnet mask address is correct using the "blade" command. If it is not, MeetingPlace cannot send voice packets to the phone. You must use the "restart" command to restart the system for any changes to take effect.

Step 2 Type **tvportstat -all** and press **Enter**.

Step 3 While monitoring the output of this command, make a test call to verify the IP call is seen by the server.

Step 4 Type **cptrace -T 5** and press **Enter**.

Step 5 While monitoring the output of this command, make a test call to verify the IP call is seen by the server.

Step 6 Type **tvportstat <port # used in tests above> -s** and press **Enter**. Look at "RTCP packets sent by far end" to verify that the phone is transmitting voice data to MeetingPlace. If so, at least you know there is a one-way connection.

Things to check on the MeetingPlace IP Gateway

Step 1 Open the Gateway SIM eventlog and verify the log entries below have the correct IP addresses for each Multi Access Blade used for the IP configuration:

- MP RTP info. IP=10.10.10.1 Port=5010
- MP RTCP info. IP=10.10.10.2 Port=5011

Step 2 Still looking at the Gateway SIM eventlog, verify the log entries below have the IP phone's correct IP address:

- Remote RTP info. IP=10.10.10.3 Port=6510
- Remote RTCP info. IP=10.10.10.4 Port=6511

Step 3 Use the "ping" command to ping the IP addresses of all Multi Access Blades used for the IP configuration and the address of the IP phone to verify both are reachable.

Things to check on the IP phone

Step 1 Press the blue "i" button quickly twice.

Step 2 Verify the phone is receiving and sending packets (RxCnt and TxCnt).

Step 3 Verify the expected codec has been negotiated (RxType and TxType).

Cannot outdial

Troubleshooting this problem differs for T1/E1 ports and IP ports.

Note If the server is using a translation table, this table may be preventing the outdialing. Verify the translation table contains the necessary numbering plans to allow for outdialing. In a mixed system (that is, one with both and IP configuration and either an E1, T1 PRI, or T1 CAS configuration), the translation table must contain numbering plans for both configurations. If you are unfamiliar with altering translation tables, contact the Cisco TAC.

Cannot outdial on T1 or E1 ports

When you are unable to outdial from a T1 or E1 port, follow this procedure:

Step 1 Verify that the port and port group are configured for outdial using the "port" command. See the "port" section on page A-44 for more information. Type **port** and press **Enter**. Type **1** and press **Enter** to view the port records. Type the number of the port you want to see and press **Enter**. In this example, it is all, so press **Enter** to see the records for all ports. Look for the outdial parameter and ensure it is set to "y" for all ports.

Step 2 Verify that the trunks on the PBX are configured to allow outdialing.

Step 3 Schedule a meeting and use the #3 feature to hear if there is an error tone from the PBX.

Cannot outdial on IP ports

When you are unable to outdial from an IP port, follow this procedure:

Things to check on the MeetingPlace Audio Server

Step 1 Verify incoming calls to the server are connecting. If not, follow the procedure in the "IP ports that do not answer" section on page 6-5.

Step 2 Verify the port group is enabled for outgoing calls using the "port" command.

Step 3 Check the translation table to verify IP calls are being directed to a port group configured for IP. (Use the "xltest" command to check which port group is used for the dialed number.) This is especially important for mixed systems (those with both IP and either E1, T1 PRI, or T1 CAS configurations).

Step 4 At the tech$ prompt, type **cptrace -T 5** and press **Enter**.

Step 5 While monitoring the output of this command, make a test outdial to see why the outdial fails.

Step 6 Type **errorlog -s info -l** and press **Enter**. Scroll through the log by typing **f** and check for warnings and alarms, especially those that happen in the cpiphandler.cc and cpplacecall.cc files. To exit out of this command, type **q**.

Step 7 Type **activity** and press **Enter**.

Step 8 Type **4** and press **Enter** to make a test call. Test both internal extensions and outside numbers to try to isolate the problem.

Things to check on the MeetingPlace IP Gateway

Step 1 Open the Gateway SIM eventlog and verify the IP Gateway receives the outdial command from the server.

Step 2 Still looking at the Gateway SIM eventlog, verify the correct phone number was received by the IP Gateway.

MeetingPlace IP outdial. Phone=651515 IRC=0 PSTN=46 Unit=0

Step 3 In the MeetingPlace IP Gateway configuration, verify the outdial is sent using the appropriate protocol.

Step 4 In the MeetingPlace IP Gateway configuration, verify the gateway, gatekeeper, and proxy server addresses and ports are correct according to the desired protocol.

Step 5 In the MeetingPlace IP Gateway configuration, verify the E.164 address and H.323 ID fields are correct for H.323 outdials. Verify that display name, user name and session name are correct for SIP outdials.

Things to check on the Cisco Call Manager

Step 1 If the MeetingPlace IP Gateway resides on a gateway with multiple IP addresses, verify that the Cisco Call Manager has an H.323 Gateway configuration for each IP address.

Step 2 Verify the gateway settings created for the MeetingPlace IP Gateway allow outdials.

Things to check on the IP phone

Verify the IP phone can place a direct call to the requested outdialed number.

LAN connectivity

If users cannot connect to the system using MeetingTime, follow this procedure:

Step 1 Use the "ping" command to determine if the network can access the server. See the "ping" section on page A-43 for more information.

Step 2 Use the "ping" command to ping a known good IP address on the network.

Step 3 Verify with the Network Administrator that MeetingPlace has been set up in the local host file or is set up on the Domain Name Server (DNS).

Step 4 Try connecting with an IP address rather than the host name.

If the above steps do not resolve the problem, try these:

Step 1 Check the network cabling.

Step 2 If possible, use a PC to check the LAN connectivity.

Step 3 Verify the network configuration with the "net" command. See the "net" section on page A-38 for more information.

Step 4 Verify the IP address, subnet mask, and default gateway values.

General

If the above list of troubleshooting topics does not apply to the problem, follow these steps:

- Make sure all cards and transition modules are seated properly.
- Check all cables and connections.
- Verify card configuration with the “blade”, “dcard”, and “span” commands. Refer to the “blade” section on page A-8, “dcard” section on page A-18, and “span” section on page A-59 for more information.
- Verify port configuration with the “port” command. Refer to the “port” section on page A-44 for more information.
- Check the error log with the “errorlog” command. Refer to the “errorlog” section on page A-24 for more information.

Installing a Shadow Server

MeetingPlace Audio Server 5.2 allows for shadow server capability in the 8112 environment. The 8112 shadow server is a backup system that can replace the 8112 conference server in case there is a system or site failure. The switchover of the shadow server ensures that complete MeetingPlace functionality can be returned with a minimum loss of time and disruption in service.

Note The 8112 shadow server system behavior is different than the PCI shadow server. There is database replication, but there is no automatic fail-over mechanism.

Note In the following sections, the term "primary server" refers to the server that is used on a day-to-day basis. The term "shadow server" refers to the backup server that replicates the database from the primary server.

The following sections discuss how to install and configure the shadow server and how to switch from the primary server to the shadow server:

- Verifying requirements. Refer to the "Verifying requirements" section on page 7-2.
- Obtaining necessary information. Refer to the "Obtaining the necessary information" section on page 7-2.
- Physically installing the shadow server. Refer to the "Physically installing the shadow server" section on page 7-2.
- Checking the licenses on the shadow server. Refer to the"Checking the licenses on the shadow server" section on page 7-3.
- Configuring the primary server. Refer to the "Configuring the primary server" section on page 7-4.
- Preparing to configure the shadow server. Refer to the "Preparing to configure the shadow server" section on page 7-7.
- Configuring the shadow server while in standalone mode. Refer to the "Configuring the shadow server while in standalone mode" section on page 7-10.
- Restarting the shadow server. Refer to the "Restarting the shadow server" section on page 7-12.

Verifying requirements

Before beginning any work with the shadow server, verify each requirement below. Also, refer to the *MeetingPlace Audio Server 5.2 System Manager's Guide* for a complete list of requirements.

- MeetingPlace server requirements:
  - The primary server must be running MeetingPlace Audio Server version 5.1 or higher.
  - The shadow server must be running MeetingPlace Audio Server version 5.1 or higher with a clean database.
- License requirements:
  - Each shadow server must have a shadow server license.
- Network requirements:
  - All TCP ports need to be open between the primary server and the shadow server.
  - UDP and ICMP ports can be blocked, but IP ports need to be open.
- System up/down requirements:
  - The primary server must have a scheduled restart one time to configure the shadow server.

Obtaining the necessary information

Fill in the "Value" columns in Table 7-1 and Table 7-2. You need this information before installing the shadow server.

Table 7-1 Primary Server Network Information

Information Needed	Value
IP address	
host name	

Table 7-2 Shadow Server Network Information

Information Needed	Value
IP address	
host name	
ethernet address	
default gateway address	
subnet mask address	
IP address of NTP servers	

Physically installing the shadow server

Before physically installing the shadow server, confirm that all requirements have been met by referring to the *MeetingPlace Audio Server 5.2 System Manager's Guide*.

Physically installing the shadow server is the same as physically installing the primary server. Table 7-3 lists the steps involved with installing the shadow server.

Table 7-3 Sections to be Completed from Chapters 3 and 4

X	Section Title and Page
	"Unpacking the 8112 server" section on page 3-10
	"Unpacking the 8112 server" section on page 3-10
	"Connecting the system cables" section on page 3-18
	"Connecting your laptop" section on page 4-1
	"Setting up your laptop" section on page 4-3
	"Powering up the server" section on page 4-17

Checking the licenses on the shadow server

The shadow server needs to have, at a minimum, the same license keys as the primary server. The steps below show you how to verify the license keys.

Step 1 Verify the items in Table 7-3 have been completed and that you are connected to the shadow server.

Step 2 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 3 Log in as a super user. At the tech$ prompt, type **su** and press **Enter** and then enter the password of the day and press **Enter**. If you do not know the password, contact the Cisco TAC.

Step 4 At the su$ prompt, type **om -c** and press **Enter**.

This outputs the list of licenses, similar to Figure 7-1. You need to run this same command on the primary server and compare the output.

If the shadow server does not have the same licenses as the primary server, do not proceed. Contact the Cisco TAC.

Figure 7-1 Example of om -c Command

```
meetingplace:csc$ om -c
avail (erc )  name           versn  ocount  xdate      sdate      ecode
1152  (0   )  accessports    1.000  1152    01-jan-00  01-jan-00  E020407148BF2B2B1218
1     (0   )  calendar       1.000  1       01-jan-00  01-jan-00  4060307132CF3B6F8BCF
1152  (0   )  confports      1.000  1152    01-jan-00  01-jan-00  A030D0D1B6E5506A4E31
1152  (0   )  dataconf       1.000  1152    01-jan-00  01-jan-00  B0D0F081EE68D032F3D4
1     (0   )  directory      1.000  1       01-jan-00  01-jan-00  7070F0311B9D735C392C
0     (0   )  exchg dataconf 1.000  0       01-jan-00  01-jan-00  C0706061E6FB23E88C3D
1     (0   )  fax            1.000  1       01-jan-00  01-jan-00  40C000E1CFC36D27B34D
2     (0   )  flexmenus      1.000  2       01-jan-00  01-jan-00  6030F041291617D58FF3
4     (0   )  languages      1.000  4       01-jan-00  01-jan-00  5010F0B18D6D2064DD07
1152  (0   )  mndata         1.000  1152    01-jan-00  01-jan-00  E020C03113B2AE45FA21
1     (0   )  msmail         1.000  1       01-jan-00  01-jan-00  00D0F0E156B4DE3A521F
0     (0   )  multiunit      1.000  0       01-jan-00  01-jan-00  7030D06123620CCDEFF2
4     (0   )  netmgt         1.000  4       01-jan-00  01-jan-00  10B030317DB69CB553E5
1     (0   )  notes calendar 1.000  1       01-jan-00  01-jan-00  B0B030A1511C4394F52E
1152  (0   )  notification   1.000  1152    01-jan-00  01-jan-00  20D0C00160E54739B783
1152  (0   )  recording      1.000  1152    01-jan-00  01-jan-00  B01000319AF57C3E767D
1     (0   )  sametime       1.000  1       01-jan-00  01-jan-00  6070504132A7B0D34AD9
1     (0   )  shadow         1.000  1       01-jan-00  01-jan-00  0020300157B29FAC4B23
1     (0   )  smtp           1.000  1       01-jan-00  01-jan-00  00407041A02A61098DC7
1152  (0   )  voting         1.000  1152    01-jan-00  01-jan-00  00E0309147D19CA84A17
2     (0   )  web            1.000  2       01-jan-00  01-jan-00  507000F1173F84D91619
200   (0   )  workstations   1.000  200     01-jan-00  01-jan-00  309090E10C840031B759
```

Configuring the primary server

This section explains how to configure the primary server.

Note The primary server must be configured before the shadow server is configured.

Using the "net" command

Step 1 If not already connected, access the command line interface (CLI) by following the procedures in the "Connecting your laptop" section on page 4-1 and the "Setting up your laptop" section on page 4-3.

Note CLI commands are case sensitive. For CLI command information, refer to Appendix A, "CLI Reference".

Step 2 Log in as technician. The tech$ prompt appears.

Step 3 If you do not already have terminal logging turned on, turn it on before proceeding. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 4 At the tech$ prompt, type **net** and press **Enter**. The first six lines in Figure 7-2 appear. The last line prompts you to enter a selection.

Figure 7-2 net Command Menu

```
meetingplace:csc$ net
 1) View the server & site configuration
 2) Modify the server configuration
 3) Select another server (current unit = #0)
99) Quit
Select: 3
Unit: 9
 1) View the server & site configuration
 2) Modify the server configuration
 3) Select another server (current unit = #9)
99) Quit
Select: 2
```

Step 5 Type **3** and press **Enter** to select another server. The seventh line in Figure 7-2 appears prompting you to enter a unit number.

Step 6 Type **9** to select unit 9 and press **Enter**. The last five lines in Figure 7-2 appear.

Step 7 Type **2** and press **Enter** to modify the server configuration.

Step 8 If unit 9 is currently inactive (which it should be) you are asked if you want to make it active. Type **y** and press **Enter** to make it active. See Figure 7-3.

Figure 7-3 Modifying Unit 9

```
You have selected a new configuration for this unit.
Unit class = SHADOW
Site class = REMOTE
Update the initialization file (y/[n])? y
DONE
NOTE: Changes take effect with the next restart of the unit.
Unit class = SHADOW/REMOTE
```

Step 9 Select options **3**, **4**, **5**, and **6** consecutively and enter the appropriate data collected from Table 7-2 by following the prompts.

If you do not want to change a specific value, simply press **Enter** and nothing is changed.

Step 10 If the shadow server is located at a different site, type **2** and press **Enter** to select a different site for the shadow server.

Step 11 Once you have confirmed that the shadow server is set to active, type **99** and press **Enter** to return to the main "net" command menu. A screen similar to the first 14 lines of Figure 7-4 appears.

Figure 7-4 net Command Confirmation

```
Select: 99
Current server configuration:
    Unit:                  #9 (vp9)
    Active:                YES
    Description:           Shadow Server
    Kind:                  Shadow server
    IP Address:            10.10.10.10
    Ethernet address:      0001bc0211b8
    Site:                  #0 (Home Site)
    Site subnet mask:      255.255.255.0
    Site broadcast addr:   0.0.0.0
    Site default gateway:  10.10.10.1
    Route daemon:          disabled
Do you wish to commit these changes (y/n)? y
 1) View the server & site configuration
 2) Modify the server configuration
 3) Select another server (current unit = #9)
99) Quit
Select: 99
```

Step 12 Confirm the settings shown here match what you have listed in Table 7-2.

Step 13 If the settings do not match, type **n** and press **Enter** and repeat the necessary steps of the procedure entering the correct data.

If the settings do match, type **y** and press **Enter** to commit to and save the changes. The last five lines of Figure 7-4 appear.

Step 14 Type **99** and press **Enter** to exit the "net" utility.

Using MeetingTime to attach the shadow server

Follow these steps to attach the shadow server.

Step 1 Using MeetingTime, log into the primary server.

Step 2 Go to the **Configure** tab and select **Usage Parameters** from the left pane.

Step 3 Click **Query**. Values appear in the right pane.

Step 4 Scroll to the **Network Shadow Svr** section about half way down.

Step 5 Change the value for **Shadow attached?** from "No" to "Yes".

Step 6 Click **Save Changes** in the bottom right corner.

Step 7 Log out and close MeetingTime.

Restarting the primary server

The primary server must be restarted at this point. This restart should have been previously scheduled with the customer.

Step 1 If not already connected, access the command line interface (CLI) by following the procedures in the "Connecting your laptop" section on page 4-1 and Figure 4-2.

Step 2 Log in as technician. The tech$ prompt appears.

Step 3 Type **restart enable** and press **Enter**. The system prompts you to verify you really want to restart the server.

Step 4 Type **y** and press **Enter** to confirm. The primary server restarts.

Backing up the primary server's database

The primary server's database should be backed up at this point.

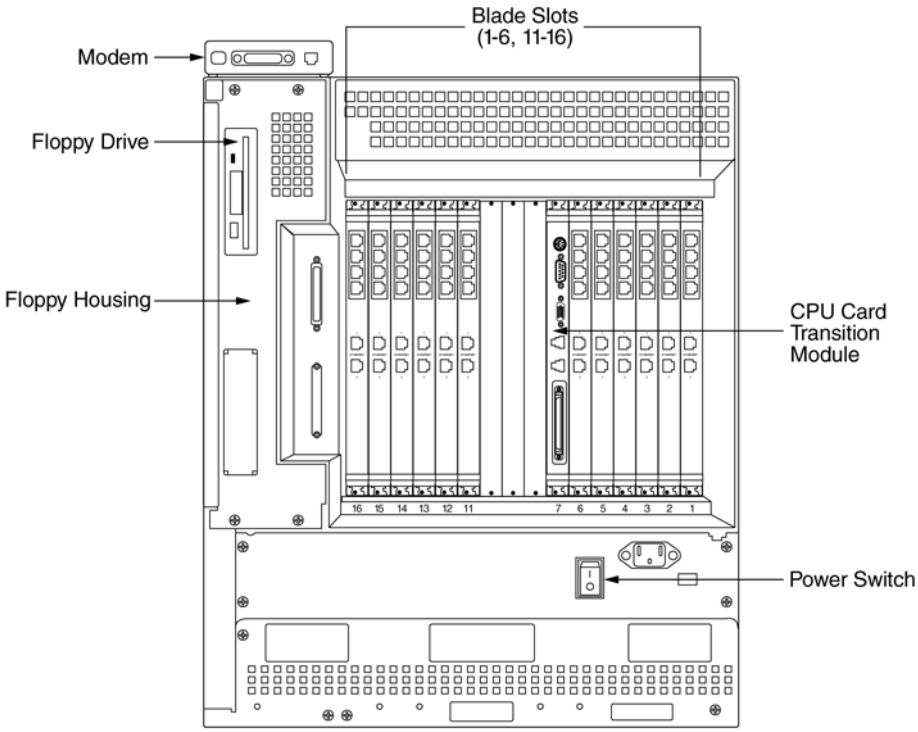
The backup mechanism has changed in this version of MeetingPlace Audio Server. It is now done through the MeetingPlace Backup Gateway. For information on how to install, configure, and use the backup gateway, refer to the *MeetingPlace Backup Gateway System Manager's Guide*.

Preparing to configure the shadow server

This section explains the steps necessary before the shadow server can be configured.

Step 1 Power on the shadow server by flipping the power switch to the on ("|") position. The power switch is located on the back of the server in the bottom left corner. See Figure 7-5.

Figure 7-5 Back of 8112 Server



Step 2 If not already connected, access the command line interface (CLI) by following the procedures in the "Connecting your laptop" section on page 4-1 and "Setting up your laptop" section on page 4-3.

Step 3 Log in as technician. The tech$ prompt appears.

Step 4 Start logging your terminal session. For information on logging, see the "Logging your HyperTerminal session" section on page 4-6.

Step 5 At the tech$ prompt, type **swstatus** and press **Enter**.

Confirm that the shadow server is configured as a conference server as shown in line two of Figure 7-6. If it is not, contact the Cisco TAC.

Figure 7-6 swstatus Command Screen

```
meetingplace:tech$ swstatus
Conference server 5.2.0   S/N: M00002    Latitude Comm.
System status: Operating
System mode: Up
Temperature: 30
Power supply: OK

MODULE NAME          STATUS     VERSION
SIM                  UP         "11/14/02 20:08 MPBUILD-rel520"
LSH                  UP         "11/14/02 18:53 MPBUILD-rel520"
SNMPD                UP         "11/14/02 20:33 MPBUILD-rel520"
DBQSERVER            UP         "11/14/02 19:13 MPBUILD-rel520"
DBSERVER             UP         "11/14/02 19:13 MPBUILD-rel520"
POSERVER             UP         "11/14/02 19:43 MPBUILD-rel520"
CPSERVER             UP         "11/14/02 19:40 MPBUILD-rel520"
CONFSCHED            UP         "11/14/02 19:58 MPBUILD-rel520"
WSSERVER             UP         "11/14/02 20:09 MPBUILD-rel520"
VOICESERVER          UP         "11/14/02 20:28 MPBUILD-rel520"
GWSIMMGR             UP         "11/14/02 20:41 MPBUILD-rel520"

UNIT SITE  STATUS    RUN LEVEL  UNIT KIND   LAST ATTACH
  10    0  OK        UP         GATEWAY     11/23/02 04:38:08
  11    0  OK        UP         GATEWAY     11/23/02 04:37:38
  12    0  OK        UP         GATEWAY     11/25/02 12:25:26
  13    0  OK        UP         GATEWAY     11/21/02 19:41:28
  14    0  OK        UP         GATEWAY     11/23/02 04:37:19
```

Step 6 At the tech$ prompt, type **down disable** and press **Enter**.

Step 7 Once the system is down, insert a disk into the floppy drive. The floppy drive is located on the back of the server. See Figure 7-5.

Step 8 At the tech$ prompt, type **savelicense** and press **Enter**.

Step 9 Once the "savelicense" command is finished, remove the disk from the floppy drive by pressing the eject button and removing the disk.

Step 10 Locate the backup you performed on the primary server in the "Backing up the primary server's database" section on page 7-7.

Step 11 Restore the backup by typing **restore** and pressing **Enter**.

Note The "restore" command restores the primary server's database to the shadow server. This may take a while depending on the size of the database.

Step 12 Once the restore is complete, insert the disk described in Step 7 above into the floppy drive.

Step 13 At the tech$ prompt, type **update** and press **Enter**.

Step 14 Once the update is complete, remove the disk from the floppy drive by pressing the eject button and removing the disk.

Configuring the shadow server while in standalone mode

Before configuring the shadow server as a shadow server, the following items must be configured:

- telephony configuration. Refer to the "Configuring the system" section on page 4-18.
- LAN parameters. Refer to the "Configuring the LAN parameters" section on page 4-19.
- MeetingTime telephony access parameters. Refer to the "Telephony and LAN parameters configuration" section on page 7-10.
- MeetingTime max recording space. Refer to the "MeetingTime server configuration" section on page 7-10.
- MeetingTime server configuration. Refer to the "MeetingTime server configuration" section on page 7-10.
- necessary languages. Refer to the "Languages confirmation" section on page 7-11.
- gateway routing. Refer to the "Gateway routing" section on page 7-11.

Telephony and LAN parameters configuration

Step 1 Run the "net" and "blade" commands to configure the telephony and LAN parameters. Use the information in Table 7-2.

For more information about these commands, refer to Appendix A, "CLI Reference".

Note When configuring the shadow server's LAN parameters, it is configured locally as unit 0.

Step 2 Once the telephony and LAN configuration is complete, the system must be restarted. At the tech$ prompt, type **restart** and press **Enter**.

MeetingTime server configuration

Step 1 Once the system is back up, log into MeetingTime and go to the **Configure** tab.

Note All MeetingTime values are replicated to the shadow server via the restore that was done. All values that are different between the primary server and the shadow server need to be manually configured in MeetingTime.

Step 2 Select **Telephony Access** from the left pane and click **Query**. Values appear in the right pane.

Step 3 Verify the main telephone number and any other applicable parameters. Change them as needed. Depending on the configuration, these values may be the same or different from the primary server's values.

Step 4 Click **Save Changes** in the bottom right corner.

Step 5 Click **Server Configuration** in the left pane.

Step 6 Click **Query** and values appear in the right pane.

Step 7 Verify that all values are accurate.

Step 8 Verify the **Max Recording Space (min.)** field is set appropriately for the current configuration.

Languages confirmation

Verify that all languages installed on the primary server are also installed on the shadow server.

Gateway routing

How you configure the gateway routing depends if you have a set of backup gateway machines.

- *With* a set of backup gateway machines. The gateways must be installed and connected before bringing the shadow server online configured as a shadow server. The backup gateways need to be set up and connected while the shadow server is in standalone server mode. Refer to the appropriate *MeetingPlace Audio Server 5.2 System Manager's Guide* for gateway installation procedures.

  When the system is converted to a shadow server, the gateways are down attempting to connect to the server. Once the shadow server is brought into service as the primary server, the gateways reconnect.

- *Without* a set of backup gateway machines. The customer must correctly configure his network such that if the primary server goes down, the TCP requests are re-routed to the shadow server.

Other considerations

- FlexMenus. If the primary server is configured with FlexMenus, the shadow server must also be configured with FlexMenus before converting the system to a shadow server.
- Custom prompts. If the primary server is configured with custom prompts, the shadow server must also be configured with custom prompts before converting the system to a shadow server.
- Translation tables. The translation tables for the primary server are not replicated. You need to configure the translation table on the shadow server to match the primary server as needed. However, the translation tables may be different, especially if the shadow server is in a different location.

Restarting the shadow server

At this point, you must restart the shadow server.

Step 1 If not already connected, access the command line interface (CLI) by following the procedures in the "Connecting your laptop" section on page 4-1 and "Setting up your laptop" section on page 4-3.

Step 2 Log in as technician. The tech$ prompt appears.

Step 3 At the tech$ prompt, type **restart enable** and press **Enter**.

Step 4 Type **y** and press **Enter** to confirm that you want to restart the system.

Verifying shadow server configuration while in standalone mode

The following steps must be done while the shadow server is still in standalone server mode.

Step 1 Confirm the shadow server functionality by completing the steps in the "Testing the installation" section on page 4-95.

Step 2 Verify that you can log into MeetingTime.

Step 3 Verify all gateway functionality and connectivity. Refer to the appropriate gateway system manager's guide for more information.

Changing the shadow server to act as a shadow server

This section explains how to change the shadow server's setup from standalone mode to shadow server mode.

Note If the "net" command is run at any point after the "setup" command, the setup configuration is overwritten and must be redone.

Step 1 If not already connected, access the command line interface (CLI) by following the procedures in the "Connecting your laptop" section on page 4-1 and "Setting up your laptop" section on page 4-3.

Step 2 Log in as technician. The tech$ prompt appears.

Step 3 At the tech$ prompt, type **down** and press **Enter**.

Step 4 Type **y** and press **Enter** to confirm that you want to bring down the system.

Step 5 Once the system is down, type **setup** and press **Enter**. The first ten lines of "" on page <$chapnum13 appear.

Figure 7-7 setup Command for the Shadow Server

```
meetingplace:tech$ setup
This program determines the basic personality of this unit.
Current unit class = SINGLE
Current site class = LOCAL

Select the unit class:
 1) MeetingPlace -- Standalone (SINGLE).
 5) Shadow Network Server (SHADOW).
99) Quit.
Select: 5
You will now be prompted for host name and IP address of the primary
server.
This information is used to establish the network connection.  Please,
when prompted for a host name, enter a proper Internet host name, with
no spaces or funny characters, not the IP address.

Host name of the primary server []:
```

Step 6 Type **5** and press **Enter** to select shadow network server.

Step 7 The system prompts you to enter the server's host name. Be sure to enter the proper Internet host name with no spaces, not the IP address.

Step 8 Continue following the prompts to enter the other necessary information.

Note At the end of the setup, you see an indication that the site class is "REMOTE" as in Figure 7-7. This is always the case, even if the shadow server is located at the same site as the primary server.

Step 9 Type **y** and press **Enter** to update the initialization file as in line four of Figure 7-8.

Figure 7-8 Setting the Shadow Server's Class

```
You have selected a new configuration for this unit.
Unit class = SHADOW
Site class = REMOTE
Update the initialization file (y/[n])? y
DONE
NOTE: Changes take effect with the next restart of the unit.
Unit class = SHADOW/REMOTE
```

Step 10 At the tech$ prompt, type **restart enable** and press **Enter** to bring the server back up.

Post-configuration steps

Step 1 If not already connected, access the primary server's CLI by following the procedures in the "Connecting your laptop" section on page 4-1 and "Setting up your laptop" section on page 4-3.

Step 2 Log in as technician. The tech$ prompt appears.

Step 3 Type **swstatus** and press **Enter**.

Step 4 Verify that the shadow server, unit 9, is connected.

Step 5 If not already connected, access the shadow server's CLI by following the procedures in the "Connecting your laptop" section on page 4-1 and "Setting up your laptop" section on page 4-3.

Step 6 Type **swstatus** and press **Enter**.

Step 7 Verify that it is connected to the primary server, unit 0.

Step 8 Wait at least 15 minutes.

Step 9 If there are meetings taking place on the primary server, log onto the shadow server via the CLI, then type **cptrace** and press **Enter**.

If the data is replicating properly, you will see data being logged from the call traces. If there is nothing in the trace, contact the Cisco TAC.

Step 10 Type **q** and press **Enter** to exit the "cptrace" utility.

Step 11 At the tech$ prompt, type **alarm** and press **Enter**.

Step 12 Make a note of any alarms.

Step 13 Clear the alarms by typing **clearalarm all** and pressing **Enter**.

Step 14 At the tech$ prompt, type **date** and press **Enter**. Confirm that the date and time are correct.

Note While the shadow server is operating in shadow server mode, the telephony interfaces are not active. A connected PBX sees a red T1 alarm on all spans.

Testing the switchover

This section explains how to test the switchover to ensure that the data is replicating correctly.

Note Allow a few hours to pass before testing the switchover.

Running MeetingTime reports

Step 1 Log into MeetingTime on the primary server.

Step 2 Go to the **Report** tab and select **Raw Meeting Details** in the left pane.

Step 3 Click **Execute**.

Step 4 Once the report is finished, save it to a convenient location.

Step 5 Select **Raw Profile Information** in the left pane.

Step 6 Click **Execute**.

Step 7 Once the report is finished, save it in a convenient location.

Step 8 Exit MeetingTime.

Shutting down the primary server

Step 1 If not already connected, access the primary server's CLI by following the procedures in the "Connecting your laptop" section on page 4-1 and "Setting up your laptop" section on page 4-3.

Step 2 Log in as technician. The tech$ prompt appears.

Step 3 Type **down disable** and press **Enter**.

Step 4 Type **y** and press **Enter** to confirm that you want to shut down the system.

Switching shadow server to primary server

Step 1 If not already connected, access the shadow server's CLI by following the procedures in the "Connecting your laptop" section on page 4-1 and "Setting up your laptop" section on page 4-3.

Step 2 Log in as technician. The tech$ prompt appears.

Step 3 Type **setup** and press **Enter**.

Step 4 Type **1** and press **Enter** to select "MeetingPlace -- Standalone (SINGLE)".

Step 5 Once the setup has been changed, type **restart enable** and press **Enter**.

Step 6 Complete the steps in Table 7-4.

Table 7-4 Post-switchover Tasks

X	Task
	Compare the Raw Meeting Details Report from the "Running MeetingTime reports" section on page 7-14 to the newly configured primary server's (original shadow server) information to be sure it is replicating.
	Compare the Raw Profile Information Report from the "Running MeetingTime reports" section on page 7-14 to the newly configured primary server's (original shadow server) information to be sure it is replicating.
	At the CLI, type **gwstatus** and press **Enter** to confirm the gateways have reconnected.

Table 7-4 Post-switchover Tasks

X	Task
	At the CLI, type **spanstat -s** and press **Enter** to confirm the spans are up.
	Log into MeetingTime to confirm you can connect.

Changing the shadow server back to shadow server mode

After completing the test switchover, the shadow server must be reconfigured as a shadow server.

Step 1 If not already connected, access the shadow server's CLI by following the procedures in the "Connecting your laptop" section on page 4-1 and the "Setting up your laptop" section on page 4-3.

Step 2 Log in as technician. The tech$ prompt appears.

Step 3 Type **down** and press **Enter**.

Step 4 Type **y** and press **Enter** to confirm that you want to bring the system down.

Step 5 Once the server is down, type **setup** and press **Enter**.

Step 6 Type **5** and press **Enter** to select shadow server mode.

Step 7 Enter the necessary information as you are prompted.

Step 8 Once the setup is complete, type **restart enable** and press **Enter**.

Note If the "net" command is run at any point after the "setup" command, the "setup" configuration is overwritten and must be redone.

Bringing the primary server back online

Step 1 If not already connected, access the primary server's CLI by following the procedures in the "Connecting your laptop" section on page 4-1 and "Setting up your laptop" section on page 4-3.

Step 2 Log in as technician. The tech$ prompt appears.

Step 3 Type **restart enable** and press **Enter**.

Step 4 Once the system is back up, type **swstatus** and press **Enter**.

Step 5 Confirm that the shadow server, unit 9, has reconnected.

Step 6 Log into the shadow server via the CLI.

Step 7 Type **swstatus** and press **Enter**.

Step 8 Confirm that the shadow server shows itself as being connected to the primary server, unit 0.

Step 9 Wait at least 15 minutes.

Step 10 If there are meetings taking place on the primary server, log onto the shadow server via the CLI.

Step 11 Type **cptrace** and press **Enter**. If the data is replicating properly, you see data being logged from the call traces. If there is nothing in the trace, contact the Cisco TAC.

Step 12 Type **q** and press **Enter** to exit the "cptrace" utility.

CLI Reference

This appendix contains information about the command line interface (CLI) technician commands. It is organized into the following sections:

- online help
- short description of technician commands
- detailed description of technician commands

Online help

When you are logged into MeetingPlace via a telnet session, you can see a list of most technician commands in Table A-1 by typing **help** and pressing **Enter**.

To look up information about a specific command:

Step 1 Type **help** followed by the command name and press **Enter**. The command description is presented one screen at a time.

Step 2 To just see the next line, type **1** and press **Enter**. To see more lines, type a larger number and press **Enter**. Larger numbers cause more lines to appear.

To see the next screen, press the space bar. If the amount of text displayed has a problem, use the resize command. At the end of the file, `(END)` appears.

Step 3 To return to the tech$ prompt, press **q**. You do not need to press **Enter**.

Short description of technician commands

This section provides a short explanation for the CLI commands available to the technician profile.

Table A-1 Short Description of Technician Commands

Command	Page	Short Description
activity	page 4	shows a summary of port activity
alarm	page 6	shows the contents of the system alarm table
alarmtest	page 7	generates a test alarm condition

Table A-1 Short Description of Technician Commands (continued)

Command	Page	Short Description
blade	page 8	configures all T1, E1, and IP ports
clear	page 10	clears the screen
clearalarm	page 11	clears the contents of the alarm table
configdiskcap	page 12	configures the file system threshold capacity
cptrace	page 13	lists the call processing trace log
date	page 15	shows or sets the system's date and time
dbsize	page 17	shows the number of database records
dcard	page 18	views or modifies a Smart Blade beyond the capabilities of the "blade" command
down	page 19	shuts down MeetingPlace leaving the CLI active
downblade	page 20	brings down a blade
e1card	page 21	views or modifies a Multi-Access Blade record
e1span	page 22	views or modifies an E1 span record
errorlog	page 24	lists the exception log
exc	page 26	prints information about an exception code
exit	page 27	logs out of the system
getether	page 28	shows the server's Ethernet address
gwcptrace	page 29	displays the GWSIM eventlog
gwstatus	page 30	displays the status of all connected MeetingPlace gateways and their services
halt	page 31	shuts down and halts MeetingPlace
help	page 32	prints help information
hwconfig	page 33	displays the current hardware configuration
license	page 35	shows copyright and license information
mtgconflicts	page 36	reports any meeting ID conflicts when you turn on reservationless meetings
mtgmode	page 37	configures meeting scheduling mode
net	page 37	views or modifies the network configuration
ntpstatus	page 40	shows the status of the Network Time Protocol
passwd	page 42	changes the technician's password
ping	page 43	tests network connectivity
port	page 44	views or modifies a port or port group record
portstat	page 46	shows the current port active and inactive status, the port group assignment, and port and card mapping
protparm	page 47	views or modifies the protocol parameter table

Table A-1 Short Description of Technician Commands (continued)

Command	Page	Short Description
recover	page 48	fixes corrupted database structures and forces database and voice file system consistency
release	page 49	shows the software release number
resize	page 50	resets the terminal settings to your screen size
restart	page 51	shuts down and reboots MeetingPlace
restore	page 52	restores the database from tape
revert	page 53	activates the previous configuration
save	page 54	saves the current configuration
savelicense	page 55	saves the software license keys to a floppy
setipcodec	page 56	sets IP codec configuration
setsn	page 56	sets or displays the system's serial number
setup	page 58	sets the basic server configuration
span	page 59	views or modifies a T1 CAS span record
spanstat	page 61	views the status of T1 or E1 spans
swcheck	page 62	verifies the software file checksums
swstatus	page 63	shows the software status
timezone	page 64	sets the system local time zone
tvportstat	page 65	views the status of IP ports
update	page 65	runs a software update
updatedbsize	page 68	updates the database size

Detailed description of technician commands

The section gives a detailed description of each command listed in Table A-1. The commands may have the following sub-sections:

- Summary: a brief summary of the command
- Description: a more detailed description of the command
- Syntax: shows the syntax for the command
- Options: a list of the available options
- Notes: additional information about the command
- Restrictions: restrictions for using this command
- See also: a reference to other information

activity

Summary

The "activity" command shows a summary of port activity.

Description

The "activity" command shows the current status of each port and active conference on the system. It can also generate calls for testing trunk interfaces.

Options

1) Quick Status of all Ports — lists all the ports in summary form, with a two character application code for each port. A "`--`" code means the port is not in use. Type **l** and press **Enter** to see a legend of the other possible codes.

2) Verbose Status of Port Range — prompts for a range of port numbers and prints one line for each, showing the session number (for internal use only), the port number, the application running on that port (shows "`IDLE`" if not in use), the name of the user (if known), and the conference number if a caller is in a meeting. The conference number can be used as input to the "cptrace" command (with the -C option) if trace information is desired.

3) Display complete Port Information — prompts for a port number and displays information about the status of that port. Intended for engineering use only.

4) Make Test Call — allows a technician to test a port or range of ports by placing outgoing calls. You are prompted for a phone number, which should normally be a phone you can answer. You are then asked if you want to specify a particular port or range of ports. For questions ending with "`(t -- f)`", type **t** and press **Enter** for yes or type **f** and press **Enter** for no. The system places a call on the indicated ports. If successful, the phone rings and you are prompted to enter "**1**". The system then prints out what it sees.

5) Show All Confs — displays information about the active conferences in the system.

0) Quit — exits the "activity" command.

Note The acronym "VUI" stands for "Voice User Interface". This refers to the software module that manages the voice interface at a high level. The "activity" command prints out some of the internal tables kept by the VUI module.

Note When the "activity" command is executed, it first prints out the system configuration, indicating how many sessions and conferences are configured. The session count refers to the number of access ports. The conference count is always 120.

Note The "activity" command deals with ports rather than trunks. To understand the correspondence between trunks and ports, you need to use the "blade", "dcard", and "span" commands.

SEE ALSO

- "blade" section on page A-8
- "dcard" section on page A-18
- "span" section on page A-59

- "spanstat" section on page A-61
- "cptrace" section on page A-13

alarm

Summary

The “alarm” command lists the contents of the system alarm table.

Description

The “alarm” command lists the contents of the system alarm table. Each entry has two lines. The first line has several columns:

- **REFNO** — a reference number used when clearing the alarm. See the “clearalarm” command.
- **SEV** — severity of the alarm: “`MIN`” is minor and “`MAJ`” is major.
- **CODE** — exception code. When reporting an alarm, be sure to include this code.
- **COUNT** — a count of occurrences of this condition since the alarm table was last cleared.
- **FIRST** — date and time of the first occurrence since the alarm table was last cleared.
- **LAST** — date and time of the most recent occurrence.
- **SW MODULE**— used for software faults.
- **DEV** — used for hardware faults.
- **UNIT** — used for hardware faults.
- **PORT** — used for hardware faults.

  The second line is a text description of the alarm.

SEE ALSO

- “clearalarm” section on page A-11
- “errorlog” section on page A-24
- “swstatus” section on page A-63

alarmtest

Summary

The “alarmtest” command generates a test alarm condition.

Description

The “alarmtest” command generates a false minor alarm for the purpose of testing the alarm table, LEDs, and alarm outdial.

Note When testing the alarm outdial, be aware that the system will not generate an outdial until at least 30 minutes has passed since the previous alarm outdial. This is true even if the alarm table is cleared between alarms.

SEE ALSO

- “alarm” section on page A-6
- “clearalarm” section on page A-11

blade

Summary

The “blade” command configures the T1 Smart Blades, Smart Blades, and Multi Access Blades.

Description

The “blade” command configures all T1, E1, and IP ports. It can configure the ports for you automatically, or it can be run in interactive mode allowing you more flexibility.

Options

If you type **blade** and press **Enter**, the following menu appears:

- **1) View blade details** — prompts the user to enter a blade number and then displays the details of that blade.
- **2) Modify blade** — prompts the user for a blade slot number and then displays every parameter one line at a time. To change a value, enter the new value and press **Enter**. To keep the value as is, press **Enter** without entering a new value.
- **x) Exit program** — exits the “blade” command.

Syntax DescriptionS

You can configure all the blades in one command using the following syntax:

blade [-i <n>] [-t <m>] [-e <x>] [-r <y>]

- **blade -i <n>** — configures <n> IP ports in default settings starting from sysport 0.
- **blade -t <n>** — configures <n> T1 CAS ports in default settings starting from sysport 0.
- **blade -i <n> -t <m>** — configures <n> IP ports and <m> T1 CAS ports in default settings with T1 CAS starting at sysport 0, then IP ports follow.
- **blade -p <n>** — configures <n> T1 PRI ports in default settings starting from sysport 0.
- **blade -i <n> -p <m>** — configures <n> IP ports and <m> T1 PRI ports starting from sysport 0.
- **blade -e <n>** — configures <n> E1 ports in default settings starting from sysport 0.
- **blade -i <n> -e <m>** — configures <n> IP ports and <m> E1 ports in default settings with E1 starting from sysport 0, then IP ports follow.
- **blade -t <n> -r <m>** — configures <n> T1 CAS ports and reserves slot <m> for later use. Multiple slots may be reserved by stringing together several -r options with each -r specifying a different slot number.
- **blade -e <n> -r <m>** — configures <n> E1 ports and reserves slot <m> for later use. Multiple slots may be reserved by stringing together several -r options with each -r specifying a different slot number.
- **blade -p <n> -r <m>** — configures <n> T1 PRI ports and reserves slot <m> for later use. Multiple slots may be reserved by stringing together several -r options with each -r specifying a different slot number.
- **blade -i <n> -r <m>** — configures <n> IP ports and reserves slot <m> for later use. Multiple slots may be reserved by stringing together several -r options with each -r specifying a different slot number.

EXAMPLeS

To configure a 96 port IP and 96 port T1 system, the command is:

blade –i96 –t96

To configure a 96 port IP and 96 port E1 system, the command is:

blade -i96 -e96

To configure a 96 port T1 system, while reserving slots 1 and 2 for later provisioning, the command is:

blade -t96 -r1 -r2

clear

Summary

The “clear” command clears the screen.

Description

The “clear” command simply clears the screen of your terminal.

SEE ALSO

- “resize” section on page A-50

clearalarm

Summary

The “clearalarm” command clears the contents of the alarm table.

Description

This command clears the alarm table.

Syntax DescriptionS

This command can be used in two ways:

- **clearalarm <reference number>** — allows you to clear one alarm at a time. The reference number is listed by the alarm command.
- **clearalarm all** — clears the entire alarm table.

SEE ALSO

- “alarm” section on page A-6

configdiskcap

Summary

The “configdiskcap” command configures the disk capacity monitoring for MeetingPlace.

Description

This command views or changes the disk capacity monitoring configuration for the MeetingPlace server. This information is used by the system to monitor disk use and raise an alarm when a specified utilization threshold has been exceeded.

After you type **configdiskcap** and press **Enter**, the system presents a list of file systems and their thresholds. Choose one and enter a new threshold value. The new value must be between 60 and 99; a value of 0 disables threshold checking for that file system.

cptrace

Summary

The “cptrace” command lists the call processing trace log.

Description

The “cptrace” command lists selected portions of the call processing trace log. Generally, it is used to find out what was going on when some anomalous condition occurred. Information in the log includes every input (incoming calls, DTMF tones, call progress tones, disconnect indications, etc.) and every high-level action taken for each voice call into the system.

By default, the “cptrace” command lists events associated with the voice user interface (VUI) module, which is concerned with ordinary call and voice processing events. However, if the -C option flag is specified, the “cptrace” command lists events associated with the conference scheduler module, which is concerned with scheduling plus events associated with a conference.

For each event listed, the output shows the date and time, accurate to 10 milliseconds, plus the port or conference number (if assigned), the class of event, and an event-specific tag showing what happened. Event classes include:

- Action — An action taken by the system. The tag is the name of the action.
- Applicat — The caller has entered a new application area. The tag is the name of the application.
- Input — Some input (tone or other event) has been detected.
- Timeout — There has been no activity for some period of time. After a few timeouts, the system disconnects the call.
- Outdial — The system is dialing out on a port. The tag indicates the numeric user ID associated with the call, a return code indicating success or failure, plus the phone numbers dialed before and after being processed through the digit translation table.

In addition, the following apply if the -C option is specified:

- Blast OD — An automated outdial, where the system dials out to bring participants into the system.
- Delete — Shows deletion of the specified conference from the active conference list.
- Purged — The conference record has been purged from the system.
- ReSched — A meeting has been rescheduled.
- Schedule — Scheduling of a new meeting.

At the end of each screen page, the “cptrace” command pauses and displays a colon. Press **Enter** to see one more line or press the space bar to see a new page. Type **q** and press **Enter** to stop the command.

Options

The “cptrace” command can be used with the following options:

- **cptrace -b <time>** — restricts output to events occurring after the specified time and date. The time parameter is in the same format as accepted by the “date” command.
- **cptrace -c** — only lists events associated with the specified conference number. This is applicable only when used with the -C option.
- **cptrace -C** — lists information from the conference scheduler log rather than from the VUI log.
- **cptrace -e <time>** — restricts output to events occurring before the specified time and date. The time parameter is in the same format as accepted by the “date” command.

- **cptrace -f** — lists events in forward time order.
- **cptrace -h** — displays the syntax for the command.
- **cptrace -p** — only lists the events associated with the specified port number.
- **cptrace -r** — lists the events in reverse time order. This is the default unless the -f, -t, or -b options are used.
- **cptrace -t** — lists the most recent events in the log and continues listing new events as they are entered into the log. Use <CTRL><C> to stop the command.
- **cptrace -T <number 0-5> option** — lists the low-level call processing specifics.
- **cptrace -v** — lists more information than the default. This is primarily for use in engineering.
- **cptrace -V** — lists the link date and software release number from when the command was built.

Note Port numbers are visible using the "activity" command or through the in-session screens on MeetingTime. Conference numbers are unique identifiers, not the same as the meeting indentifiers shown in MeetingTime. They are visible during the meeting by using the "activity" command. The call processing log takes up 5 MB on the system disk. This is enough space for approximately a million events, or approximately 10,000 calls.

Note Events are flushed to the log files in batches. On an idle system, it is possible for the last log entries to remain in memory, and not available for display, indefinitely. To force the last entries to disk, place a new call into the system.

Note The "eventlog" command displays the same information as the "cptrace" command, but does so in log form. The "eventlog -T 5" command displays ISDN tracing accumulated, assuming layer 2 and 3 tracing has been activated via the "acsetrace" command. The "eventlog" command can only be run while logged on as a super user.

SEE ALSO

- "errorlog" section on page A-24
- "date" section on page A-15
- "activity" section on page A-4

date

Summary

The “date” command lists or sets the system’s date and time.

Description

The “date” command lists or sets the system’s date and time.

Options

The “date” command can be used in three ways:

- **date** — displays the current date, time, and abbreviated time zone.
- **date <new date and time>** — with a new date as a parameter, sets the system’s date and time.
- **date -u** — uses GMT instead of the local time.

To set a new date, type **date** followed by a space and then type a date or time in any of the following formats, and then press **Enter**:

- yyyymmddhhmm — year (all four digits), month, day, hour, minute
- yymmddhhmm — year (last two digits), month, day, hour, minute
- mmddhhmm — month, day, hour, minute
- ddhhmm — day, hour, minute
- hhmm — hour, minute

The month, day, hour, and minute values are all two digits, with a zero prefix for values less than 10. For the year, you can either use all four digits of the year (for example, “1998”) or just the last two digits (for example, “02” for the year 2002). The hour is in 24-hour format (00-23). You can append seconds to any format by adding a period and two digits (for example “.34” means 34 seconds).

It is vital that the system’s time zone be set correctly before using the “date” command to set the time. Prior to setting the time, use the “date” command to list the current time and time zone. If the time zone is not correct, use the “timezone” command before setting the time. The date and time is set in the factory before the system is shipped. Normally, the time does not drift more than a few minutes a month, so any correction should be only a few minutes. If the time is off by more than 10 minutes, please consult the Cisco TAC prior to adjusting the time.

Warning **Setting the time incorrectly results in undesired system behavior. All meeting scheduling will be off. If the time is set ahead of the current time, meetings scheduled to occur in the meantime are lost.**

examples

- **date 0102271501.36** — sets the date to February 27, 2001 at 3:01:36 PM
- **date 0202270001** — sets the date to February 27, 2001 at 12:01 AM
- **date 1501** — sets the time to 3:01 PM today

Restrictions

The system must be shut down prior to setting the date or time. To shut the system down, use the “down” command. When finished, restart the system with the “restart” command.

SEE ALSO

- "down" section on page A-19
- "restart" section on page A-51
- "timezone" section on page A-64

dbsize

Summary

The “dbsize” command shows the number of database records. It is used during the PCI to 8112 server conversion procedure to verify that the database is empty. It is also used to estimate the conversion time and verify that the database migrated correctly. It is also used to verify the correct number of meetings or profiles were imported during a meeting or profile import.

Description

The “dbsize” command shows the number of database records in the following categories:

- user profiles
- groups
- conferences
- conference participants
- conference time records
- conference notifications
- conference category records
- conference attachments
- team lists
- team list members
- meeting number reservations
- voice space reservations

An example of the output from the “dbsize” command is shown in Figure A-1.

Figure A-1 dbsize Command Output

```
meetingplace:tech$ dbsize
User profiles:                          1235
Groups:                                   27
Conferences:                           13540
Conference participants:               80345
Conference time records:              130766
Conference notifications:              19818
Conference category records:           17987
Conference attachments:                  680
Team lists:                               33
Team list members:                       134
Meeting number reservations:           13132
Voice space reservations:                126
```

dcard

Summary

The “dcard” command is used to view or modify a Smart Blade beyond the capabilities of the “blade” command.

Description

The “dcard” command is used to configure a Smart Blade in the database in situations where the “blade” command does not fit the needs of the configuration.

Options

After typing **dcard** and pressing **Enter**, you see the following menu:

- **1) View DTI card record(s)** — prompts the user to select a specific card or all cards. The system then prints whether the card is active, the number of spans, and the record number of each span.
- **2) Modify DTI card record** — prompts the user to select a specific card and then prompts the user for whether the card should be activated, how many spans are attached, and record number for each span.
- **3) Set encoding type** — sets the encoding type.
- **x) Exit program** — exits the “dcard” utility command.

Note The install procedure will not operate if the drive does not have a proper MeetingPlace key.

Note Spans are numbered 0-47. Each DTI card can handle four spans, labeled A, B, C, and D.

Note The assignment of ports to trunks within a span is performed using the “span” command. The individual port records are configured through the “port” command or through the MeetingTime Configure tab. In MeetingTime, note that the port record references the DTI card and span records for that port. It is important that the card, span, and port records be consistent within the database, cross-referencing accurately.

Note Changes made by the “dcard” command take effect only after the next system restart.

SEE ALSO

- “blade” section on page A-8
- “port” section on page A-44
- “span” section on page A-59
- “restart” section on page A-51

down

Summary

The “down” command shuts down MeetingPlace for maintenance.

Description

The “down” command performs an orderly shut down of the MeetingPlace application, logging everyone off the system except technicians using the CLI. This is necessary before performing some maintenance operations. To return the system to the normal state, use the “restart” command.

Options

The “down” command can be used in three ways:

- **down courtesy** — allows users up to 5 minutes to quit before the system shuts down.
- **down disable** — prevents the system from coming back online after a restart. This allows a technician to reboot the system multiple times during a maintenance procedure.
- **down** — prompts you to verify that you really want to bring the system down and then brings the system down. The system comes back online after a system restart.

Note To bring the system back online, you must use the “restart” or “halt” command with the enable option (i.e., “restart enable”, “halt enable”).

SEE ALSO

- “halt” section on page A-31
- “restart” section on page A-51

downblade

Summary

The “downblade” command brings down the PRC or MSC functionality of a Smart Blade.

Syntax DescriptionS

downblade -b <blade number> [options]

Options

The “downblade” command options include:

- **-p** — brings down the PRC only, giving a courtesy message first
- **-m** — brings down the MSC only, giving a courtesy message first

The default is that both the PRC and MSC are brought down after giving a courtesy message. If only the PRC or PMSC is affected (for example, a specific DSP failure), you can choose to only disable the PRC or MSC component.

Note The “downblade” command brings down the PRC or MSC functionality of a Smart Blade. The effects of the “downblade” command are not reversible. Once the PRC or MSC has been brought down, the only way to restore it is to restart the server.

Note Also, the effect of the “downblade” command does not persist over a restart. To have the blade continue to be down after the system restarts, you must invoke the “downblade” command again after the system restarts.

e1card

Summary

The "e1card" command allows you to view or modify a Multi Access Blade record for E1 and T1 PRI systems.

Description

The "e1card" command configures a Multi Access Blade in the database. This command allows a technician to view or set whether the blade is supposed to be active, the type of signaling used and the configuration specifics, the number of spans attached to the blade, and which span attaches to each line on the blade.

Options

This command has the following menu:

1) View ACTI card record(s) — prompts the user to select a specific blade or all blades. The system then prints whether the blade is active, the number of spans attached to the blade, the signaling type, the configuration specifics for the signaling type, and the record number of each span connected to a line on the blade.

2) Modify ACTI card record — prompts the user to select a specific blade. The user is then prompted for whether the blade should be activated, how many spans are attached to it, the signaling type and its corresponding configuration string, and the record number for each span connected to each line on the blade.

x) Exit program — exits the "e1card" utility.

Note The assignment of ports to trunks within a span is pre-formed using the "e1span" command. The individual port records are configured through the "blade" command or through the MeetingTime **Configure** tab. In MeetingTime, note that the port record references the Multi Access Blade and span records for that port. It is important that the blade, span, and port records be consistent within the database, cross-referencing accurately.

Note Changes made by the "e1card" command take effect only after the next system restart.

SEE ALSO

- "e1span" section on page A-22
- "restart" section on page A-51
- "protparm" section on page A-47

e1span

Summary

The “e1span” command allows you to view or modify a span record for E1 and T1 PRI systems.

Description

The “e1span” command is used to view or modify an E1 or T1 PRI span record in the database. This tells the system whether the span should be active, various characteristics of the span, and the mapping between trunks and internal port numbers.

The following characteristics are set by the “e1span” command:

- Timing external or internal. This determines whether the span is permitted to supply trunk timing for the system. Specify external if the span is connected to the public network or a trusted system. At least one span should always be designated external.
- External sync priority. A number (1-255) or never. This controls the priority (1 is highest, 255 is slowest) of the spans that are set for external timing. The system picks the highest priority operational span to provide timing. If two spans have the same priority, the lowered numbered span wins.

Options

After typing **e1span** and pressing **Enter**, the following menu appears:

- 1) View ACTI span record(s) — prompts the user to select a specific span or all spans. The system then prints whether the span is active, the characteristics of the span, and the port number for each trunk.
- 2) Modify ACTI span record — prompts the user to select a specific span. The user is then prompted for whether the span should be activated, the characteristics of the span, and the port number assignment for each trunk.
- x) Exit — exits the “e1span” utility command.

Note E1 spans are numbered 0-31. Trunks on a span are numbered 1-30. Ports are numbered for the number of licensed access ports minus 1. There are up to 16 span records for each Multi Access Blade. The span record is referenced by both parameters set using the “e1card” command and parameters set using the “blade” command. It is important to be sure that these references are consistent. If a port is referenced in a span record, the corresponding port record must reference that span.

Note If the Multi Access Blade is not active, then the 16 spans will not operate even if they are set to active in the span record.

Note Changes to a span record will only take effect after the next system restart.

SEE ALSO

- “e1card” section on page A-21
- “blade” section on page A-8
- “protparm” section on page A-47

- "spanstat" section on page A-61
- "restart" section on page A-51

errorlog

Summary

The “errorlog” command lists the system exception log.

Description

The “errorlog” command lists the contents of the system exception log. By default, entries are listed in reverse chronological order, starting from the present. The output lists the date and time of the exception (accurate to the nearest second), the exception code, and a text description of the exception. Additional information is provided if the -l option is selected.

At the end of each screen page, the “errorlog” command pauses and displays a colon. Press **Enter** to see one more line or the space bar to see a new page. Type **q** to stop the command.

Options

The “errorlog” command can be used with the following options:

- **errorlog -b <time>** — restrict output to exceptions occurring after the specified time and date. The time parameter is in the same format as accepted by the “date” command.
- **errorlog -e <time>** — restricts output to exceptions occurring before the specified time and date. The time parameter is in the same format as accepted by the “date” command.
- **errorlog -f** — lists the log in forward time order.
- **errorlog -h** — displays the syntax of the command.
- **errorlog -l** — lists the log in a more verbose manner. The output switches to a two-line format for each entry, with the text string on the second line and more information on the first line. This information includes the numeric code of the reporting software module, the name of the software source file where the exception was reported, the line number within that source file, and the four supplementary arguments passed to the exception logger. Normally, this is of interest only to Cisco personnel.
- **errorlog -r** — lists the log in reverse time order. This is the default except when the -f, -t, or -b flags are used.
- **errorlog -s** — specifies the minimum severity level of exceptions to be listed. The severity levels are info, warning, minor, and major. Use info to see everything in the log. At a minimum, you need to specify the first two letters of the severity desired (“in” for “info”). By default, only minor and major exceptions are listed. Normally, “info” and “warning” messages are of interest only to Cisco personnel.
- **errorlog -t** — lists the most recent entries in the log and continues listing new entries as they are entered into the log. Use **<CTRL><C>** to stop the command.
- **errorlog -V** — lists the link date and software release number from when the command was built.

Note The system exception log has room for 16,384 entries, after which it wraps around.

Restrictions

Only one person at a time can use the “errorlog” command. All other users get errors.

SEE ALSO

- "alarm" section on page A-6
- "cptrace" section on page A-13

exc

Summary

The “exc” command shows the meaning of an exception code.

Description

The “exc” command lists the meaning of an exception code as listed in the “errorlog” command’s output. Be sure to include the “0x” prefix if you are looking up a hexadecimal number.

Syntax DescriptionS

The “exc” command is used in the following way:

exc <exception code>

example
exc 0x10001

SEE ALSO

“errorlog” section on page A-24

“alarm” section on page A-6

exit

Summary

The “exit” command logs the user out of the system.

getether

Summary

The “getether” command shows the server’s Ethernet address.

gwcptrace

Summary

The “gwcptrace” command displays the gateway SIM event log which provides useful information on how the MeetingPlace gateway is functioning. This log is used for troubleshooting gateway problems and to verify the MeetingPlace gateway can connect to the necessary machines (Exchange server, MeetingPlace server, etc.).

gwstatus

Summary

The “gwstatus” command displays the current status of all the connected MeetingPlace gateways and the MeetingPlace services running on those gateways.

halt

Summary

The “halt” command shuts down MeetingPlace and halts the processor.

Description

The “halt” command performs an orderly shut down of the MeetingPlace application, logging everyone off the system, then halting the processor. This is necessary before powering down the system.

Options

The “halt” command can be used in the following ways:

- **halt courtesy** — allows users up to 5 minutes to quit before the system shuts down.
- **halt disable** — prevents the system from coming back online after a restart. This allows a technician to reboot the system multiple times during a maintenance procedure.

  Note To bring the system back online, you must use the “restart” or “halt” command with the enable option (that is, “restart enable” or “halt enable”).

- **halt enable** — cancels the effect of a previous “down disable” or “halt disable” command. This allows the system to come back online when the power is restored.

Note It is important to allow the system long enough to actually halt before shutting off power. If in doubt, use the “down” command first, then type **halt** and press **Enter**, then wait 10 seconds before powering off. If you are connected to the console, you should see a signoff message from the operating system (“LynxOS is down” with some asterisks) right before the processor halts.

Note The watchdog timer is not shut off when the system is halted. Thus, a server automatically restarts approximately 6 minutes after it is halted. You may get a watchdog timeout alarm after the system comes up if the system reboots in this fashion. If you wish to keep the system down, power the system off within a few minutes of halting.

SEE ALSO

- “down” section on page A-19
- “restart” section on page A-51

help

Summary

The “help” command displays a brief summary of most of the technician commands.

hwconfig

Summary

The “hwconfig” command displays the current hardware configuration. The display includes a list of disk drives, power supply units, hot swap controllers, and installed blades.

Details

Upon typing **hwconfig** and pressing **Enter**, depending on your system you see either Figure A-2 or Figure A-3.

Figure A-2 hwconfig Command — T1 System

```
meetingplace:tech$ hwconfig
Cabinet:                Motorola CPX8216T
Bus architecture:       CompactPCI
Processor card:         CPV5370 S/N=5129443
    Processor:          Pentium III, Model 8, 700 MHz
    Memory:             512MB
    Temperature:        31C
    Voltages:           3.32V, 5.02V, 12.06V
Power Supplies:
    PS1:                OK, fan is OK
    PS2:                OK, fan is OK
    PS3:                OK, fan is OK
SCSI Adapter:           NCR 810
    DISK 1:             36000MB (SEAGATE  ST336704LW       REV=0004)
    DISK 2:             36000MB (SEAGATE  ST336704LW       REV=0004)
    Solid State Disk:   IMPERIAL "MG-35/400 ULTRA" S/N=0128 REV=B403
                        Battery: usage = 307 days, charge is OK
Ethernet:               Intel 8225x PCI 10/100 (0001af03c05e)
Modem:                  Absent or unrecognized
Smart Blades:
    Slot 16:            NMS CG6000C S/N=20363257 REV=5894-B2 MSC0 PRC0
    Slot 15:            NMS CG6000C S/N=20363261 REV=5894-B2 MSC1 PRC1
```

Figure A-3 hwconfig Command — E1 System

```
meetingplace:tech$ hwconfig
Cabinet:                Motorola CPX8216T
Bus architecture:       CompactPCI
Processor card:         CPV5370 S/N=5119906
    Processor:          Pentium III, Model 8, 700 MHz
    Memory:             512MB
    Temperature:        32C
    Voltages:           3.30V, 5.02V, 12.06V
Power Supplies:
    PS1:                OK, fan is OK
    PS2:                OK, fan is OK
    PS3:                OK, fan is OK
SCSI Adapter:           NCR 810
    DISK 1:             36000MB (SEAGATE  ST336704LW       REV=0004)
    DISK 2:             36000MB (SEAGATE  ST336704LW       REV=0004)
Ethernet:               Intel 8225x PCI 10/100 (0001af03b786)
Modem:                  Absent or unrecognized
MultiAccess Blades:
    Slot  1:            AC TP1610 S/N=220287   REV=0 AC0
Smart Blades:
    Slot  3:           NMS CG6000C S/N=351660   REV=5894-B2 MSC0 PRC0
    Slot  4:           NMS CG6000C S/N=20363244 REV=5894-B2 MSC1 PRC1
    Slot  5:           NMS CG6000C S/N=20363278 REV=5894-B2 MSC2 PRC2
    Slot  6:           NMS CG6000C S/N=336916   REV=5894-A2 MSC3 PRC3
    Slot 11:           NMS CG6000C S/N=311027   REV=5894-A2 MSC4 PRC4
    Slot 12:           NMS CG6000C S/N=352273   REV=5894-B2 (in reset)
    Slot 14:           NMS CG6000C S/N=20380179 REV=5894-B4 (in reset)
```

license

Summary

The “license” command displays MeetingPlace copyright and license information.

mtgconflicts

Summary

The “mtgconflicts” command reports any meeting ID conflicts when you turn on reservationless meetings.

Description

When migrating from standard, scheduled meetings to combined scheduled and reservationless meetings, the “mtgconflicts” command helps you identify profile ID and meeting ID conflicts. When a conflict is found, the “mtgconflicts” command lists the conflicting meetings. You can then decide whether to retain the scheduled meetings or to change the meeting IDs to resolve the conflict.

Syntax DescriptionS

mtgconflicts [ ] [-s] [-f] [-l]

- **mtgconflicts** — reports any meeting conflicts.
- **mtgconflicts -s** — shows the entire list of meeting ID and user profile ID conflicts in short format.
- **mtgconflicts -f** — shows a list of user profiles where a meeting ID matches a profile ID.
- **mtgconflicts -l** — shows the entire list of meeting ID and user profile ID conflicts in a long format.

Note The system must be down to run the “mtgconflicts” command.

SEE ALSO

- “mtgmode” section on page A-37
- “down” section on page A-19
- “restart” section on page A-51

mtgmode

Summary

The “mtgmode” command configures meeting scheduling mode.

Description

The “mtgmode” command allows you to check and change the settings for reservationless meetings.

Syntax DescriptionS

mtgmode [-s] [-r]

- **mtgmode -s** — disables reservationless meetings; scheduled meetings only
- **mtgmode -r** — enables both reservationless meetings and scheduled meetings

Note The “mtgmode” command is only available when logged in as a super user. If you are unable to log in as a super user, contact the Cisco TAC.

Note To change secondary settings, use MeetingTime.

SEE ALSO

- “mtgconflicts” section on page A-36
- “restart” section on page A-51

net

Summary

The “net” command views or modifies the MeetingPlace network configuration.

Description

The “net” command is used to view or change the network configuration for MeetingPlace. This is the information required to set up and maintain TCP/IP connections between a MeetingPlace server and various other entries on the network.

Options

After typing **net** and pressing **Enter**, the following menu appears:

- **1) View the server & site configuration** — shows the configuration of the server and the site.
- **2) Modify the server configuration** — brings up the menu below.
- **3) Select another server (current unit = #0)** — lets you choose another server.
- **99) Quit** — quits the “net” command.

When you select the “modify” option, the “net” command presents a menu allowing you to modify various attributes of the configuration. These include:

- **1) View the current configuration** — displays the current configuration.
- **2) Select a different site for this server** — prompts the user to enter a new site number.
- **3) Change the host and site names** — sets the host name for the server, a description for the server, and the name of the site. Note that the host name must start with a letter and cannot contain spaces. Any character string may be used for the description and site name.
- **4) Change server IP address and Ethernet address** — sets the Internet protocol and Ethernet addresses for the server.
- **5) Change site subnet mask or broadcast addr** — the subnet mask determines which part of the IP address is a network address and which part is the host address. The broadcast address is the IP address used for broadcasting packets on the local network. Normally, the default broadcast address offered by net is the correct one, assuming the IP address and subnet mask have been entered correctly.
- **6) Change site routing information** — allows you to specify the default gateway and whether or not to run the route daemon. The default gateway is the IP address of a gateway machine on the local network. This is the address where packets with non-local addresses are sent if no other route is known. Normally, this is the address of a router. The route daemon allows the system to use router information protocol packets broadcast by various routers on the network.
- **7) Change network time protocol servers** — allows the server to synchronize its internal clock with up to three Network Time Protocol (RFC 1305) servers. This should be done if NTP servers are available on the network.
- **99) Return to the main menu** — prompts you to save the information and updates the configuration if you choose yes.

Note Most of the information set with this command does not take effect until the system is restarted. Most of this same information can be set using MeetingTime.

SEE ALSO

- "restart" section on page A-51
- "setup" section on page A-58

ntpstatus

Summary

The “ntpstatus” command shows the status of the Network Time Protocol (NTP). It verifies that the system can access the NTP server.

Description

The “ntpstatus” command shows the connectivity status between the local host and any NTP servers that have been configured. If the NTP service is not running, you get a “read: Connection refused” response; otherwise, you see a table with a header and a line for each NTP server configured into the system. See Figure A-4.

Figure A-4 ntpstatus Command

```
meetingplace:tech$ ntpstatus
 remote    refid        st t when poll reach  delay  offset   disp
=====================================================================
 LOCAL(3)  LOCAL(3)     12 l   12   64  377    0.00    0.000   10.01
+latcom    10.10.0.165   3 u  184  256  377    0.69   27.713   27.42
*stout     64.67.62.194  2 u  156  256  377    0.53   27.348    4.14
```

Below is an explanation of what the “ntpstatus” command returns.

- **remote** — the name of the NTP server.
- **refid** — defines where the server gets its clock source; either the clock type or the IP address of the clock source.
- **st** — the NTP strata (1-16). The lower the strata number the closer the server is to an accurate clock. The local clock is set to 12; a server at strata 13-16 is not used.
- **t** — the type of clock.
- **when** — defines, in seconds, the last time the NTP server was polled.
- **poll** — defines, in seconds, the interval in which the NTP server is polled.
- **reach** — defines how often the NTP was reached by MeetingPlace. This is a bit map field and contains octal numbers. After converting the value to a binary number, each bit represents one attempt. A binary value of 0 means that the attempt failed and a value of 1 means success. For example, 377 (octal) = 11111111 (binary), which is a perfect reach, meaning that MeetingPlace succeed to reach the NTP server eight times out of eight tries. A value of 37 (octal) = 00011111 (binary), which means that out of the last eight attempts, it was only able to reach the NTP server five times.
- **delay** — defines the transmission delay, in milliseconds, for communication with the server.
- **offset** — defines the calculated clock skew between the client and the server in milliseconds.
- **disp** — defines the measure of goodness. The smaller the number, the better.

There is also a character before the name of each remote NTP server. This character indicates the fate of the peer in the clock selection process. The codes mean:

- **<SPACE>** — discarded due to high stratum or failed sanity checks.
- **X** — designated false ticker by the intersection algorithm.

- **.** — called from the end of the candidate list.
- **-** — discarded by the clustering algorithm.
- **+** — included in the final selection set.
- **#** — selected for synchronization; but distance exceeds maximum.
- ***** — selected for synchronization.
- **O** — selected for synchronization, pps signal in use.

Note Only the network server communicates with the NTP servers. All other units reference time from the network server.

passwd

Summary

The “passwd” command changes the technician’s password.

Description

The “passwd” command is used to change the password for the technician login account. You enter the old password and then enter the new password twice for verification purposes.

Note Only the first eight characters of a password are used.

ping

Summary

The “ping” command tests network connectivity.

Description

The Internet is a large and complex aggregation of network hardware, connected together by gateways. Tracking a single-point hardware or software failure can often be difficult. The “ping” command utilizes the ICMP protocol’s mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams (“pings”) have an IP and ICMP header, followed by a struct timeval, and then an arbitrary number of “pad” bytes used to fill out the packet. Default datagram length is 64 bytes, but this may be changed using the command-line option.

Options

The “ping” command can be used in the following ways:

- **ping -r <host>** — bypasses the normal routing tables and sends directly to a host on an attached network. If the host is not on a directly attached network, returns an error. This option can be used to ping a local host through an interface that has no route through it (for example, after the interface was dropped by routed).
- **ping -v <host>** — lists ICMP packets other than ECHO_RESPONSE that are received.

Note The <host> argument is either a host name or IP address. MeetingPlace has no host name lookup mechanism, so normally an IP address should be used.

Note When using the “ping” command for fault isolation, run it first on the local host to verify the local network interface is up and running. Then hosts and gateways further and further away should be pinged. The “ping” command sends one datagram per second and prints one line of output for every ECHO_RESPONSE returned. No output is produced if there is no response. If an optional count is given, only that number of requests is sent. Round-trip times and packet loss statistics are computed. When all responses have been received or the program times out (with a count specified), or if the program is terminated with a SIGINT, a brief summary is displayed.

Note The “ping” command is intended for use in network testing, measurement, and management. It should be used primarily for manual fault isolation. Because of the load it could impose on the network, it is unwise to use the “ping” command during normal operations or from automated scripts.

port

Summary

The “port” command views or modifies a port or port group record.

Description

The “port” command is used to configure port and port group records in the database. It is very similar to the capability offered through the MeetingTime Configure tab. For a port, this determines which group this port belongs to, if any. If the port does not belong to a group, the port itself can be configured whether it should be active, the type of trunk signaling, the number of DID digits, whether there is human assistance, whether it can be flash transferred, and whether it can be outdialed on. For a port group, this determines whether all ports belonging to this group are active, the type of trunk signaling, the type of card, the number of DID digits, whether there is human assistance, wether it can be flash transferred, and whether it can be outdialed on.

Options

After typing **port** and pressing **Enter**, the following menu appears:

- **1) View port record(s)** — prompts the user to select a specific port or all ports. If the port belongs to a group, the system prints which group the port belongs to, and shows the port characteristics as defined by the group record. If the port does not belong to a group, the port characters for that port are shown.
- **2) Modify port record** — prompts the user to select a specific port. If the user specifies that the port belongs to a group, no additional modification is necessary. All the port characteristics are taken from the group. If the user specifies that the port does not belong to a group, the user is prompted for all the port characteristics. When modifying the port record, always enter “n” for flash transfer.
- **3) Copy port records** — prompts the user to select a specific port to copy from and a range of ports to copy to. You can also copy to a single port. All the port characteristics are copied from the source port to all the destinations.
- **4) View group record(s)** — prompts the user to select a specific port group or all port groups. The characters for each of the selected groups are shown.
- **5) Modify group record** — prompts the user to select a specific port group, then prompts the user to enter all the group characteristics. When modifying the group record, always enter “n” for flash transfer.
- **x) Exit** — exits the “port” command.

Note On each voice processor unit, ports are numbered from 0-119 (or one less than the licensed number of access ports). Before configuring the ports, each individual port needs to have been assigned to a hardware trunk in the span command. A port of one hardware type cannot be assigned to a group of different hardware type.

Note The individual port and port group records can also be reconfigured through the MeetingTime Configure tab. Note that the port record references the card record for that port. It is important that the card and port records be consistent within the database, cross-referencing accurately.

Note Changes made by the "port" command take effect after the next system restart.

SEE ALSO

- "blade" section on page A-8
- "dcard" section on page A-18
- "span" section on page A-59
- "restart" section on page A-51

portstat

Summary

The “portstat” command displays the current port active or inactive status, the port group assignment, and port and card mapping.

Syntax Descriptions

portstat [[<start#>] [<end#>]] [-db] [-mvip] [-ce] [-all] [-c]

where [<start#>] is the starting port number and [<end#>] is the ending port number.

- **portstat [[<start#>] [<end#>]] [-db]** — displays all the database information for the chosen ports.
- **portstat [[<start#>] [<end#>]] [-mvip]** — displays the MVIP timeslot assignments.
- **portstat [[<start#>] [<end#>]] [-ce]** — displays the most recent PRC command and event.
- **portstat [[<start#>] [<end#>]] [-all]** — displays information about each option above.
- **portstat [[<start#>] [<end#>]] [-c]** — continuous status. Only available for the [-mvip] and [-ce] options.

protparm

Summary

The "protparm" command is used to view, modify, copy, and delete the protocol parameter table.

Description

The "protparm" command is used to view, modify, copy, and delete the protocol parameter table. It lets you develop signaling protocol tables for linecards.

In the general information list, it tells the system whether the table is active, gives a description, signaling type, protocol, and options for CAS signaling table file name, default clearing cause, B-channel negotiation, and protocol side.

Options

After typing **protparm** and pressing **Enter**, the following menu appears:

- **1) View protocol parameter table(s)** — prompts the user to select one or all protocol table numbers. The system then prints a menu allowing the user to select what information they would like to view.
- **2) Modify protocol parameter table** — prompts the user to enter a specific protocol parameter number. The system then prints a menu allowing the user to select which information they would like to modify.
- **3) Copy protocol table** — prompts the user to enter the protocol table number to copy from. The user is then prompted to enter the protocol table number to copy to.
- **4) Delete protocol table(s)** — allows the user to delete any or all protocol tables by entering the numbers of the tables.

Note Changes to the protocol tables only take effect after the next system restart.

SEE ALSO

- "e1card" section on page A-21
- "e1span" section on page A-22
- "restart" section on page A-51

recover

Summary

The “recover” command fixes corrupted database structures and forces database and voice file system consistency.

Description

The “recover” command examines all the linkages and structures of the database and voice file system and forces consistency between all the records. On successful completion, the database should be fully consistent, although some inconsistent data may have been discarded. This command is useful in cases where portions of the database have been corrupted due to power failures or other problems.

Warning **The” recover” command should only be run on systems with fully functional and trusted hardware. This command can cause severe and irreparable damage to a system that is not operating properly at the hardware level. Do not use this command on a system that does not have all of its disk drives installed and operating correctly.**

Restrictions

The time required for this command to run is proportional to the number of records in the database and the amount of voice storage. On a system with a large database and a lot of voice storage, this may take many hours.

Caution We suggest running a system backup before running recover.

MeetingPlace must be down to run the “recover” command. Use the “down” command to shut down MeetingPlace.

SEE ALSO

- “down” section on page A-19
- “restart” section on page A-51

release

Summary

The “release” command shows the MeetingPlace software release number.

Description

The “release” command shows the MeetingPlace software release number.

Options

The “release” command can be used with the following options:

- **release -r** — displays the release number. This is the default if no arguments are specified.
- **release -l** — displays the build date (the date the release command was linked) and the version control tag.

Note Release numbers consist of three integers connected by dots. The first integer is the major release, the second is the minor release, and the third is the patch level.

SEE ALSO

- “swstatus” section on page A-63

resize

Summary

The “resize” command resets the terminal settings to your screen size.

restart

Summary

The “restart” command shuts down and restarts MeetingPlace.

Description

The “restart” command performs an orderly shut down of the MeetingPlace application, logging everyone off the system, and then restarts the system. This is necessary to bring back up a system that has been shut down using the “down” command.

Options

The “restart” command can be used alone or with the following options:

- **restart courtesy** — gives users up to 5 minutes to quit before the system shuts down.
- **restart disable** — prevents the system from coming back online after the restart. This allows you to reboot the system multiple times during a maintenance procedure. To bring the system back online, you must use the “restart enable” or “halt enable” commands.
- **restart enable** — cancels the effect of a previous use of the “down”, “halt”, or “restart” commands with the disable option. This allows the system to come back online when power is restored.

SEE ALSO

- “down” section on page A-19
- “halt” section on page A-31

restore

Summary

The “restore” command restores the MeetingPlace database from the network backup.

Description

The “restore” command copies the contents of a system backup onto the system disk. It also makes sure that the restored database is self-consistent. This procedure is appropriate only if the database is missing (as in where the system disk has failed and been replaced) or irreparably corrupted in some manner.

Consult Cisco TAC before using this command.

Note Because the backup gateway contains only database information, with no voice files, linkages between a restored database and the voice file system will have many inconsistencies. Any voice recordings created or modified since the time of the backup will be lost and cannot be recovered.

Note To assure consistency between the database and voice file systems, the “restore” command executes the “recover” command automatically. Because the “recover” command can be destructive if all disks are not fully accessible, the “restore” command should not be executed if any disk is not mounted or not working properly.

Note The recovery portion of this operation takes time proportional to the number of database records and the amount of voice storage on the system. On a system with a large database and a lot of voice storage, it can take many hours.

Restrictions

The system must be down before running the “restore” command. Use the “down” command to shut down MeetingPlace before running the “restore” command.

SEE ALSO

- “down” section on page A-19
- “recover” section on page A-48
- “restart” section on page A-51

revert

Summary

The “revert” command activates the previous configuration.

Description

The “revert” command allows you to activate the previous configuration. It is useful in situations when, after an upgrade, you do not get the expected result. If you did not run the “save” command yet, you can run the “revert” command to restore the system back to its original condition before the upgrade. You have to run the “save” command after running the “revert” command.

save

Summary

The “save” command saves the current configuration.

Description

The “save” command commits the current configuration and starts the periodical backup process. If the system is down, it saves immediately. If the system is up, only application files and prompts are saved immediately. The rest are saved at the regular scheduled time (on the hour). For each software upgrade, after verification, run the “save” command.

savelicense

Summary

The “savelicense” command saves the software license keys to a floppy disk.

Description

The “savelicense” command saves the software license keys to a floppy disk.

Note If the Ethernet card is being replaced and the new license keys are going to be loaded using a floppy disk, insert the floppy disk, type **update**, and press **Enter**. This updates the server with the new license keys associated with the new Ethernet card.

SEE ALSO

- “update” section on page A-66

setipcodec

Summary

The “setipcodec” command sets the IP codec configuration.

Description

The “setipcodec” command is used to view and modify the IP codec configuration. When initially enabling an IP system, it is important to enable and test each codec individually by enabling all the codecs that are used, giving them the proper priorities, and placing calls to verify the correct codec is used. If different devices use different codecs, test each of them to verify the proper codec is selected.

Note This version supports 711 a-law, 711 u-law, and 729. The server can accept both 729 and 729a codec data, however it only sends 729a codec data.

setsn

Summary

The “setsn” command sets or displays the system’s serial number.

Description

The “setsn” command is used to either view or set the system serial number in the database.

Options

- setsn — displays the system’s serial number and customer name.
- **setsn <serial number>** — sets the serial number in the database.

Note Setting the serial number is normally a factory procedure. However, if the original database is lost or corrupted, it may be necessary to set the serial number in the field. The serial number in the database should match the label on the back of the machine. Setting the serial number incorrectly may result in future service difficulties.

setup

Summary

The "setup" command configures the server as either a standalone server or a shadow server.

Options

The options for the server configuration include the following:

- standalone — the MeetingPlace conference server is not connected to a MeetingPlace network server. This is the default configuration.
- shadow network server — this is a redundant network server operating in shadow mode.

After selecting the configuration, the system prompts you for a time zone.

Warning **Incorrectly entering the time zone prevents the server from operating correctly. Restarting a system when it is not configured correctly may result in damage that can only be corrected by reloading the system software from a backup gateway.**

SEE ALSO

- "net" section on page A-38
- "update" section on page A-66

span

Summary

The “span” command views or modifies a T1 CAS span record.

Description

The “span” command is used to view or modify a T1 CAS span record in the database. This tells the system whether the span should be active, various characteristics of the span, and the mapping between trunks and internal port numbers.

The following characteristics are set by the “span” command:

- Framing — D4 or ESF. The framing protocol used on this span. This is determined by the service provider. We recommend using ESF only.
- Zero code suppression — none, B8ZS, or jammed bit. This protocol is determined by the service provider. We recommend using B8ZS only.
- Timing — external or internal. This determines whether the span is permitted to supply trunk timing for the system. Specify external if the span is connected to the public network or a trusted system. At least one span should always be designated external.
- External sync priority — a number (1-255) or never that controls the priority (1 is highest, 255 is lowest) of the spans that are set for external timing. The system picks the highest priority operational span to provide the timing. If two spans have the same priority, the lower numbered span is used.
- Remote loopback to network? — y or n. If yes, this puts the span into a loopback mode for testing from the remote end. For normal operation, set to n.
- Internal data loopback? — y or n. If yes, this causes the span to loop back locally for running diagnostics. For normal operation, set to n.

Options

After typing **span** and pressing **Enter**, the following menu appears:

- **1) View DTI span record(s)** — prompts the user to select a specific span or all spans. The system displays whether the card is active, the characteristics of the span, and the port number of each trunk.
- **2) Modify DTI span record** — prompts the user to select a specific span, then prompts the user for whether the span should be active, the characteristics of the span, and the port number assignment for each trunk.
- **x) Exit** — exits the “span” command.

Note For each voice processor unit, the spans are numbered 0-4. Trunks on a span are numbered 1-24. Ports are numbered 0-119 (or the number of licensed access ports minus 1). There are up to four span records for each Smart Blade.

Note The span record is referenced by both a Smart Blade record (see the “blade” command) and each port record (configured from the port command and MeetingTime). It is important to be sure that these references are consistent. If a port is referenced in a span record, the corresponding port record must reference that span.

Note If a Smart Blade is not active, the four spans will not operate even if they are set to active in the span record.

Note Changes to a span record take effect after the next system restart.

SEE ALSO

- "port" section on page A-44
- "blade" section on page A-8
- "dcard" section on page A-18
- "spanstat" section on page A-61
- "restart" section on page A-51

spanstat

Summary

The “spanstat” command shows the status of T1 or E1 spans.

Description

The “spanstat” command shows the status of the T1 or E1 spans in the system. Entered with no options, it displays a line for each of the span records, indicating which Smart Blade and line the span is attached to, and whether the span is up. If a span number is specified, only information about that span is displayed.

Options

The “spanstat” command can be used with the following options:

- **spanstat -ab** — monitors the signaling state, one span at a time, for the span numbers specified (or for all spans if no span number is specified). For the specified span, shows the signaling state for both transmit (TE->NT) and receive (NT->TE) on each trunk. This is refreshed continuously until you stop the command. Press **q** to quit or go to the next span. (You do not need to press Enter.) Press <CTRL><C> to immediately stop the command.
- **spanstat -s** — show the span’s statistics. This lists various exception counts associated with the span.
- **spanstat -cl** — clears the statistics for the span numbers specified (or for all spans if no span number is specified). This clears the exception counts for the spans.
- **spanstat -all** — shows the span activity for 20 spans at a time. Type **n** and press **Enter** for the next page.
- **spanstat -pa** — paginates the span summary output.

SEE ALSO

- “activity” section on page A-4
- “span” section on page A-59
- “errorlog” section on page A-24
- “cptrace” section on page A-13
- “e1span” section on page A-22

swcheck

Summary

The “swcheck” command verifies the software file checksums.

Description

The “swcheck” command generates a 32-bit CRC checksum on each of the application software files in the system and then compares the generated checksums against known good values. Any discrepancies are displayed.

Note Some software patches may not update the checksum file. This results in discrepancies when the “swcheck” command is run. In this particular case, discrepancies are expected and should not be a cause for alarm.

Note The “swcheck” command is useful for diagnosing certain system integrity problems. Unexplained discrepancies can result from file corruption or a failure to correctly transfer data from the system disk. In the latter case, running this command again yields a different result.

SEE ALSO

- “release” section on page A-49

swstatus

Summary

The “swstatus” command displays the current status of the system’s software.

Description

The “swstatus” command displays certain information about the system, plus the list of software modules loaded into memory. General information includes the following:

- software release number — the version of the system software.
- serial number — the serial number listed in the database.
- customer name — the customer name listed in the database.
- system mode — the current loading status of the MeetingPlace software. One of the following: up, down, shutting down, loading, coming up, and unloaded.
- temperature — the temperature (in degrees Celsius) as measure on the MSC card inside the cabinet.
- power supply — displays either “OK” or displays a count of the times the voltage was out of tolerance.

The software module information includes:

- module name — the name of the software module.
- status — status of the module, either up, down, starting, going down, exiting, or gone.
- version — shows the build date and the software release built into each software module.

SEE ALSO

- “alarm” section on page A-6
- “errorlog” section on page A-24

timezone

Summary

The “timezone” command sets the system’s local time zone.

Description

The “timezone” command sets the time zone used for CLI commands. It also sets local time zone for end users. On entry, the technician is presented with a list of available time zones. These are listed by continent and city. The technician should pick the city that uses the same time zone as the local site.

Options

Type **timezone** and press **Enter** to bring up the following options:

- **1) Europe** — brings up a screen of time zones for Europe.
- **2) Far East** — brings up a screen of time zones for Asia and Australia.
- **3) North America** — brings up a screen of time zones for North America.
- **99) quit** — quits the “timezone” command and takes you back to the tech$ prompt.

Note Fort Wayne, Indiana and Phoenix, Arizona are listed as time zone options because their states do not conform to the normal US daylight savings time rules. Do not choose these options for sites outside their respective areas.

Restrictions

Only time zones for the United States, UK, Hong Kong, Australia, and Singapore are listed.

SEE ALSO

- “date” section on page A-15

tvportstat

Summary

The “tvportstat” command shows the status of IP ports.

Description

The “tvportstat” command is used to show the status of IP ports in the system. Entered with no options, the help screen is displayed.

Syntax DescriptionS

tvportstat <low sysport #> [high sysport #] [options]

where <low sysport #> is a number from 0-1151 and <high sysport #> is a number from 0-1151.

Options

The “tvportstat” command can be used with the following options:

- **tvportstat -all** — displays the signaling state for all ports or for a specific range of ports when used with the low port/high port option. This screen continuously refreshes.
- **tvportstat -p<low port> -p<high port> -s** — displays the statistics for one or more ports.
- **tvportstat -p<low port> -p<high port> -cl** — clears the statistics for one or more ports.
- **tvportstat -p<low port> -p<high port> -c** — displays the configuration for one or more ports.
- **tvportstat -h** — displays the help screen.

update

Summary

The “update” command runs a software update and supports patch application.

Description

The “update” command is used to start a software update procedure. After prompting the user to enter the location of the update file, the “update” command automatically extracts all the files and installs the update or patch.

After typing **update** and pressing **Enter**, you see a menu asking where the update file is located. You are shown the following options:

1) CD — prompts the user to enter a CD into the CD-ROM drive.

2) Diskette — prompts the user to enter a diskette into the floppy disk drive.

3) Remote File — prompts the user to enter whether the remote file is FTP or gateway SIM. Type **f** and press **Enter** for FTP (the default) or type **g** and press **Enter** for gateway SIM.

The gateway SIM method requires an operational gateway SIM agent on the remote system where the patch resides, and an operational SIM on the MeetingPlace server. This means the server must be up during the distribution step if the gateway SIM method is to be used. Gateway SIM version 4.2 and above will support this feature. Gateway SIM is much slower than FTP.

If you are going to use FTP or gateway SIM to apply the update, obtain the necessary information before you start the update.

Table A-2 Information Needed for Applying Patch via FTP Distribution

Description		Value
Obtain information about FTP server	IP Address or name of FTP server	IP Address _____ Or Name _____
	User ID on FTP server	User ID _____
	Password for the User ID	Password _____
Path to the patch file and patch file name on FTP server	If you place a file in the default ftp directory for the specify user ID, then all you need to specify is the filename, if not you need to specify the path plus the file name. For example: R5.2/Path/update.tar.gz	Path/name _____ _____

Table A-3 Information Needed for Applying Patch via GWSIM Distribution

Description		Value
Obtain information about Gateway server	Unit number of the Gateway	Unit _____
Path to the patch file and patch file name on the gateway	You need to specify the path plus the file name. For example: c:/R5.2/Path/update.tar.gz	Path/name _____ _____

4) Local File — prompts the user to enter a local file name. The local file path cannot contain embedded spaces. Forward slashes ("/") must be used as path separators.

q) (Quit Update) — exits the "update" command.

Options

The "update" command can be used with the following options:

- **update status** — shows a quick status of the upgrade. Indicates how long it has been since the last write to the log file and gives a general system status. If the status shows as "operating", then an upgrade is NOT in progress.
- **update stop** — can be used via HyperTerminal session, via the front panel, or via a modem to stop an upgrade. To continue with the upgrade, you must run the "revert" command, then the "restart" command to return the system back to its pre-upgrade state. Then you have to begin the upgrade again.
- **update trace** — allows you to monitor the output of an upgrade over a modem line. The display should be updated every five minutes; however, before declaring the upgrade is stuck, allow 30 minutes.

Note Before running the "update" command, run the backup procedure to back up the database.

Restrictions

The "update" command can run if the system is up or down, but the batch file loaded from the disk may refuse to execute if the system is not down. Normally, you should bring the system down before running the "update" command.

SEE ALSO

- "down" section on page A-19

updatedbsize

Summary

The “updatedbsize” command updates the database size.

Description

The “updatedbsize” command determines the database configuration appropriate to the size of the disk and then allocates space on the disk according to that configuration.

SEE ALSO

- “recover” section on page A-48
- “restore” section on page A-52

Required Toolkit

Before installing MeetingPlace, verify that you have these tools necessary for a successful installation:

- laptop computer
- null modem female to female DB9 serial cable. For details, see the"Connecting your laptop" section on page 4-1.
- screwdriver blade type #2
- screwdriver Phillips #1
- screwdriver Phillips #2
- anti-static grounding strap
- connectivity tester (Ohm tester or pen light)
- crossover cable for RJ-48 connectors. See Figure B-1.

Figure B-1 Crossover Cable Pinouts

Specifications

This appendix lists the specifications for MeetingPlace Audio Server 5.2 for 8112 server.

Key features

- Carrier-grade compact PCI voice conferencing system.
- MeetingPlace leading application software with integrated web conferencing capabilities.
- Calendar integration with Microsoft Outlook and Lotus Notes.
- Corporate LDAP directory management.
- Notifications through e-mail and fax.

Technical specifications

Capacity

- Up to 1152 ports in a T1 CAS system.
- Up to 736 ports in a T1 PRI system (North America only).
- Up to 960 IP ports, supports vocoders G.71.1 (A-law and u-law) and G.729a, supports signaling H.323 and SIP.
- Mix and match T1 and IP end points.
- Non-blocking N/2 simultaneous conferences.
- Up to 960 ports in an E1 system.
- Mix and match E1 and IP end points.

Size and weight

- Height: 21 inches (53 cm)
- Width: 18.9 inches (48 cm)

- Depth: 17.1 inches (43 cm)
- Up to 130 lbs (59.1 kg) fully loaded

Mounting

- Per EIA standard RS-310-C in 19-inch or 23-inch rack with mounting brackets

Telephony trunking

- T1 CAS framing: ESF or D4/SF framing
- T1 CAS linecodes: AMI or B8ZS
- T1 CAS protocols: E&M wink start, ground start, or loop start
- T1 PRI framing: ESF or D4/SF framing
- T1 PRI linecodes: AMI or B8ZS
- T1 PRI protocols: AT&T (TR41459), Bell (NI-2), Nortel (DMS-100)
- E1 framing: CRC4 or non-CRC4
- E1 linecodes: HDB3
- E1 protocols: Euro ISDN or QSIG (QSIG-ECMA and QSIG-ETSI)

Redundancy

- Three hot-swappable redundant power supply units and fans
- Dual 36GB disk drives
- Dual Compact PCI backplane

Environment

- 10-40 degrees Celsius (50-104 degrees Fahrenheit) operating
- 5-80% humidity, non-condensing

Electrical

- System power: 90-260 VAC, 47-63 Hz
- 350 Watts output

Serviceability

- Front access service and installation of platform components
- Rear connection of I/O allows Smart Blade removal without disconnecting field wiring

Note The MeetingPlace server has the ability to cancel an echo. The maximum echo tail length it can cancel is 128 ms. For more information, contact the Cisco TAC.

Configuring NSF Codes

This appendix explains how to configure MeetingPlace with the correct NSF codes *when necessary.*

Configuring NSF codes on the MeetingPlace server may be necessary when making outdials directly to the PSTN (without an intervening PBX) on trunks using the ISDN protocol.

Note For the most part, NSF codes are used only in Canada and the United States.

Note To determine if this system requires NSF code configuration, ask the telephone service provider if the system uses NSF codes. This should have been determined prior to installation and recorded in worksheet F-1 in the *MeetingPlace Audio Server 5.2 Installation Planning Guide*.

If the system uses NSF codes, you will need to use the steps in this appendix to configure MeetingPlace correctly. If the system does not use NSF codes, you do not need to complete the steps in this appendix.

MeetingPlace needs to be configured with the proper NSF code information to operate with the PSTN. Failure to set up the NSF codes properly (or not configure them at all) has two main effects:

- Failed outdials — Outdials directly to the PSTN are rejected. However, outdials via an intervening PBX probably still work.
- Higher phone service costs — Outdials might work directly to the PSTN but a carrier's standard or premium rates may be applied, rather than discounted rates. As part of provisioning a service, a carrier will require that customers use specific NSF code information. This information must be sent out on every call to get a specific discounted service rate for the call.

Understanding NSF codes

The ISDN protocol allows telephone service providers to add to the ISDN protocol with their own custom protocol extensions. These extensions allow carriers to provide various localized services that are not defined in the general ISDN specifications. These extensions are contained in the Network Specific Facility (NSF) Information Element (IE). They are generally called "NSF" codes for short. The NSF code is also called the Binary Facility Coding Value (BFCV).

NSF codes consist of the following:

- NSF code type (service or feature). Refer to "NSF code type" section on page D-2
- NSF code value (which service or feature is desired). Refer to "NSF code value" section on page D-2

- Carrier Identification Code (CIC) (optional) — identifies which carrier is providing a service or feature. Refer to "Carrier identification code (optional)" section on page D-2
- Modifying parameter (optional). Refer to "Modifying parameter (optional)" section on page D-3

This NSF code information should be obtained from the customer prior to installation. See worksheet F-1 in the *MeetingPlace Audio Server 5.2 Installation Planning Guide*.

NSF code type

This section explains what an NSF code type is. To get the NSF code type for this installation, refer to worksheet F-1 in the *MeetingPlace Audio Server 5.2 Installation Planning Guide*.

NSF codes determine if it is a service or feature. There are four options as listed in Table D-1.

Table D-1 Examples of NSF Code Types

NSF Code Type	Examples
service	Software Defined Network (SDN) by AT&T
feature	Billing Number preferred for ANI by AT&T
service plus modifying parameter	Outwats and Tie Line by Bell Canada
feature plus modifying parameter	Vari-A-Bill (Flexible Billing) by AT&T

NSF code value

This section explains the NSF code value. To get the NSF code value for this installation, refer to worksheet F-1 in the *MeetingPlace Audio Server 5.2 Installation Planning Guide*.

The NSF code value is also referred to as the Binary Facility Coded Value (BFCV). This value indicates the specific ID of the service or feature. This value can range from 0-31. Table D-2 gives some common code types and their value.

Table D-2 Examples of NSF Code Values for Specific Code Types

Specific NSF Code Type	NSF Code Value (BFCV)
Software Defined Network (SDN) by AT&T	1
Billing Number preferred for ANI by AT&T	4
Outwats by Bell Canada	3
Vari-A-Bill by AT&T	9

Carrier identification code (optional)

This section gives information about the Carrier Identification Code (CIC). For specific information on the CIC for this installation, refer to worksheet F-1 in the *MeetingPlace Audio Server 5.2 Installation Planning Guide*.

The CIC is a four-digit decimal code established by the FCC in the United States to identify each telephone company. For example, the CIC for AT&T is 1288. If a subscriber has a variety of services available from various carriers, this code can be used to select a carrier. This code is not always included in an NSF code. Whether or not it is included is dictated by the specific carrier providing the connection from MeetingPlace to the Central Office.

Note Some carriers prefer to abbreviate their CIC to three digits (dropping the most significant digit). Therefore, when requesting CIC information, it is important to determine if the carrier uses three or four digits.

Modifying parameter (optional)

This section gives information about the modifying parameter. For specific information on the modifying parameter for this installation, refer to worksheet F-1 in the *MeetingPlace Audio Server 5.2 Installation Planning Guide*.

The modifying parameter, if used, is a value from 0-255. For example, Bell Canada uses this parameter as a "Service IDentifier" (SID). For their Outwats service, the NSF code is not complete unless it has a BFCV of 3 and a parameter (SID) of 2. Another example is that Vari-A-Bill by AT&T has a BFCV of 9 and a parameter of 6.

Configuring NSF codes

This section gives step-by-step instructions on how to configure the NSF code type. This procedure consists of entering the information from worksheet F-1 in the *MeetingPlace Audio Server 5.2 Installation Planning Guide* into a protocol table on the MeetingPlace server. The protocol table is used when MeetingPlace outdials to the PSTN. The default protocol tables (0-49) do not enable NSF codes and are read-only. Therefore, it is necessary to create a new protocol table. To create the new protocol table, make a copy of an existing protocol table and make modifications to the new table.

Copying an existing protocol table to create a new protocol table

This section explains how to use the "protparm" command to copy an existing protocol table to create a new protocol table. Refer to "protparm" section on page A-47 for more information.

Step 1 At the tech$ prompt, type **protparm** and press **Enter**.The "protparm" configuration menu appears as in Figure D-1.

Figure D-1 Copying a Protocol Table

```
meetingplace:tech$ protparm

*****   P R O T P A R M   C O N F I G   M E N U   *****

        1)  View protocol parameter table(s)
        2)  Modify protocol parameter table
        3)  Copy protocol table
        4)  Delete protocol table(s)
        x)  Exit program

Enter command: 3
Enter protocol table to copy from [0..99] : 3
Enter protocol table(s) to copy to [50-99] : 50
Copied to protocol table(s) 50.
```

Step 2 Type **3** and press **Enter** to copy a protocol table, as shown in line eleven in Figure D-1.

Step 3 Enter the protocol table number you want to copy from. In this example, it is protocol table number 3, so type **3** and press **Enter**.

Refer to Table D-3 for assistance with choosing which table to copy from.

Note If this is part of an upgrade from a pre-5.1 release, the default protocol tables 3 and 4 are not correct. To resolve this, use the "protparm" command to delete tables 3 and 4. This restores them to the defaults as listed in Table D-3.

Table D-3 Protocol Table Defaults

T1 PRI Protocol Type	Protocol Table Number to Copy From
AT&T	2
Nortel	3
Bell	4

Step 4 Enter the protocol table number you want to copy to. In this example, it is protocol table number 50, so type **50** and press **Enter**. See Table D-3.

The new protocol table number must be a new number (one not already used by an existing table). Systems are shipped with tables 0-49 already configured, so when creating new tables, you must use 50 or higher.

The system returns by telling you the protocol table was copied as in the last line in Figure D-1.

Step 5 Type **x** and press **Enter** to exit the "protparm" utility.

Modifying the new protocol table

This section explains how to modify the newly-created protocol table so the NSF code information is correct.

Note The following steps assume that the information copied to this new protocol table in the "Copying an existing protocol table to create a new protocol table" section on page D-3 is correct, with the exception of the NSF code information.

Step 1 At the tech$ prompt, type **protparm** and press **Enter**.The "protparm" configuration menu appears.

Step 2 Type **2** and press **Enter** to modify the protocol parameter table. See Figure D-2.

Step 3 Type the table number for the new protocol table you created in the "Copying an existing protocol table to create a new protocol table" section on page D-3. In this example, it is table 50, so type **50** and press **Enter**. See Figure D-2.

Figure D-2 protparm Modify Menu

```
Enter command: 2
Enter protocol table number [50..99] : 50

*****   M O D I F Y   M E N U   *****

   1)  Modify entire table
   2)  Modify general information
   3)  Modify incoming called party number processing (DDI)
   4)  Modify incoming calling party number processing (CLI)
   5)  Modify outgoing calling party information
   6)  Modify outgoing called party type of number (TON)
   7)  Modify outgoing called party numbering plan (NPI)
   8)  Modify outgoing private number definition
   9)  Modify outgoing local number definition
   a)  Modify outgoing long distance number definition
   b)  Modify outgoing international number definition
   c)  Modify outgoing Network Specific Facilities (NSF) codes
   d)  Modify outgoing NSF Carrier Identification Code (CIC)
   x)  Exit to main menu

Enter modify command [table 50]: c
```

Step 4 Type **c** and press **Enter** to modify the outgoing Network Specific Facilities (NSF) codes as shown in the last line of Figure D-2.

Each time you press **Enter**, you move to the next line. See Figure D-3.

Figure D-3 Modifying Outgoing NSF Codes

```
Enter modify command [table 50]: c

----------------- PROTOCOL TABLE 50 -----------------
------- To skip over a field, just press <cr> -------

Outgoing Network Specific Facilities (NSF) Codes
------------------------------------------------
  NSF code 1 type             [    not used] :
  BFCV 1 value                    [not used] :
  Extra 1 param                   [not used] :
  NSF code 2 type             [    not used] :
  BFCV 2 value                    [not used] :
  Extra 2 param                   [not used] :

Enter modify command [table 50]:
```

Step 5 Enter the NSF code type and press **Enter**. Depending on the installation, it is “service”, feature”, “parm service”, or “parm feature”. Refer to worksheet F-1 in the *MeetingPlace Audio Server 5.2 Installation Planning Guide*.

Step 6 Enter the NSF code value (BFCV) and press **Enter**. Refer to worksheet F-1 in the *MeetingPlace Audio Server 5.2 Installation Planning Guide.*

Step 7 Enter the modified parameter, if there is one, and press **Enter**.

Note The menu gives you the option of entering a second NSF code. If there is no second code, then continue pressing **Enter** to bypass this.

Step 8 The modify command prompt appears when you are finished, as shown in the last line of Figure D-3.

Step 9 Type **d** and press **Enter** to modify the outgoing NSF Carrier Identification Code (CIC). See Figure D-4.

Figure D-4 Modifying the NSF CIC

```
Enter modify command [table 50]: d

----------------- PROTOCOL TABLE 50 -----------------
------- To skip over a field, just press <cr> -------

Outgoing NSF Carrier Identification Code (CIC)
------------------------------------------------
  CIC network type               [     natl] :
  CIC code                            [1288] :

Enter modify command [table 50]:
```

Step 10 Type the CIC network type and press **Enter**. Depending on the installation, it is “user”, “natl”, “intl”, “user4”, “natl4”, or “intl4”. Refer to worksheet F-1 in the *MeetingPlace Audio Server 5.2 Installation Planning Guide*.

Step 11 Type the CIC code from worksheet F-1 in the *MeetingPlace Audio Server 5.2 Installation Planning Guide* and press **Enter**.

Step 12 Type **x** and press **Enter** to go back to the main “protparm” utility menu.

Step 13 Type **x** and press **Enter** to exit the “protparm” utility.

Assigning necessary port groups to use the new protocol table

All port groups that have ports using NSF codes need to be assigned to use the new protocol table. For more information, refer to “port” section on page A-44.

Step 1 At the tech$ prompt, type **port** and press **Enter**. Figure D-5 appears.

Figure D-5 port Command Menu

```
meetingplace:tech$ port
MeetingPlace is up

*****   P O R T / G R O U P   C O N F I G   M E N U   *****

        1)  View port record(s)
        2)  Modify port record
        3)  Copy port records
        4)  View group record(s)
        5)  Modify group record
        x)  Exit program

Enter command:
```

Step 2 Type **5** and press **Enter** to modify the group record. The second line in Figure D-6 appears.

Figure D-6 Modifying the Port Group

```
Enter command: 5
Enter port group record number [0..31] : 0

------------     GROUP  0      --------------
--- To skip over a field, just press <cr> ---
  Activate the group?             [y] :
  Card type                  [    T1] :
  Signaling          [    loop start] :  protocol table
  Protocol table                [ 0] :  50
  Number of DID digits          [ 0] :
  Human assistance?              [n] :
  Flash transfer?                [n] :
  Outdial?                       [y] :

Enter command: x
```

Step 3 Select the appropriate port group. In this example, it is port group 0, so type **0** and press **Enter**. The rest of Figure D-6 appears.

Step 4 Continue pressing **Enter** until you reach Signaling.

Step 5 Type **protocol table** and press **Enter** to select signaling.

Step 6 Select the appropriate protocol table number. In this example, it is protocol table 50, so type **50** and press **Enter**. Continue pressing **Enter** until you have finished all fields.

Step 7 Repeat this procedure if more than one port group uses NSF codes.

Step 8 Type **x** and press **Enter** to exit the "port" command utility.

Note Customers might have spans going to different carriers. In this case, each carrier may require different NSF codes. To resolve this, you can assign the ports from one carrier to one port group and the ports from a different carrier to a different port group. You must configure the port groups to use different protocol parameter tables, and configure each port group's associated protocol parameter table with the NSF codes that the port group's carrier requires.

Restarting the system

The system needs to be restarted for these changes to be activated. For more information about the "restart" command, see the "restart" section on page A-51.

Step 1 At the tech$ prompt, type **restart** and press **Enter**.

Step 2 Wait for the system to come back up and proceed to the next section.

Testing NSF codes

To test if the NSF codes you entered are working correctly, follow this procedure using the "activity" command. For more information, see the "activity" section on page A-4.

Step 1 At the tech$ prompt, type **activity** and press **Enter**. Figure D-7 appears.

Figure D-7 activity Command Menu

```
meetingplace:tech$ activity
VUI Configuration: 1152 Sessions, 1200 Confs

 ***    VUI INTERNAL STATUS  UTILITY    ***

DebugMenu:
 1) Quick Status of all Ports            4) Make Test Call
 2) Verbose Status of Port Range         5) Show All Confs
 3) Display complete Port Information    0) Quit
Enter the Command   (0 -- 100):
```

Step 2 To make a test call, type **4** and press **Enter**. A prompt appears as in Figure D-8 requesting a destination telephone number.

Figure D-8 activity Command — Make a Test Call

```
meetingplace:tech$ activity
VUI Configuration: 1152 Sessions, 1200 Confs

 ***    VUI INTERNAL STATUS  UTILITY    ***

DebugMenu:
 1) Quick Status of all Ports            4) Make Test Call
 2) Verbose Status of Port Range         5) Show All Confs
 3) Display complete Port Information    0) Quit
Enter the Command   (0 -- 100): 4
You entered 4.
Enter destination for your call:
```

Step 3 Enter a nearby telephone number to call and press **Enter**. A prompt asks if you want specific ports.

Step 4 Enter **t** for true and press **Enter**. A prompt asks if you want to specify a range of ports.

Step 5 Enter **f** for false and press **Enter**. A prompt asks for the port number.

Step 6 Enter a port number that is configured to use NSF codes and press **Enter**.

If the call goes through, the NSF codes are correct.

If the call does not go through, retrace the steps in this appendix and verify everything was done correctly. If it still does not work, contact the Cisco TAC.

Step 7 Type **0** and press **Enter** to exit the "activity" command utility.

Note There is a trace utility called "acsetrace" that can be used to troubleshoot outdial problems.

Installation Checklists

This appendix includes the following checklists:

- pre-installation checklist ("Pre-installation checklist" section on page E-1)
- installation checklist ("Installation checklist" section on page E-1)
- post-installation checklist ("Post-installation checklist" section on page E-3)

Use these checklists when installing the MeetingPlace Audio Server 5.2 for the 8112 server.

Pre-installation checklist

Complete this checklist before beginning any installation.

Table E-1 Pre-installation Checklist

X	Procedure	Section and page
	Verify you have the tools necessary.	Appendix B, "Required Toolkit"
	Verify environmental requirements.	"Environmental requirements" section on page 3-2
	Verify power requirements.	"Power requirements" section on page 3-2
	Verify T1 digital trunk requirements.	"T1 digital trunk requirements" section on page 3-3
	Verify E1 digital trunk requirements.	"E1 digital trunk requirements" section on page 3-6
	Verify service modem requirements.	"Modem requirements" section on page 3-7
	Verify LAN connection requirements.	"LAN requirements" section on page 3-8

Installation checklist

The items in Table E-2 should be completed during the installation and configuration process. They should be completed after all items in Table E-1 have been completed, and before any items in Table E-3 are started.

Table E-2 Installation Checklist

X	Procedure	Section and Page
	Remove the shipping material.	"Removing the shipping material" section on page 3-10
	Inspect the server for damage.	"Inspecting for damage" section on page 3-12
	Verify the contents of the boxes.	"Verifying the contents of the boxes" section on page 3-12
	Mount the server.	"Mounting the 8112 server" section on page 3-13
	Mount the breakout box (if necessary).	"Mounting a breakout box" section on page 3-16
	Connect the power cable.	"Connecting the power cable" section on page 3-18
	Connect the SCSI cable.	"Connecting the SCSI cable" section on page 3-19
	Connect the LAN cable to the CPU.	"Connecting the LAN cable to the CPU" section on page 3-22
	Connect T1 digital trunks (for T1 CAS systems).	"Connecting telephony cables for a T1 CAS system" section on page 3-23
	Connect E1/T1 PRI digital trunks.	"Connecting telephony cables for E1 and T1 PRI systems" section on page 3-24
	Connect trunks for IP systems (if necessary).	"Connecting telephony cables for pure IP systems" section on page 3-33
	Connect the modem.	"Installing and connecting the modem" section on page 3-40
	Connect your laptop.	"Connecting your laptop" section on page 4-1
	Set up your laptop.	"Setting up your laptop" section on page 4-3
	Power up the server.	"Powering up the server" section on page 4-17
	Configure the LAN parameters.	"Configuring the LAN parameters" section on page 4-19
	Configure the server's time zone.	"Configuring the server's time zone" section on page 4-24

Table E-2 Installation Checklist (continued)

X	Procedure	Section and Page
	Configure blades.	"Configuring blades" section on page 4-26
	Configure T1 spans for T1 CAS, if necessary.	"Configuring spans for a T1 CAS system" section on page 4-29
	Configure T1 spans for T1 PRI, if necessary.	"Configuring T1 spans for a T1 PRI system" section on page 4-41
	Configure E1 spans, if necessary.	"Configuring spans for an E1 system" section on page 4-55
	Configure the system's date and time.	"Configuring the system's date and time" section on page 4-81
	Use MeetingTime to configure ports.	"Using MeetingTime to configure ports" section on page 4-84

Post-installation checklist

Complete this checklist after the system installation and configuration is complete.

Table E-3 Post-installation Checklist

X	Procedure	Section and Page
	Test telephony.	"Testing T1 telephony" section on page 4-96 and "Testing E1 telephony" section on page 4-99
	Test scheduling.	"Testing scheduling" section on page 4-101
	Test conferencing.	"Testing conferencing" section on page 4-102
	Test network latency.	"Testing network latency" section on page 4-103

Acronyms

ACTI	Audio Codes Trunk Interface
AMI	Alternate Mark Inversion
B8ZS	Binary 8 Zero Substitution
BFCV	Binary Facility Coding Value
BTU	British Thermal Unit
CAS	Channel Associated Signaling, also referred to as CT1 or CE
CCS	Common Channel Signaling
CIC	Carrier Identification Code
CLI	Command Line Interface
COM	communication
CPU	Central Processing Unit
CRC4	Cyclic Redundancy Check 4 (bit)
CRC6	Cyclic Redundancy Check 6 (bit)
CSU	Channel Service Unit
D4	The fourth generation channel bank (the interface between the T1 and an analog premises device such as an analog PBX)
DCD	Data Carrier Detect
DNIS	Dialed Number Identification Service
DNS	Domain Name Server
DPNSS	Digital Private Network Signaling System
DSCP	Differentiated Services Code Point
DSR	Data Set Ready
DTI	Digital Trunk Interface
DTMF	Dual-tone Multi-frequency
E1	A digital transmission link with capacity 2.048 Mbps
E&M Wink Start	A trunking arrangement for two way switch-to-switch or switch-to-network connections
EIA	Electronic Industries Alliance

EISA	Extended Industry Standard Architecture
EMC	Electromagnetic Compatibility
ESF	Extended Superframe
Euro ISDN	European implementation of ISDN
FCC	Federal Communications Commission
FTP	File Transfer Protocol
FRU	Field-replaceable Unit
GMT	Greenwich Mean Time
HDB3	High Density Bipolar 3 code
ICMP	Internet Control Message Protocol
IP	Internet Protocol
ISDN	Integrated Services Digital Network
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LED	Light Emitting Diode
MA-4	Multi Access Blade 4
MA-16	Multi Access Blade 16
MAC	Media Access Control
MSC	Master Switch Controller
MVIP	Multi-vendor Integration Protocol
NEBS	Network Equipment Building System
NIU	Network Interface Unit
NSF	Network Specific Facility
NTP	Network Time Protocol
PBX	Private Branch Exchange
PCI	Peripheral Component Interconnect
PRC	Port Resource Card
PRI	Primary Rate Interface
PSTN	Public Switch Telephone Network
QoS	Quality of Service
QSIG	An inter-PBX signaling system based upon a “Q” signaling reference point between two PBXs
RAS	Registration, Admission, and Status
SCSI	Small Computer System Interface
SDN	Software Defined Network
SID	Service Identifier
SSH	Secure Shell
T1	A digital transmission link with a capacity of 1,544 Mbps

TCP	Transmission Control Protocol
telco	telephone company
TM	Transition Module
ToS	Type of Service
TSAP	Transport Service Access Point
UDP	Universal Data Protocol
UPS	Uninterruptible Power Supply
VoIP	Voice-over Internet Protocol
VUI	Voice User Interface
WAN	Wide Area Network

Glossary

The following definitions apply to terms used in this document. Refer to Appendix F, "Acronyms" for a list of acronyms.

Numerics

8112 server A version of the MeetingPlace Audio Server platform that's capable of supporting up to 1152 connections.

A

Audio Server *See* MeetingPlace Audio Server.

B

breakout box A hardware component that provides a standard RJ-45 telephony interface for E1/T1 PRI systems.

C

Channel Service Unit *See* CSU.

CODEC COder-DECoder. A device that encodes or decodes a signal and used typically for converting analog to digital or compressing digital information into more efficient formats. In IP, *codec* refers to any technology for compressing and decompressing data.

CSU Channel Service Unit. A device used to connect a digital phone line from the phone company into network access equipment located on a customer's premises. A CSU may also be built into the network interface of the network access equipment.

D

DNS Domain Name Server. An Internet service that translates domain names into IP addresses.

domain name The portion of a symbolic name that corresponds to the network number in the IP address. In the symbolic name *name@mycompany.com*, the domain name is *mycompany.com*.

Domain Name Server *See* DNS.

DTMF Dual Tone Multi-Frequency. A signaling method that allocates a specific pair of frequencies to each key on a touch-tone telephone. DTMF makes it possible to use the telephone keys for UI input.

Dual Tone Multi-Frequency *See* DTMF.

dynamic IP The process of assigning an IP address to a caller from an IP address pool.

E

E1 line A 2.048-Mbps line that supports 32 64-Kbps channels, each of which can transmit and receive data or digitized voice.

EISA Enhanced Industry Standard Architecture. A type of high-speed IBM PC data bus.

Enhanced Industry Standard Architecture *See* EISA.

Ethernet A LAN that connects devices like computers, printers, and terminals. Ethernet operates over twisted-pair or coaxial cable at speeds at 10 or 100 Mbps.

Euro ISDN line European Integrated Services Digital Network line, which uses 30 B channels for user data, 164 kbps D channel for ISDN D-channel signaling, and one framing channel. The B channels can be all switched, all nailed up (private lines), or a combination of switched and nailed up. This line is standard in Europe and Asia, called CEPT G.703.

F

flex field A customizable field used by organizations to track additional profile or meeting information.

frame relay A form of packet switching that uses smaller packets and less error checking than traditional forms of packet switching (such as X.25). Frame relay is now an international standard for efficiently handling high-speed, bursty data (information transferred in spurts with long intervals of silence) over wide area networks.

G

gateway An application that connects the core application components of MeetingPlace to existing applications. Microsoft Outlook, Lotus Notes, Directory Services, IP, and Instant Messaging are examples of applications for which a gateway exists.

H

H.323 A standard that specifies the components, protocols, and procedures for multimedia communications services: real-time audio, video, and data communications over IP-based networks. H.323 is an umbrella recommendation from the International Telecommunications Union (ITU) that sets standards for multimedia communications over Local Area Networks (LANs) that do not provide a guaranteed quality of service.

HTML HyperText Markup Language. The authoring language used to create hypertext documents for the World Wide Web. Like the Standard Generalized Markup Language (SGML), on which it is based, HTML identifies the types of information in a document rather than the exact way it is to be presented. The presentation is left to the software that converts the contents to a suitable format for viewing.

HTTP HyperText Transfer Protocol. The application protocol for moving hypertext files across the Internet. This protocol requires an HTTP client program on one end of a connection and an HTTP server program on the other.

hunt group In telephony, a group of channels that share the same phone number. When a call comes in using the phone number assigned to the hunt group, the switch hunts for an available channel in the group.

Hypertext Markup Language *See* HTML.

Hypertext Transfer Protocol *See* HTTP.

I

IP address An address that uniquely identifies each host on a network or Internet.

IP subnet A number appended to the IP address to subdivide a network into smaller networks. IP subnets allow for more computers on a network with a single IP address. For example, 195.112.56.75/14, 195.112.56.75/15, and 195.112.56.75/16 are all IP addresses with subnets of 14, 15, and 16.

IP Telephony IP telephony allows users to make phone calls over the Internet, intranets, or private LANs and WANs that use the TCP/IP protocol.

L

LAN Local Area Network. A digital network that operates in a limited geographical area, usually a single company location or campus. Communication within a LAN is not usually subjected to external regulations.

latency The time between initiating a request for data and the beginning of the actual data transfer. Network latency is the delay introduced when a packet is momentarily stored, analyzed, and then forwarded.

LDAP Lightweight Directory Access Protocol. A standard protocol that enables users to locate organizations, individuals, and other resources, such as files and devices in a network, on the Internet or an intranet.

Lightweight Directory Access Protocol *See* LDAP.

Local Area Network *See* LAN.

logging The process of saving information about application activities.

M

Master Switch Controller *See* MSC.

MeetingPlace An integrated rich-media conferencing solution that allows users in different locations to communicate and share information.

MeetingPlace Audio Server The MeetingPlace audio bridge used to provide the audio portion of a meeting to interactive participants.

MeetingPlace site All the servers, regardless of number or type, at one physical location.

MeetingTime A Windows-based software application that allows select users to access advanced MeetingPlace functions and system administration tools.

MSC Master Switch Controller. The MSC acts as the controller for the Multi-vendor Integration Protocol (MVIP) bus and performs the bridging for timeslots. It is responsible for all conference related functions such as conference set up, tear down, conference recording, and conference prompt playback.

Multi Access Blade A Cisco Systems' proprietary, high-performance conference card that includes the necessary trunk interface functionality for T1 ISDN-PRI, IP, and Euro ISDN digital telephony.

multi-site system A MeetingPlace system with servers in multiple physical locations.

O

outdial A MeetingPlace feature that enables the system to initiate an audio connection with a person currently not in the meeting.

P

packet A block of information sometimes called a cell, frame, data unit, server unit, or signaling unit. Although each of these elements has unique attributes, in essence, all are packets.

packet switching Sending data in packets through a network to a remote location and reassembling the packets in the correct order at their destination.

PBX Private Branch Exchange. A private switching system, usually serving an organization, such as a business or a government agency, and usually located on the customer's premises.

platform The hardware on which the software runs.

port The connection between MeetingPlace Audio Server hardware and the telephone and/or IP network.

port group A configuration parameter used to define signaling information for multiple ports simultaneously.

Port Resource Card *See* PRC.

PRC The part of the Smart Blade responsible for managing all port related functions including dual-tone multi frequency (DTMF) detection, DTMF suppression, echo cancellation, speech detection, voice recording and recording for individual ports.

PRI An integrated services digital network (ISDN) interface standard that is designated in North America as having a 23B+D channels, in which all circuit-switched B channels operate at 64 Kbs, and in which the D channel also operates at 64 Kbs.

Primary Rate Interface *See* PRI.

Private Branch Exchange *See* PBX.

PSTN Public Switched Telephony Network. The international telephone system based on copper wires that carries analog voice data. This is in contrast to telephone networks based on digital technologies, such as ISDN.

Public Switched Telephony Network *See* PSTN.

R

reservationless meeting A special case of the immediate meeting. Each profile user is assigned a unique ID, which is the same for all reservationless meetings.

RJ-45 connector Registered Jack-45. A telephone connector that holds up to eight wires. RJ-45 plugs and sockets are used in Ethernet and Token Ring devices.

S

shadow server A standard MeetingPlace Audio Server that is assigned as a backup to the primary MeetingPlace Audio Server. In the case of a system failure, the shadow server takes over as the primary MeetingPlace Audio Server.

site contact Customer personnel with sufficient information to support the MeetingPlace installation who is allowed to contact Cisco TAC support.

Smart Blade Cisco Systems' proprietary conferencing card that holds the application software for audio conferencing functionality.

span A multiple signal transmission line which typically runs between telephony switching systems.

standalone system One or more MeetingPlace servers (of any type) that are connected to provide a complete multi-media solution.

system One or more MeetingPlace servers (of any type) that are connected.

system manager A user class. Customer personnel who have sufficient information and training to support MeetingPlace installation and respond to future calls relating to MeetingPlace maintenance.

T

T1 A digital transmission link with a capacity of 1.544 Mbit/s, used in North America. Typically channelized into 24 DS0s, each is capable of carrying a single voice conversation or data stream. Uses two pairs of twisted pair wires.

T1 Smart Blade Cisco System's proprietary conferencing card enhanced with T1 PSTN connectivity. A T1 Smart Blade is required to provide physical connectivity to a T1 telephone network.

TCP/IP Transmission Control Protocol/Internet Protocol. An open network standard that defines how devices from different manufacturers communicate with each other over interconnected networks. TCP/IP protocols are the foundation of the Internet.

time zone The temporal equivalent of a geographical location in terms of Greenwich Mean Time (GMT). In MeetingPlace each profile has a time zone setting, which should be set to reflect the office location where the user regularly does business.

Transmission Control Protocol/Internet Protocol *See* TCP/IP.

trunk In telephony communications, the circuit between two telephony nodes.

twisted pair Relatively low-speed transmission medium consisting of two insulated wires, shielded or unshielded, in regular spiral patterns. The wires are twisted around each other to minimize interference from other twisted pairs in the cable. Twisted pair is common in telephone wiring and is increasingly common in data networks. Other high-speed forms of cable include coaxial and fiber optic cables.

V

Voice over Internet protocol *See* VoIP.

VoIP Voice over Internet Protocol. A set of facilities for managing the delivery of voice information using IP. Voice information is sent in digital form in discrete packets over the Internet instead of in analog form over PSTN. A major advantage of VoIP is that it avoids the tolls charged by ordinary telephone service.

W

WAN Wide Area Network. A data network typically extending a LAN outside a building or beyond a campus, over IXC or LEC lines to link to other LANs at remote sites. Typically created by using bridges or routers to connect geographically separated LANs.

Wide Area Network *See* WAN.

Symbols

Numerics

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W