MITEL

3300 Integrated Communications Platform

TECHNICIAN'S HANDBOOK

Release 7.0

MITEL | it's about YOU

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

Trademarks

Mitel, SX-2000, SUPERCONSOLE 1000, and SUPERSET are trademarks of Mitel Networks Corporation.

Windows is a trademark of Microsoft Corporation.
Cisco is a trademark of Cisco Systems, Inc.
VT100 is a trademark of Digital Equipment Corporation.
Java is a trademark of Sun Microsystems Incorporated.

Other product names mentioned in this document may be trademarks of their respective companies and are hereby acknowledged.

3300 Integrated Communications Platform
Technician's Handbook
Release 7.0
51009611, Rev. A
May 2006

Chapter 1 : Introduction

Chapter 2 : Installation

Chapter 3 : Software Procedures

Chapter 4 : Upgrades and FRUs

Chapter 5 : Troubleshooting

Chapter 6 : Maintenance

Appendix A : Hardware Reference

Appendix B : Installation Planner

Appendix C : Typical Network Configurations

Appendix D : Status LEDs

Appendix E : FRU Part Numbers

Appendix F : System Capacity and Parameters

Chapter 1
Introduction

Purpose of this Handbook

This handbook provides instructions to install, upgrade, maintain and troubleshoot the Mitel® 3300 Integrated Communications Platform (ICP). This handbook is written for certified 3300 ICP technicians. For information on programming tasks, please refer to the System Administration Tool Help system.

Symbols Used in the Handbook

Tip: Provides additional information you should know about a topic.

Time: Indicates the time it takes to complete a procedure.

CAUTION: Indicates a potentially hazardous situation that could result in damage to the equipment.

WARNING: INDICATES A HAZARDOUS SITUATION THAT COULD RESULT IN INJURY OR DEATH.

Safety Instructions

A printable version of the Safety Instructions is available on the Mitel Customer Documentation web site.

CAUTION: Failure to follow all instructions may result in improper equipment operation and/or risk of electrical shock. Refer to "3300 Safety Instructions" for complete safety information.

CAUTION: To prevent ESD damage to the equipment: (1) Ensure that the system is grounded before you install a card. (2) Whenever you handle cards, wear an anti-static strap (attached to the cabinet). (3) When removing cards from the cabinet, immediately place them in an anti-static bag.

Note: The ground symbol within a circle identifies the terminal to be connected to an external protective conductor. Connect this terminal to earth ground before you make any other connections to the equipment.

Start Here Guide

What You Received

- ❒ Options sheet with password from Mitel OnLine (see page 11)
- ❒ 3300 ICP Controller
- ❒ Hard drive
- ❒ System ID module or System i-Button
- ❒ Software CD-ROM
- ❒ NSU, ASU (optional)
- ❒ Set of feet, rack ears, and screws for each unit
- ❒ Review your purchase order for other, optional, components.

Installation Tools and Equipment

- ❒ Installation Planner (Appendix B on page 295)
- ❒ Typical Network Configurations (Appendix C on page 317)
- ❒ Computer for programming the 3300 ICP
- ❒ CAT 5 or better Cable with RJ-45 connector
- ❒ IP addresses for the controller, E2T, and IP telephones
- ❒ List of purchased options and password
- ❒ IMAT (not required if you have Embedded PRI)
- ❒ Phillips screwdrivers
- ❒ Static strap.

Installation Checklist

- ❒ Obtain your options and password from Mitel OnLine
- ❒ Complete the Installation Planner Appendix (see page 295)
- ❒ Install controller hardware (see page 15)
- ❒ Connect maintenance PC to Controller (see page 22)
- ❒ Power up the Controller (see page 22)
- ❒ Launch the System Administration Tool (see page 8)
- ❒ Program the License and Options Selection (see page 25)
- ❒ Perform a DBMS Save (see page 25)
- ❒ Set the Date and Time (see page 26)
- ❒ Program the Controller modules (see page 26)
- ❒ Establish an Ethernet connection to the Controller (see page 27)
- ❒ Set the Controller RTC IP address (see page 28)
- ❒ Program the DHCP server (see page 29)
- ❒ Configure the Layer 2 switch (see page 35)
- ❒ Install NSU, ASU, Peripheral Cabinet, DSU, SUPERSET™ Hub (page 36)
- ❒ Program Units and Modules (follows each installation procedure)
- ❒ Install Telephones (see page 51)
- ❒ Register IP Devices (see page 52)
- ❒ Program Telephones (see page 54)
- ❒ Install a DNIC Music on Hold /Paging Unit (see page 57)
- ❒ Program Trunks (see System Administration Tool OnLine Help)
- ❒ Program Automatic Route Selection (see OnLine Help)
- ❒ Program Voice Mail (see OnLine Help)
- ❒ Program Paging (see OnLine Help)
- ❒ Program Music on Hold (see OnLine Help)
- ❒ Program Automatic Call Distribution (see OnLine Help)
- ❒ Program Hotel/Motel (see OnLine Help)
- ❒ Perform a DBMS Save (see page 25)

About the 3300 ICP

The 3300 ICP is a Voice over IP solution that delivers voice capabilities and features to the enterprise. There are several system configurations: the 100-user system; the MX with embedded analog, that can support 200 users; the CX and the CXi with embedded analog and embedded Layer2 switch for sites with an 8-64 line size; the MXe base with embedded analog that can support 200 users before expansion; and the LX that can support 700 users (with 256 MB RTC memory) or 1400 users (with 512 MB RTC memory from Release 6.0).

Programming Tools

The system includes a number of programming tools:

- **Embedded System Management (ESM)** consists of:
  - **System Administration Tool** that provides a Web-based interface that trained technicians use to program the system.
  - **Group Administration Tool** that provides a Web-based interface to enable administrators to make changes to user information.
  - **Desktop Tool** that provides a Web-based interface to enable display IP telephone users to program feature keys on their phone.
- **Configuration Wizard**, introduced with Release 7.0, allows you to customize initial system programming. After you specify the system setup, you can save the details for future use or apply the changes to the 3300 ICP.
- **ISDN Maintenance and Administration Tool** (**IMAT**) provides the programming interface for PRI and R2 protocols delivered via an NSU or DSU. Embedded PRI via the Dual T1/E1 Framer is programmed though the System Administration Tool.
- **ICP Software Installer Tool** expedites the distribution of 3300 ICP software by eliminating a number of interactive steps (see page 69). The tool restores saved databases and, from Release 7.0 UR1, enables databases from legacy SX-2000® LIGHT, SX-2000 MicroLIGHT, 3200 ICP, and 3800 WAG systems to migrate to the 3300 ICP. The Software Installer Tool replaces the Configuration Tool.
- **Configuration Tool** restores saved databases and enables legacy SX-2000® LIGHT, SX-2000 MicroLIGHT, 3200 ICP, and 3800 WAG systems to migrate to the 3300 ICP.

- **IP Phone Analyzer** collects performance information about the IP devices connected to the 3300 ICP. You can use one PC to monitor the debug and status information of IP phones (see page 248).
- **OPS Manager** enables you to control the maintenance and operation of a network of elements. With OPS Manager, you can, for example, manage a network telephone directory, schedule move, add, change, and delete user operations, and integrate the network telephone directory with a directory service database.

Application Management Center (AMC)

The online licensing process, managed by the Mitel Application Management Centre (AMC) allows Solution Providers who have accounts on the AMC to manage software licenses online. Each company is able to supply customers instantly if new licenses are required. Refer to “Requirements for AMC Connection” on page 23 for Software Installer Tool and 3300 ICP system networking requirements.

Installation/Maintenance Computer

You need a Windows-based computer to program, maintain and troubleshoot the 3300 ICP, and to install/upgrade 3300 ICP software.

Computer Recommendations

- Windows® NT 4.0, Windows 2000, or Windows XP

Computer Requirements

- Windows 98, Windows NT 4.0, Windows 2000, or Windows XP
- Network interface card (NIC)
- 525 MB free disk space (minimum)
- Internet Explorer 6.0 with the latest Service Pack and 128-bit encryption
- VT100™ emulator program
- FTP server (can be installed with Microsoft® IIS or PWS, for example)

Tip: Windows 98 with PWS does NOT include an FTP server application, and will not work for the software installation/upgrade process unless a third-party server application is used.

Launching the Programming Tools

Embedded System Management Tools

To log into one of the ESM tools:

1. Launch a browser and go to the URL of the 3300 Controller - https://<hostname>/main.htm (<hostname> is the name or IP address assigned to the Controller if no DNS is available). Refer to "Setting the Controller RTC IP address (for Release 6.0 and later)" on page 27 or "Setting the Controller RTC IP address (prior to Release 6.0)" on page 28.
2. The first time you connect, you must install the Mitel Root CA security certificate (see "Secure Sockets Layer (SSL) and Security Certificate" on page 236).
3. Log into the 3300 ICP ESM using the default username (**system**) and password (**password**).

Tip: To prevent unauthorized use, change the username and password the first time you log in.

4. Click the desired Tool (Desktop, Group Administration, or System Administration).
5. You will be prompted to install some XML Components when you log into the System Administration Tool for the first time. At the following prompt, "Do you wish to install or upgrade the required XML components?", click "Install Now". The install takes less than 30 seconds and you do not need to restart your computer.

Tip: Your PC must have the same subnet address as the RTC IP (for example, 192.168.1.x) to launch ESM.

The system will allow up to 5 System Administration Tool users, 5 Group Administration Tool users, and 10 Desktop Tool users at one time.

The System Administration Tool will temporarily lock you out for 15 minutes after three consecutive attempts to log in have failed.

ISDN Maintenance and Administration Tool

To launch IMAT on the Installation/Maintenance PC:

- On the **Start** menu, point to **Programs**, and click **IMAT**.

Software Installer Tool

To launch the Software Installer Tool:

- On the **Start** menu, point to **Programs**, and click **Mitel 3300 ICP Software Installer Tool**.

IP Phone Analyzer

To launch the IP Phone Analyzer:

- On the **Start** menu, point to **Programs**, and click **Mitel IP Phone Analyzer** (see page 248 for details).

3300 ICP Documentation

The 3300 ICP documentation set includes the following components:

- Printed documents (also available on Mitel OnLine)
  - General Information Guide
  - Technician's Handbook
  - Safety Instructions
- Documents on Mitel OnLine
  - Hardware Technical Reference Manual
  - System Administration Tool Help
  - Voice Clustering (Portable Directory Number)
  - Resiliency
  - IP Phone Analyzer Online Help
  - Software Installer Tool Help
  - IP-DECT Wireless Solution Documentation
  - CITELlink Gateway Documentation
  - Symbol NetVision MiNET Phone Installation and Programming Instructions
  - SpectraLink Documentation
  - Engineering Guidelines
  - Telephone, Attendant, and Voice Mail User Guides
  - 6000 Managed Application Server (MAS) Documentation

- Online Help
  - System Administration Tool Online Help
  - Group Administration Tool Embedded Help
  - Desktop Tool Embedded Help
  - IMAT Online Help
  - IP Phone Analyzer Online Help
  - Software Installer Tool Online Help
  - OPS Manager Online Help

Tip: In the software application (System Administration Tool, IMAT, etc.), click the **Help** link or button to access the tool's Online Help.

- Knowledge Base Articles on Mitel OnLine
  - Technical Bulletin
  - How-To Guide
  - Troubleshooting Guide
  - Known Product Issue
  - Release Notes
  - Program Information.

Mitel OnLine

You can access Mitel OnLine from the **www.mitel.com** Web site.

Tip: You must be a registered user to access Mitel OnLine.

Access Product and Technical Documentation

1. Log into **Mitel OnLine**.
2. Click **Technical Support**.
3. Click **Product Documentation** for Technical Documents, User Guides, and Installation Guides.
   -OR-
   Click **Knowledge Base** for TBs and RNs.

Tip: To view a document, click on the name of the document. To download a document, right-click on the name of the document and select Save Target As.

Create Telephone User Guides with ManualMaker

1. Log into **Mitel OnLine**.
2. Click **Technical Support** and then click **Product Documentation**.
3. Click **ManualMaker**.
4. Click the **Help** button for instructions on creating User Guides with ManualMaker.

Access Your Mitel Options Password

You must obtain your Mitel Options Password through Mitel OnLine (www.mitel.com). This password is required during a software upgrade or installation procedure, so you MUST keep a proper record of it. A new password is issued to you if you are purchasing new options. Before attempting to upgrade software, to confirm a current password or to purchase new options and receive a new password, call Mitel Customer Service during normal business hours.

Contacting Mitel

Sending Feedback

If you have suggestions on how to improve this documentation, please contact us at **techpubs@mitel.com**.

Order Desk

You can reach the Order Desk at 1-800-796-4835.

Repair Department

You must get a Return of Merchandise Authorization (RMA) form from the Repairs Department before sending equipment back to Mitel.

You can reach the Repairs Department at 1-888-222-6483.

Technical Support

Please contact Mitel Technical Support if you require technical assistance.

If you cannot resolve the problem by using the Troubleshooting chapter (page 165), please collect the required information listed in the applicable section(s) of the Troubleshooting chapter **before** calling Mitel Technical Support.

You can reach Technical Support at 1-800-561-0860 or 1-613-592-2122.

Chapter 2
Installation

Install Controller Components

This chapter contains instructions on how to install a 3300 ICP. For information on upgrading and replacing components, see page 104.

In the following illustrations, the components listed in **bold** text are installed in the factory (Release 7.0 and later). If you receive a CX/CXi/MXe and those identified components are not installed, refer to Chapter 4 on page 95 for installation instructions.

Tip: In the following illustrations, T1/E1 refers to Dual T1/E1 or T1/E1 Combo, with exception of the CX/CXi controllers which support only the Combo.

<table>
<tr><td rowspan="3">Power Supply</td><td>Slot 8
DSP</td><td>Slot 7
DSP</td><td>Slot 6
Echo Canceller or DSP</td><td>Slot 5
Echo Canceller</td></tr>
<tr><td>SysID</td><td colspan="3"></td></tr>
<tr><td>Slot 1
FIM, T1/E1, or BRI</td><td>Slot 2
FIM, T1/E1, or BRI</td><td>Slot 3
FIM, DSP, T1/E1, or BRI</td><td>Slot 4
FIM, DSP</td></tr>
</table>

Figure 1: Slot Locations for the LX, 250, and 700-User Controllers

<table>
<tr><td>Power Supply</td><td colspan="2">Analog Main Board
Analog Option Board
(optional, installed on AMB)</td><td>Hard Drive</td></tr>
<tr><td></td><td colspan="2">Clock Module</td><td>SysID</td></tr>
<tr><td>Slot 1
FIM, T1/E1, or BRI</td><td>Slot 2
FIM, DSP, T1/E1, BRI</td><td>Slot 3
DSP, T1/E1, or BRI</td><td>Slot 4
DSP</td></tr>
</table>

Figure 2: Slot Locations for the MX Controller

<table>
<tr><td>Hard Drive
or RAID</td><td colspan="2">Analog Main Board</td><td>PSU 2</td><td colspan="2">PSU 1</td></tr>
<tr><td colspan="2">Clock Module</td><td colspan="2" rowspan="2">Slot 5
DSP or Echo Canceller</td><td>i-Button</td><td></td></tr>
<tr><td colspan="2">Slot 6
DSP or Echo Canceller</td><td colspan="2"></td></tr>
<tr><td>Slot 1
FIM, T1/E1, BRI</td><td>Slot 2
FIM, T1/E1, BRI</td><td>Slot 3
FIM, DSP, T1/E1, BRI</td><td>Slot 4
FIM, DSP, T1/E1, BRI</td><td colspan="2"></td></tr>
</table>

Figure 3: Slot Locations for the MXe Controller

<table>
<tr><td>Hard Drive</td><td>Power Supply</td><td colspan="2">Analog Main Board
Analog Option Board
(optional)</td></tr>
<tr><td></td><td colspan="2">Clock Module</td><td>i-Button</td></tr>
<tr><td>Slot 1
Combo (T1/E1, DSP, Echo), BRI</td><td>Slot 2
Combo (T1/E1, DSP, Echo), BRI</td><td>Slot 3
DSP</td><td>16 Port Ethernet L2 Switch</td></tr>
</table>

Figure 4: Slot Locations for the CXi Controller (with an Ethernet L2 Switch)

<table>
<tr><td>Hard Drive</td><td>Power Supply</td><td colspan="2">Analog Main Board
Analog Option Board
(both optional)</td></tr>
<tr><td></td><td colspan="2">Clock Module</td><td>i-Button</td></tr>
<tr><td>Slot 1
Combo (T1/E1, DSP, Echo), BRI</td><td>Slot 2
Combo (T1/E1, DSP, Echo), BRI</td><td>Slot 3
DSP</td><td></td></tr>
</table>

Figure 5: Slot Locations for the CX Controller (without an Ethernet L2 Switch)

Power Supply		SysID		
	Slot 1 FIM, T1/E1, or BRI	**Slot 2** FIM, T1/E1, or BRI	**Slot 3** DSP or BRI	**Slot 4 DSP**

Figure 6: Slot Locations for 100-User Controller

Read the Safety Instructions before performing the procedures in this chapter (see “Safety Instructions” on page 3).

CAUTION: To prevent ESD damage to the equipment: (1) Ensure that the system is grounded before you install a card. (2) Whenever you handle cards, wear an anti-static strap (always attach the wrist strap from the cabinet).

Tip: Before installing a 3300 ICP, **always** read the RN for the software you are installing (see “3300 ICP Documentation” on page 9).

CAUTION: All installation, field replacement, and servicing procedures must be carried out by service personnel who have successfully completed the Mitel Installation and maintenance training course.

CAUTION: Provide a permanent ground for all controllers and units, through the ground connection on each cabinet.

- ❒ Connect the installation/maintenance PC to the Controller (page 22)
- ❒ Power up the Controller (see page 22)
- ❒ Launch the System Administration Tool (see page 8)
- ❒ Complete basic programming and Data Save (see page 25)
- ❒ Establish an Ethernet connection to the Controller (see page 27)
- ❒ Set the Controller RTC IP address (see page 28)
- ❒ Program the DHCP server (see page 29)
- ❒ Configure the Layer 2 switch (see page 35)
- ❒ Install the Units (see page 36)
- ❒ Install the Telephones and peripherals (see page 51)

Controller Component Options

Table 1: Controller Component and Upgrade Options

Processor speed	300[1]				450		266
Components	**100**	**250**	**700**	**MX**	**LX**	**MXe[5]**	**CX[4]**
CIM	√	√	√	√	√	√	—
FIM (page 104)	√	√	√	√	√	√	—
DSP (page 105)	√	√[2]	√[2]	√	√	√	√
T1/E1 (page 110)	√	√	√	√	√	√	—
BRI (page 110)	√	√	√	√	√	√	√
T1/E1 Combo (page 111)	√	√	√	√	√	√	√
AMB (page 136)	—	—	—	—	—	√	√
AOB (page 114)	—	—	—	—	—	—	√
AMB (page 134)	—	—	—	√	—	—	—
AOB (page 113)	—	—	—	√	—	—	—
Redundant Power Supply (page 123)	—	—	—	—	—	√	—
RAID controller (page 116)	—	—	—	—	—	√	—
E2T (page 123)	—	—	—	—	—	√	—
Upgrading to a 300 or 450 MHz Controller (page 102)	—	√	√	—	—	—	—
Upgrading to a 1400-User System	—	—	—	—	√[3]	√[6]	—

Note: 1. Requires 3300 ICP software version 3.2 or higher.
2. 64 compression channels requires a minimum 300 MHz controller.
3. Requires a controller with 512 MB of memory on the RTC (RIs 6.0 or later).
4. The CX only supports Release 6.0 or later software.
5. Release 7.0 and later software.
6. Requires the installation of a second processor, the E2T.
7. Refer to page 365 for component part numbers.

Hard Drive

CAUTION: If you move a programmed hard drive from one controller type to another (for example, an MX system to an LX or CX system), you MUST manually install the software (see page 77) and restore the database. A new hard drive purchased from Mitel is configured for installation in any system.

Tip: The CX/CXi/MXe controllers are shipped with the hard drive installed. If you receive a CX/CXi/MXe and the hard drive is not installed, refer to page 128 or page 131 for installation instructions.

LX, 100, 250 and 700-User Hard Drive

To install a new hard drive in a new LX/100/250/700-user controller:

1. Remove the controller from its packaging.
2. Remove the hard drive and attached backing plate from its packaging.
3. Locate the hard drive ribbon cable and power cable in the controller hard drive enclosure.
4. Cut and discard the tie wrap securing the cables to the controller stand-off post.
5. Connect the power and ribbon cables in the hard drive enclosure to the corresponding connectors on the hard drive.
6. Insert the hard drive.
7. Secure the plate to the controller using the 6 border screws provided with the hard drive.

MX Hard Drive

To install a new hard drive in a new MX controller:

1. Remove the controller and hard drive from their packaging.
2. Remove the top cover of the controller (see page 100).
3. Discard the backing plate that is shipped with the hard drive.
4. Locate the hard drive ribbon cable and power cable in the controller hard drive enclosure.

5. Connect the power and ribbon cables to the corresponding connectors on the hard drive.
6. Insert the hard drive.
7. Secure the hard drive to the controller using the screws provided.

System ID Module

Tip: The CX/CXi/MXe controllers are shipped with the **i-Button** installed. If you receive a CX/CXi/MXe and the i-Button is not installed, refer to page 133 for installation instructions.

To install a SysID module in a LX/MX/100/250/700-user controller:

1. Remove the System ID module from its packaging.
2. Remove the protective cover from the System ID module's connector.
3. Remove the controller cover (see page 99 or page 100).
4. Install the module connector in its mate on the controller.
   - 100-user controller: behind slot 2
   - MX controller: behind slot 4
   - LX and 250/700-User controller: between slots 1 and 8.
5. Secure the System ID module using the screw provided.

Other Controller Components

Refer to "Upgrades and FRUs" on page 95 for instructions to install additional controller components.

Mounting the MXe Controller

Tip: Mount the MXe in a rack without the hard drives and power supplies to reduce the weight.

To rack-mount the MXe:

1. Attach the mounting brackets to the MXe using the flat head screws provided.
2. Loosely install one frame mounting screw on each side of the frame:
   - in the bottom hole position of the space that the MXe will occupy.

- loosely enough that the frame mounting bracket can be dropped into position, resting on the screw thread (see Figure 7).

3. Position the MXe on the frame, resting the MXe mounting brackets on the frame mounting screw thread.
   - The MXe will rest on those screws while the remaining screws are installed.
4. Install two more screws on each side of the frame, in the 3rd and 6th hole positions.
5. Tighten all six of the mounting screws.

CAUTION: Remove the MXe from the rack in reverse order. Loosen the bottom screws before the other screws are removed.
Never turn the bottom screws while the rack is resting on them.

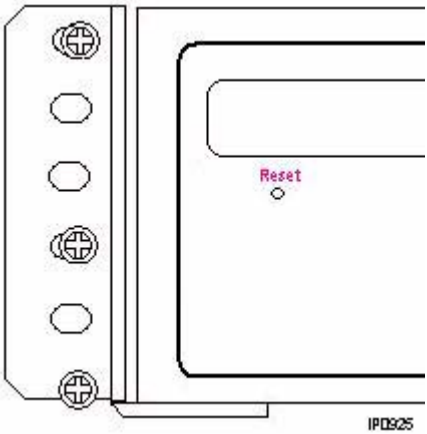


Figure 7: MXe Rack-mount Screw Placement

Connecting the Maintenance PC to the Controller

1. Connect an RS-232 straight DTE male to female serial cable between the controller's **Maintenance** port and the PC's serial port (cable not provided).
2. Program the PC's serial port (from the communication program) with the following settings:
   - Baud Rate: **9600**
   - Data Bits: **8**
   - Parity: **None**
   - Stop Bits: **1**
   - Flow Control: **None**
3. Connect a straight-through Ethernet cable (RJ-45) from the controller leftmost Ethernet port (port 17 on the CXi; port 1 on the MXe) and the PC's network interface card (NIC).
4. Program the PC's NIC with the following settings:
   - IP Address: **192.168.1.n** (where n is a value between 30 and 254)
   - Subnet Mask: **255.255.255.0**

Powering Up the Controller

1. Connect the female end of the power cable to the controller, and secure it with the latch (if provided).
2. Connect the other end of the power cable to a protected outlet. If necessary turn on power switch. The controller turns on.

Time: The controller can take up to 10-15 minutes to start-up.

Verify the Connections

Perform the steps below to verify the connections between the Maintenance PC and the controller.

1. To verify the serial connection, in the VT100 emulator, press ENTER.
   - If the serial connection is installed and programmed properly, a right-pointing arrow (→) is displayed when you press ENTER.
2. To verify the Ethernet connection, from the PC, PING the controller's RTC IP address (default is 192.168.1.2).
   - If the connection is installed and programmed correctly, the controller replies to the PING.

Requirements for AMC Connection

Connecting to the Application Management Center (AMC) Server requires specific settings for the Software Installer Tool and the 3300 System Administration Tool.

Software Installer (SI) Tool Requirements

The PC that is running the SI Tool has the following network requirements:

1. **DNS Name Resolution:** Because the SI win32sync client performs a name lookup on “register.mitel-amc.com”, the SI host PC needs to be properly configured for DNS name resolution.
2. **TCP/IP Source Port on the SI Host:** A Windows operating system will use an arbitrary high port for the TCP connection to the AMC. If the SI PC is behind a firewall, the firewall must allow connections from high ports (greater than 1024).
3. **TCP/IP Destination Port on the AMC:** The SI win32sync client will attempt to establish a connection to register.mitel-amc.com TCP port 22. After 5 seconds, if the connection is not established, the client will try port 8222. If there is still no success, the third attempt is with port 80 using the HTTP/1.1 protocol CONNECT method.
   If the SI PC is behind a firewall, the firewall must allow connection to at least one of port 22, port 8222, or port 8.
4. **SI Host PC behind an HTTP Proxy Server:** If the HTTP/1.1 CONNECT method is used and the SI PC is configured to use an HTTP proxy server, then the CONNECT request will be through the proxy server. This is the same method used by web browsers to establish HTTPS connections through proxy servers. If the SI host PC can reach https://www.mitel-amc.com from a web browser, then it should also be able to establish a win32sync connection by using the HTTP/1.1 CONNECT method. If there is a problem reaching https://www.mitel-amc.com from a browser on the SI host PC, then the firewall and/or proxy server on the customer premise may need to be reconfigured to allow HTTP/1.1 CONNECT requests.

3300 ICP System Requirements

1. **DNS Name Resolution:** Because the MiSync client performs a name lookup on “register.mitel-amc.com” and “sync.mitel-amc.com”, the ICP needs to be properly configured for DNS name resolution using the System IP Configuration form in the System Administration Tool.

2. **TCP/IP Source Port on the ICP:** The MiSync client will connect to TCP port 443 (https) on the AMC. If the ICP is behind a firewall, the firewall must allow TCP connections from the ICP to TCP port 443 on the AMC.
3. **ICP behind an HTTP Proxy Server:** The MiSync client uses HTTPS to communicate with the AMC. The HTTP/1.1 CONNECT method is the standard used by proxy servers to proxy HTTPS. There should be no extra configuration work required. See Step 4, "SI Host PC behind an HTTP Proxy Server" on page 23.
4. **CX/CXi/MXe-Specific WAN Considerations:** Program the Internet Gateway (WAN interface) IP address details (see "CXi/MXe Requirements for IP Networking" on page 297).

Basic Programming and Data Save

Programming the License and Option Selection Form

Tip: Installations and upgrades require a new purchased-options password from the Mitel Application Management Center (AMC). If you use the old password, an error message is displayed.

Tip: Before you make any changes to Configuration Options, after entering the Mitel Options Password and programming the database, ensure that you have a system backup.

To select licenses and options prior to software release 6.0:

1. Log into the System Administration Tool (see page 8).
2. Select the **License and Option Selection** form.
3. Click **Change** and fill in the fields as required (see your Mitel Options sheet). For more information, click **Help.**

Tip: When you **Change** and **Save** in the License and Option Selection form (prior to Release 7.0), an error message that references “sysid # 65535“ means that the SysID or i-Button is not installed or not seated correctly.

Tip: Enable **Networking Option** and **Mitai/Tapi Computer Integration**.

4. Enter the Mitel Options Password and click **Save**.

Time: The Save procedure takes approximately three minutes.

5. **Reboot** the controller (see page 99).

To manually select licenses and options for release 6.0 and later:

1. Access the **License and Option Selection** form.
2. Click **Change** and leave the **Application Record ID** field blank.
3. Enter the number of licenses in the appropriate fields.
4. Select the appropriate Country variant and Configuration Options.
5. Enter your Password.
6. Click **Save** to commit your changes to the database.
7. **Reboot** the controller (see page 99).

To automatically select licenses and options for release 6.0 and later:

1. Complete the **System IP Configuration** form to enable the Primary and Secondary DNS Servers to establish a connection with the Application Management Center (AMC) Server (see "Requirements for AMC Connection" on page 23).

Tip: The PC that is running the Software Installer Tool has networking requirements that must be met to establish a connection with the AMC. Refer to "Installing the Software Installer Tool" on page 69 for details.

2. Access the **License and Option Selection** form.
3. Click **Change** and enter your Application Record ID.
4. Click **Retrieve Licenses** to query the Application Management Center (AMC) and retrieve your Purchased Options and Password.
5. Select the appropriate Country variant and Configuration Options.
6. Click **Save** to commit your changes to the database and to the AMC.
7. **Reboot** the controller (see page 99).

Setting the Date and Time and Saving the Settings

Tip: The DBMS SAVE command will ensure that all future programming changes are saved. You must perform the DBMS SAVE command before the programmed internal DHCP server will run (see page 29 for DHCP programming instructions).

To set the system date and time:

1. Log into the System Administration Tool (see page 8).
2. In the **All forms (alphabetical)** list, click **Maintenance Commands**.
3. Enter **writedatetime <year> <month> <day> <day of the week> <hours> <mins> <seconds>** to set the date and time. For example, **writedatetime 2004 4 3 2 12 31 51** (2004 April 3rd Tuesday 12:31:51).
4. Perform a DBMS save using the **dbms save** maintenance command.
5. Enter the **dbms stat** command to verify the DBMS save.The system response is **DBMS info: DBMS_INITIALIZED is on**.

Programming the Controller Modules

1. Access the **Controller Module Configuration** form.
2. Highlight the module (slots 1 to 4) and click **Change**.

3. Select the module in the drop-down list. Choose Dual FIM, Dual Framer, Quad BRI Framer, or T1/E1 Combo.
4. If you have installed Framer or Combo modules, refer to “Program Embedded PRI/Q.SIG Trunks”, “Program T1/D4 Trunks”, or “Program Embedded BRI Trunks” in the Online Help for information.
5. Power down the controller (see page 99).

Connecting the Controller to the Network

This section assumes that the network is already set up, and that there is a serial connection between the Maintenance PC and the controller.

Tip: See Table 58, “T1 and E1 Connector Pin Allocation,” on page 270 for Embedded T1/E1 pinout information.

- Setting the Controller RTC IP address (prior to Release 6.0) (page 28).
- Programming DHCP (page 29)
- Verifying the Operation of the Controller (page 34).
- Configuring the Layer 2 Switch (page 35).

Setting the Controller RTC IP address (for Release 6.0 and later)

Tip: The Maintenance PC must be on the same subnet as the controller.

1. Launch a browser and go to the URL of the 3300 Controller (default RTC IP address is 192.168.1.2, default gateway 192.168.1.1).
2. The first time you connect, you must install the Mitel Root CA security certificate (see “Secure Sockets Layer (SSL) and Security Certificate” on page 236).
3. Log into the 3300 ICP ESM using the default username (**system**) and password (**password**).
4. Complete the IP Networking Configuration form to change the IP addresses.

Setting the Controller RTC IP address (prior to Release 6.0)

Tip: The Maintenance PC must be on the same subnet as the controller.

1. Start the communication program on the Maintenance PC.
2. Power up the controller (see page 22).
3. Press the **Reset** button on the controller (use a small non-metallic pointed object).
4. The communication program will instruct you to **Press <SPACE><SPACE><SPACE> to stop auto-boot AFTER countdown starts** (Release 5.2 and later) or **Press any key to stop auto-boot** (prior to Release 5.2).
5. When **[VxWorks Boot]:** is displayed, type **c** and press ENTER.
6. For each VxWorks setting shown in **bold** inTable 76 on page 300, enter a value, and then press ENTER. For all other settings, press ENTER to accept the default:

Tip: If DHCP (flags=0x40) is being used on the E2T, leave the inet on ethernet field blank.

- inet on ethernet (e), **IP address and subnet mask (hex) for controller RTC** (Get it from your IT administrator.)
- gateway inet (g), **IP address of the default gateway for the 3300** (must be outside the DHCP range)
- user (u), **ftp**
- ftp password (ftp)), **ftp**.

CAUTION: Do not use leading zeroes in the IP addresses. For example, enter 192.168.1.2; not 192.168.001.002.

7. At [VXWorks Boot], type @, or press the **Reset** button on the controller.

Time: The controller can take up to 10–15 minutes to restart.

Programming DHCP

Programming the Controller DHCP Server Settings (prior to RIs 7.0)

For additional information on programming DHCP settings for the 3300 ICP, refer to the System Administration Tool Online Help.

To use an external DHCP Server, do not enable the internal DHCP server and refer to “Configuring External DHCP Settings for E2T” on page 307 for instructions.

Tip: You may need to change the IP address of your PC to match your customers network.

1. On the Maintenance PC, access the System Administration Tool (see "Launching the Programming Tools" on page 8).
2. In the **All forms (alphabetical)** list, click **DHCP Subnet** form, enter the subnet name, IP address and bit mask.
3. In the **DHCP Static IP** form, enter a static IP address for the E2T using the information on page 301 (skip this step for the MX and 100-user controllers). Assign IP addresses to specific devices by using the MAC address of the device. Assign a static IP Address to any IP Console in a cluster.
4. In the **DHCP IP Address Range** form, program the scope using the information on page 301.

   Tip: The following IP addresses are reserved for the AMB and ASUs: 192.168.10.1 *to* 192.168.10.15 through 192.168.13.1 *to* 192.168.13.15

5. In the **DHCP Options** form, program the options listed in Table 78 on page 301 for the scope you just programmed. Always create the following options:

   - 3 Router, IP address
   - 66 TFTP Server, IP address format
   - 67 Boot file, string value (always /sysro/E2T8260)
   - 128 TFTP, IP address format (typically the controller)
   - 129 RTC, IP address format (typically the controller)
   - 130 MITEL IP PHONE, string value

   In a single DHCP configuration, create the following options:

   - 132 VLAN ID (optional)

- 133 Priority, integer value of 1-6 (Optional. Required if a voice VLAN is in use. For external server use Hex LONG; for internal server use decimal value of 1-6)
- 134 Diffserv Code Point, integer value

If there are 5230 IP Appliances, create the following options:

- 6 DNS Server, IP address format
- 44 NetBIOS Name Server, IP address format

6. In the **DHCP Options** form, for a cluster environment, program IP Console (if any) with a static IP Address. Then, do the following:

   Program Options 128 and 129 with:
   - Format: IP Address
   - Value: IP Address of the controller that controls the device
   - Scope: Static: <device name><subnet>.

   If different VLAN tagging and priority information is needed for the IP Console, repeat step 6 for Options 132 and 133.

   If a different router is need for any IP Consoles, repeat step 6 for Option 3 and set the Value to the IP address of the router.

7. In the **DHCP Lease Viewer** form, ensure that there is no DHCP IP Address Lease for the IP Console MAC Addresses. If there is, delete it and then power off and power on the device.

8. In the **DHCP Server** form, enable the internal DHCP server.

To use an alternative DHCP server (see page 307 and page 308):

1. In the **DHCP Server** form, disable the internal DHCP server.

2. Program your DHCP server with the following options:

   - 128 TFTP IP address format
   - 129 RTC IP address format
   - 130 MITEL IP PHONE, string value.

Programming the Controller DHCP Server Settings (for Release 7.0 and later)

Note: DHCP options 128-133 used to configure Mitel IP endpoints have been reclassified as public options by the Internet Engineering Task Force (see RFC 2133 and RFC 3925). To comply with the change, Mitel recommends using either option 43 or 125, depending on the server's ability to support them and on administrator preference. (The embedded server supports both options with 125 as the factory-programmed default.) The old options can still be used to provide backward compatibility with IP sets that have yet to be upgraded with firmware that supports the new options. After the upgrade, the old options may be removed to prevent future conflicts with standard use or other vendors' use of these options.

Note: Ensure that all LLDP-compliant telephones are upgraded to firmware version 2.0.0.18 or later before you use LLDP on your network for VLAN Discovery.

Note: LLDP-MED non-compliant telephones cannot use LLDP for VLAN discovery. They must use DHCP VLAN discovery. Non-compliant sets are: 5001, 5005, 5010, 5020 IP Phones, 5140 IP Appliance, 5201, 5205, 5207, 5215 (single mode), 5220 (single mode), 5230 IP Phones, 5240 IP Appliance, 5485 IP Pager, and 5550 IP Console keypad.

For additional information on programming DHCP settings for the 3300 ICP, refer to the System Administration Tool Online Help.

To use an external DHCP Server, do not enable the internal DHCP server and refer to “Configuring External DHCP Settings for E2T” on page 307 for instructions.

Tip: You may need to change the IP address of your PC to match your customers network.

1. On the Maintenance PC, access the System Administration Tool (see "Launching the Programming Tools" on page 8).
2. In the **All forms (alphabetical)** list, click **DHCP Subnet** form, enter the subnet name, IP address and bit mask.
3. In the **DHCP Static IP** form, enter a static IP address for the E2T using the information on page 301 (skip this step for the MX and 100-user controllers). Assign IP addresses to specific devices by using the MAC address of the device. Assign a static IP Address to any IP Console in a cluster.
4. In the **DHCP IP Address Range** form, program the scope using the information on page 301.

Tip: The following IP addresses are reserved to provide backward compatability for legacy AMBs and ASUs:

192.168.10.1 *to* 192.168.10.15 through 192.168.13.1 *to* 192.168.13.15

The ASU II and legacy AMBs and ASUs with upgraded firmware use the following reserved addresses:
169.254.10.0 *to* 169.254.10.15 through 169.254.19.0 *to* 169.254.19.15

5. In the **DHCP Options** form, program the options listed in Table 78 on page 301 for the scope you just programmed. Always create the following options:

Note: IP sets require a firmware upgrade to support the new DHCP options introduced in Release 7.0; otherwise, the sets will fail to boot. Such failures can occur, for example, in a resilient cluster of mixed software releases or when sets with old firmware are added to a controller after it was upgraded to Release 7.0. For the sets to boot, DHCP options 128-133 must be present in the DHCP server. After the sets have booted, options 128-133 may be removed to avoid future conflicts with standard use or other vendors' use of these options.

- 3 Router, IP address
- 125 Vendor-Identifying Vendor-Specific Information or Option 43 Vendor Specific Information. Option 125 is the preferred option.
- 66 TFTP Server, IP address format
- 67 Boot file, string value (always /sysro/E2T8260)

If there are 5230 IP Appliances, create the following options:

- 6 DNS Server, IP address format
- 44 NetBIOS Name Server, IP address format

6. In the **DHCP Options** form, for a cluster environment, program IP Console (if any) with a static IP Address. Then, do the following:

Program Option 125 (preferred) or Option 43 with:

- Format: ASCII String
- Value: IP Address of the controller that controls the device and different VLAN tagging and priority information if needed for the console
- Scope: Static: <device name><subnet>.

Assign the address Option 125 (or 43) as above, specifying different VLAN tagging and priority information if needed for the console.

If a different router is need for any IP Consoles, repeat step 6 for Option 3 and set the Value to the IP address of the router.

7. In the **DHCP Lease Viewer** form, ensure that there is no DHCP IP Address Lease for the IP Console MAC Addresses. If there is, delete it and then power off and power on the device.
8. In the **DHCP Server** form, enable the internal DHCP server.

To use an alternative DHCP server (see page 307 and page 308):

1. In the **DHCP Server** form, disable the internal DHCP server.
2. Program your DHCP server with options 128-133.
3. Upgrade the IP Phones/ firmware to 2.0.0.18 or later.
4. Program your DHCP server with the following options:
   - 43 Vendor Specific Information, string value

   OR
   - 125 Vendor-Identifying Vendor-Specific Information, string value.
5. Delete options 128-133.

Note: IP sets require a firmware upgrade to support the new DHCP options introduced in Release 7.0; otherwise, the sets will fail to boot. Such failures can occur, for example, in a resilient cluster of mixed software releases or when sets with old firmware are added to a controller after it was upgraded to Release 7.0. For the sets to boot, DHCP options 128-133 must be present in the DHCP server. After the sets have booted, options 128-133 may be removed to avoid future conflicts with standard use or other vendors' use of these options

Note: Ensure that all LLDP-compliant telephones are upgraded to firmware version 2.0.0.18 or later before you use LLDP on your network for VLAN Discovery.

Note: LLDP-MED non-compliant telephones cannot use LLDP for VLAN discovery. They must use DHCP VLAN discovery. Non-compliant sets are: 5001, 5005, 5010, 5020 IP Phones, 5140 IP Appliance, 5201, 5205, 5207, 5215 (single mode), 5220 (single mode), 5230 IP Phones, 5240 IP Appliance, 5485 IP Pager, and 5550 IP Console keypad.

Program DHCP for VLAN (prior to Release 7.0):

Follow this procedure if using two DHCP servers: central server (external) on a default VLAN and other (3300 DHCP Server) on the voice VLAN.

1. Set up the central DHCP Server with the following options:
   - 130 MITEL IP PHONE, string value
   - 132 VLAN ID
   - 133 Priority, value of 1-6
   - 134 Diffserv Code Point, integer value
2. Set up the 3300 ICP DHCP Server with the following options:
   - 128 TFTP IP address format
   - 129 RTC IP address format
   - 130 MITEL IP PHONE, string value
   - 132 VLAN ID
   - 133 Priority, value of 1-6
   - 134 Diffserv Code Point, integer value
3. Program the DHCP server on the 3300 ICP (see procedure above).

Verifying the Operation of the Controller

1. On the Maintenance PC, access the System Administration Tool.
2. In the **System Hardware Profile** folder, verify that the information in each of the forms is correct, including the IP address of the E2T for the LX and 250/700-user system.
3. In **Maintenance and Diagnostics**, click **Alarm Details**.
   Verify that the following alarms do not appear (if you get an alarm, go to "Alarms" on page 189):
   - E2T Com (not applicable to the MX, CX/CXi, or 100-user controller)
   - DSP

Tip: The next four steps are optional.

4. Connect two IP Phones directly to one of the controller's Ethernet ports (for an MX and 100-user controller, only the leftmost port is functional and you must use a Layer 2 switch for these steps).
5. Program the IP Phones (refer to the System Administration Tool Online Help for details).
6. Make a call from one phone to the other.
7. Remove the IP Phones from the controller.

Configuring the Layer 2 Switch

The 3300 ICP requires a Layer 2 switch between its controller and the network. The internal Layer 2 switch in the CXi and MXe must be programmed with an IP Address in the same subnet as the RTC IP Address, or the switch will not operate properly. Do this by completing the System IP Configuration form, and then reboot the system.

Note: The 16 10/100 Mbps ports are disabled on the CXi during bootup; likewise, the right-side Gigabit port on the MXe.

Tip: Refer to the System Administration Tool Online Help for detailed instructions for programming the IP Network Configuration forms associated with the CXi and MXe.

1. Connect an Ethernet cable between the Layer 2 switch on your network and the leftmost available Ethernet port on the controller (port 17 on the CXi and the left Gigabit port on the MXe). Use a straight-through cable for the CXi and MXe and a crossover cable for all other controllers.

Tip: For an MX or 100-user system, move the Maintenance PC Ethernet connection from the controller to one of the Layer 2 switch input ports, and connect the Layer 2 switch to the leftmost Ethernet port of the controller. You can do the same for an LX, 250 and a 700-user system, if desired.

2. Program the Layer 2 switch with the appropriate settings (see “Network Configuration Examples” on page 317 for more information).

Tip: Typically, in a VLAN environment, an access port is used to connect the Layer 2 switch to the controller, and trunk ports to connect the Layer 2 switch to the IP Phones.

Tip: IP trunks cannot work through the WAN port.

   - See your IT administrator for information to set up and program a DHCP server. We recommend that you use the controller’s internal DHCP server to provide a static IP address to the E2T.

3. If you are not using the controller’s DHCP server, disable it in the **DHCP Server** form.

Tip: See “Configuring a Windows 2000 DHCP Server (prior to Release 7.0)” on page 308 for information on programming 3300 ICP DHCP settings on a Windows 2000 DHCP server.

Install Units

This section contains detailed information on installing and configuring the Network Services Unit, Analog Services Unit, Peripheral Cabinet, SUPERSET HUB, and Digital Services Unit (DSU) for the 3300 ICP.

CAUTION: Provide a permanent ground for all controllers and units, through the ground connection on each cabinet.

This section also contains information on configuring embedded analog on the MX, MXe, and CX/CXi controllers.

Tip: The CX/CXi controllers do not support Network Services Units or Analog Services Units. The CX/CXi do support embedded trunking and embedded analog.

You can install any of the following Network Services Units (NSUs):

- Universal NSU (MSDN, PRI/QSIG, T1/D4)
- R2 NSU
- BRI NSU.

You can double the number of Universal and R2 NSUs in a system by chaining a secondary NSU to each primary NSU connected to the controller. BRI NSUs cannot be chained.

Some NSUs must be programmed with the ISDN Maintenance and Administration Tool (IMAT) (see "Install and Use IMAT" on page 88).

CAUTION: To connect your NSU to the LAN, you must change the default IP and gateway addresses to match an available address on the LAN. The default address is 192.168.1.1:ffffff00. See "Programming an IP Address into the NSU" on page 88.

Universal or R2 Network Services Unit

1. Mount and secure the NSU in the desired location.
2. Set the L0/L1 port DIP switches to the appropriate termination mode and impedance (see Table 53 on page 268 and Table 58 on page 270). The default is network termination mode. See "Network Services Units" on page 267 for the location of these switches.

3. Set the Message Link DIP switch to the appropriate position. See page 267 for the location of the Message Link switch and Table 52 on page 268 for settings.
4. Connect a fiber optic cable between the NSU and the controller FIMs.
5. If you are installing a secondary NSU, connect a crossover CAT 5 cable between CIM 1 of the secondary NSU and CIM 2 of the primary NSU (see Table 55 on page 269 for CIM pinout, and Table 52 on page 268 for message link dip switch settings).
6. Connect the NSU L0 and/or L1 port to the remote system (the PSTN or another system). See Table 58 on page 270 for the pinout.
7. For the PRI and R2 protocols, program the NSU using IMAT (see "Installing IMAT on the PC" on page 88 and "Using IMAT" on page 90). Refer to the IMAT Online Help for more information.
8. Connect power to the NSU.

Tip: The NSU software will not load until the NSU programming is complete (see Step 9 below).

9. Using the System Administration Tool, program the NSU settings on the controller. In the **All forms (alphabetical)** list, click **Network Services Unit Configuration**. Refer to the Online Help for more information.

Next: Install any other required services units. When all the services units are installed, go to "Install Telephones and Peripherals" on page 51.

BRI Network Services Unit

Connect the BRI NSU to the controller via a Universal E1 MSDN NSU. Refer to "Quad BRI Framer" on page 111 for installing embedded BRI.

Tip: Program the Universal E1 NSU before connecting the BRI NSU.

1. Mount the BRI NSU.
2. Connect the BRI NSU E1 ports to the Universal NSU L0/L1 ports (see Table 53 on page 268 and Table 58 on page 270 for pinouts).

Tip: Use a CAT 5 cable between the BRI NSU E1 port and the Universal NSU that is running E1 DPNSS. Ensure that the pinout of the cable matches that of the E1 connector (pins 4 and 5 are connected). A 4-wire CAT 5 cable will only use pins 1, 2, 3, and 6.

3. Connect the BRI NSU to the ISDN devices using a 25-pair cable. See Table 60 on page 272 for the pinout.
4. Connect the BRI NSU to the maintenance PC:
   a. Connect the RS-232 port (RJ-45 connector) on the BRI NSU to a serial port on the PC.
   b. Set up the communications program on COM port 1 or 2 with the following parameters:
      - Baud Rate: **9600**
      - Data Bits: **8**
      - Parity: **None**
      - Stop Bits: **1**
      - Flow Control: **XON/XOFF**
      - Character Set: **ASCII**
5. Connect power to the BRI NSU.
6. On the PC, program the BRI NSU using a VT100 emulator (see TB #58004741 Basic Setup Guide for the MC268 BRI card).

Tip: Even though the TB is written for the SX-2000 system, the parameters described are also applicable to the 3300 BRI NSU.

Analog Services Unit

This procedure applies to the ASU, the Universal ASU, and the ASU II (compatible only with Release 7.0 software). You can connect up to four Analog Services Units to the controller (two for the MX and 100-user controllers). Ensure that there is a free CIM port on the controller.

ASU II mounting instructions:

- For rack mounting (rear or front facing), do not install the feet
- For wall mounting, install only the two bottom feet.

1. Mount the ASU. Refer to page 141 for ASU II line card installation instructions.
2. Connect a Crossover Category 5 cable with RJ-45 connector to the CIM port on the ASU and a free CIM port on the controller (see Table 55 on page 269).

Tip: The 3300 Universal ASU can be located up to 30 meters (100 feet) away from the controller. The interface uses a single standard 8-pin modular jack consisting of 2 balanced signal pairs, and is located on the front of the unit.

3. Complete telephony cabling for the ASU (see Table 64 on page 276).
4. Complete the Music on Hold and Paging cabling if required. For the Universal ASU, see Table 66 and Table 67 on page 277.
5. Connect power to the ASU. Once the CIM link synchronizes, the CIM LEDs turn on. The controller detects the ASU, and the application software downloads and starts immediately.

Tip: The ASU software will not load until the ASU programming is complete.

6. Using the System Administration Tool, program the ASU settings on the controller (see the System Administration Tool Help for details).

Tip: The ONS circuits provide positive disconnect for support of applications such as door phones.

Tip: Use the LSMeasure Tool to determine the line settings for LS trunks on an Analog Board or a Universal ASU (see page 250).

Next: Install any other required services units. When all the services units are installed, go to “Install Telephones and Peripherals” on page 51.

Embedded Analog, Configure

To configure controllers with embedded analog.

1. Complete telephony cabling for embedded analog (see Table 45 on page 263).
2. Complete the Music on Hold and Paging cabling if required (see Table 43 and Table 44 on page 263).
3. Connect power to the controller. The controller detects the Analog Main Board and Analog Option Board and the software downloads.

CAUTION: Rebooting the controller before the embedded analog software is downloaded can render the boards inoperable.

Tip: Verify, in the System Administration Tool, that 3300 Embedded Analog or 3300 Expanded Analog appears as the Installed Type in the Analog Services Unit Configuration form.

4. Using the System Administration Tool, program the analog settings on the controller. Refer to the System Administration Tool Online Help for information.

Tip: The ONS circuits provide positive disconnect for support of applications such as door phones.

Tip: Use the LSMeasure Tool to determine the line settings for LS trunks on an Analog Board, Universal ASU, or ASU II (see page 250).

Peripheral Cabinet

Tip: The CX and CXi controllers do not support Peripheral Cabinets.

To install a peripheral cabinet:

1. Unpack, position, and ground the peripheral cabinet.
2. Check the card layout (see page 41).
3. Connect the fiber cable to the node (see page 42).
4. Check the grounding (see page 42).
5. Install the power converter (see page 43).
6. Install the peripheral interface cards (see page 44).
7. Cable the node to the MDF (see page 45).

To unpack, position, and ground the cabinet:

1. Open the peripheral cabinet carton.
2. Remove the plastic bag from the top and sides of the cabinet. Lift the peripheral cabinet out of the carton.
3. Check the node and attached equipment for damage. Repack and return any damaged equipment.
4. Position the node.

CAUTION: Do NOT apply power to the peripheral cabinet until you have installed the ground cable.

5. Connect an external ground to the ground terminal on the rear panel of the peripheral cabinet. Refer to the Safety Instructions for detailed grounding requirements. These instructions are packaged with each system.
6. Remove the peripheral cabinet front panel (see “Removing/Replacing the Front Panel of a Peripheral Cabinet or DSU” on page 142).

Check the Card Layout

Typically, a peripheral cabinet is shipped with the peripheral switch controller (PSC) card and fiber interface module (FIM) installed. If these cards were not shipped in the cabinet, see page 142 for installation instructions. You must install and cable the FIM before you install the peripheral switch controller card and power converter.

Install the cards in the following configuration (see also page 280).

Slot Number	Card Type
1 to 12	Peripheral interface card
13, 14, 15 (combined)	Power converter
16	Peripheral switch controller (PSC)
17	Fiber interface module (FIM)

Note: Depending on the peripheral cabinet type, slots 16, 16B, and 17 may be used for the following purposes:

- Type A (9400-200-110-NA) has a peripheral switch controller (PSC) card in slot 16 that works in conjunction with a peripheral resource card (PRC) in the upper portion of slot 17. A fiber interface module (FIM) is located in the lower portion of slot 17.
- Type B (9400-200-113-NA) has a PSC or PSC II card in slot 16. The PSC card works in conjunction with a PRC in slot 17; a PSC II card includes PRC functionality. A FIM is located in the lower portion of slot 17.
- Peripheral cabinet II or peripheral cabinet 19" has a PSC II in slot 16 and a FIM in slot 17.

Tip: If you are installing an expanded peripheral cabinet, or expanding an existing one, the card layout will be different depending on whether the cabinet is used as the master or slave of the peripheral pair. Refer to “Installing an Expanded Peripheral Cabinet” on page 149.

Connecting the Fiber Cable to the Peripheral Cabinet

The fiber optic cable connects the FIM in the controller to the FIM in the peripheral cabinet.

To connect the fiber optic cable to the FIM in the peripheral cabinet:

1. Route the fiber optic cable through the cable port at the rear of the peripheral cabinet into the cabinet. Extend the fiber cable approximately one foot (30 cm) beyond the front of the cabinet.
2. Install a short piece of nylon spiral wrap over the cable at the point where the cable exits the rear of the cabinet.
3. Close the sliding cable port door. Ensure that the door closes on the nylon spiral-wrapped section of fiber cable.
4. Remove the plastic dust caps from the fiber optic cable connectors and the connector ferrules on the FIM faceplate.
5. Plug the fiber connectors into the connector ferrules on the FIM faceplate.

Tip: The fiber connectors have a small key that you must align with a slot on the FIM connectors. Lock each connector into position by pushing its metal collar forward and clipping it onto the FIM connector.

Checking the Grounding on an AC System

CAUTION: Ensure that the grounding meets the requirements specified in the Safety Instructions. These instructions are packaged with each system.

WARNING: DANGER TO PERSONNEL AND/OR EQUIPMENT DAMAGE COULD RESULT IF THE CABINET IS NOT POWERED OFF DURING THIS PROCEDURE.

1. Ensure that the power switch (S1) on the power distribution unit (PDU) is set to the off (0) position and that the switch on the power converter faceplate is set to the off (0) position.
2. Attach the anti-static wrist strap to your wrist.
3. Slide the installed circuit cards forward slightly so that the card connectors are not in contact with the cabinet backplane. Leave the power converter installed.
4. Remove the anti-static wrist strap.

5. Plug the external power cable from the AC commercial power supply into the power input plug on the power distribution unit (PDU).
6. Disconnect the protective earth wire from the protective earth ground stud on the rear of the cabinet.
7. Using a digital multimeter, measure the AC potential between the protective earth wire (building ground) and the protective earth ground stud. A voltage reading of less than 1 Vac is acceptable. To prevent damage to the multimeter, set it to the maximum ac scale, then reduce the setting gradually to the 10 Vac range.
8. If the potential is greater than 1 Vac, recheck the ground connections and repeat the measure.
9. If the reading still exceeds 1 Vac, the building ground is unacceptable. Connect the protective earth wire to a new building ground and repeat the steps 7 through 9 until you have an acceptable AC potential.

WARNING: DO NOT CONTINUE UNTIL YOU HAVE A POTENTIAL OF 1 VAC OR LESS BETWEEN THE BUILDING GROUND AND THE PROTECTIVE EARTH GROUND STUD. OTHERWISE, PERSONAL INJURY AND/OR EQUIPMENT DAMAGE MAY RESULT.

10. Reconnect the protective earth wire to the protective earth ground stud and attach the anti-static wrist strap to your wrist.
11. Slide the installed circuit cards back into contact with the cabinet backplane. Ensure that each card is fully inserted in its slot.
12. Remove the anti-static strap from your wrist.

Installing the Power Converter

Refer to “Safety Considerations” on page 98.

WARNING: DANGER TO PERSONNEL AND/OR EQUIPMENT DAMAGE COULD RESULT IF THE CABINET IS NOT POWERED OFF DURING INSTALLATION OF THE AC POWER CONVERTER.

1. At the rear of the cabinet, remove the two screws that fasten the internal AC power cord access cover plate to the backplane, and remove the cover plate (see Figure 8).

2. Ensure that the switch on the power converter faceplate is set to off (0).
3. Slide the power converter into slots 13 through 15.
4. Push the upper and lower latches away from you until they are vertical and the power converter is locked in place.

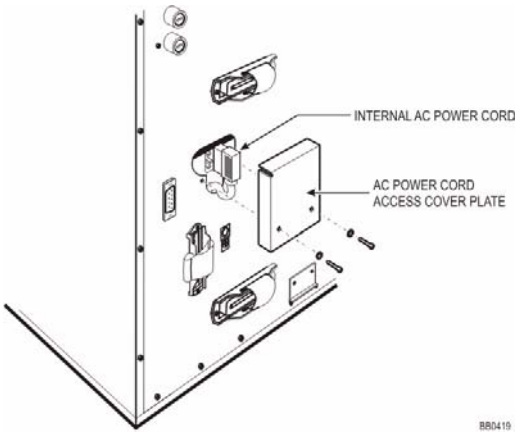


Figure 8: Peripheral Cabinet AC Power Cord Access

5. Plug the internal AC power cord from the power distribution unit (PDU) into the power converter through the access cutout in the backplane.
6. Replace the internal AC power cord access cover plate over the access cutout in the backplane, and replace the two screws.

Installing the Peripheral Interface Cards

Refer to "Safety Considerations" on page 98.

CAUTION: To prevent static damage to electrical components, ensure that the system is grounded before you install the cards. Whenever you handle circuit cards, wear an anti-static strap.

1. Set the E&M trunk card switch settings (see page 281) and the OPS line card message waiting switches (see page 283).
2. Check all card connector pins to be certain that they are straight.

3. Slide the peripheral switch controller card into slot 16 (see “Peripheral Cabinet Card Layout” on page 280 for slot locations).
4. Slide the other peripheral interface cards into their appropriate slots.
5. Push the upper and lower latches away from you until they are vertical and the cards are locked in place.

Cable the Node to the MDF

Cable the lines and trunks from the peripheral cabinet to the main distribution frame (MDF) by using the peripheral interface cabling tables (see “Peripheral Cabinet Cabling” on page 285).

Programming the Peripheral Cabinet

1. Power up the peripheral cabinet.
2. Using the System Administration Tool, program the peripheral cabinet. Refer to the System Administration Tool Online Help for details.

SUPERSET HUB

Tip: The CX and CXi controllers do not support SUPERSET HUBs.

Installing a SUPERSET HUB requires that you first install the peripheral slot FIM carrier (page 45) and then the SUPERSET HUB (page 46).

Install the Peripheral Slot FIM Carrier

WARNING: THIS PRODUCT USES A CLASS 1 LED. FIBER OPTIC SOURCES EMIT INFRARED RADIATION. THIS RADIATION IS INVISIBLE TO THE HUMAN EYE, AND CAN DAMAGE THE RETINA. NEVER LOOK DIRECTLY INTO THE END OF A FIBER OPTIC CABLE THAT YOU SUSPECT IS ENERGIZED BY A FIBER OPTIC SOURCE. WHEN WORKING WITH RAW FIBER OPTIC CABLES, BE AWARE OF FIBER ENDS AND SLIVERS WHICH CAN PUNCTURE THE SKIN AND CAUSE IRRITATION.

To install the peripheral slot FIM carrier:

1. Attach an anti-static wrist strap.
2. Unpack the peripheral slot FIM carrier and inspect it to ensure that it is not damaged.
3. Remove the peripheral cabinet front and rear panels.
4. Slide the peripheral slot FIM carrier part-way into the first available slot from the right.
5. Remove the black plastic dust caps from the fiber optic cable connectors and from the connector ferrules on the faceplate of the FIM.
6. Connect the fiber optic cables to the connectors on the FIM via the fiber optic access port on the rear of the cabinet.

Tip: The fiber optic cable connectors have a small key that you must align with a slot on the FIM connectors. Lock each connector into position by pushing its metal collar forward and clipping it onto the FIM connector.

7. Push the peripheral slot FIM carrier fully into the slot and secure it with the card latch.
8. Remove the anti-static wrist strap.
9. Route the fiber optic cables from the peripheral cabinet to the SUPERSET HUB.
10. Replace the peripheral cabinet front and rear panels.

Install the SUPERSET HUB Unit

To install the SUPERSET HUB unit:

1. Attach the rubber feet to the base of the unit.
2. If required, secure the mounting brackets to the SUPERSET HUB case by using the holes for to the selected mounting position, and install the unit in an equipment rack or mount the unit on a wall.

Tip: The side with the row of RJ-45 connectors faces the front when the unit is rack-mounted or the top when the unit is wall-mounted. If you are wall-mounting the unit, use wall anchors appropriate for the wall type, use #12 screws that are at least 1.5 inches (0.8 cm) long, and ensure that the screws are not fully tightened so that the unit may be easily removed (without the use of a tool) for servicing.

3. Ensure that the ventilation holes are not blocked.

4. Remove the black plastic dust caps from the fiber optic cables and the connector ferrules on the unit.
5. Connect the fiber optic cables from the peripheral slot FIM carrier in the peripheral cabinet to the connectors on the SUPERSET HUB unit.
6. Connect the RJ-45 connectors to the UTP distribution panel according to the building wiring plan.
7. Connect the power cable to a convenient wall socket.

Tip: Because the power cable is the main disconnect device, the wall socket must be near the unit and easily accessible.

8. Program the SUPERSET HUB as a DNI line card in the slot where the peripheral slot FIM carrier is inserted.

Tip: When installing the SUPERSET HUB in an enclosed rack, you **must** provide adequate ventilation to ensure that the maximum ambient temperature inside the rack does not exceed 40ºC (104ºF).

Tip: When mounting the SUPERSET HUB in a rack, ensure that a hazardous condition is not achieved due to any uneven mechanical loading.

Tip: When using the SUPERSET HUB in a rack, consider the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. When addressing this concern, consider the SUPERSET HUB's ratings label.

Digital Service Unit

WARNING: DO NOT APPLY POWER TO THE EQUIPMENT AT ANY TIME DURING EQUIPMENT INSTALLATION.

Tip: The CX and CXi controllers do not support Digital Service Units.

Tip: Two DSU cabinets may be programmed in a single DSU node. On the left side of the node, slots 1, 2, and 3 comprise one DSU cabinet. On the right side of the node, slots 4, 5, and 6 comprise another DSU cabinet. When you program cards in the left cabinet, **program slot 3 before slot 2**. When you program cards in the right cabinet, **program slot 5 before slot 4**. If you do not follow this order of programming, the DSU cards on the side of the node that you are programming will reset when you add the second card and the cabinet will go out of service for one or two minutes.

To install a DSU:

1. Unpack and position the DSU node.
2. Check the card layout (see page 48).
3. Connect the fiber cable to the node (see page 49).
4. Install the interface assemblies (see page 49).
5. Install the DSU cards (see page 50).

Unpack and Position the DSU Node

To unpack and position the DSU node:

CAUTION: Do not open or unpack any printed circuit board cartons at this time.

1. Open the DSU node carton.
2. Remove the plastic bag from the top and sides of the cabinet. Lift the DSU node out of the carton.
3. Check the node and attached equipment for damages. Repack and return any damaged equipment.
4. Position the node.

CAUTION: Ensure that you use the Cabinet Stacking Brackets if you want to stack cabinets on top of each other. Stacking cabinets without these brackets could result in damage to the equipment or injury.

5. Remove the DSU node front panel.

Check the Card Layout

A DSU node is shipped with two fiber interface modules (FIMs) installed. If FIM cards were not in the node see page 151 for installation instructions.

Each DSU node has one or two FIMs, depending on the number and location of DSU cards in the node. The FIM in the bottom of slot 1 provides communications with the control node for the DSU cards in slots 2 and 3, and the FIM in the bottom of slot 6 provides communications for the DSU cards in slots 4 and 5. Install and cable the FIMs before you install any cards in the DSU node. Check the DSU node card layout on page 290 to ensure that you have the parts that you need to complete the installation.

Connect the Fiber Cable to the DSU Node

The fiber optic cable connects the FIMs in the controller to the FIMs in the DSU node.

To connect the fiber optic cable to the FIM in the DSU node:

1. Route the fiber optic cable through the cable port at the rear of the DSU cabinet. Extend the fiber cable approximately 1 ft (30 cm) beyond the front of the cabinet.
2. Install a short piece of nylon spiral wrap over the cable at the point where the cable exits the rear of the cabinet.
3. Close the sliding cable port door. Ensure that the door closes on the nylon spiral-wrapped section of fiber cable.
4. Remove the plastic dust caps from the fiber optic cable connectors and the connector ferrules on the FIM faceplate.
5. Plug the fiber optic cable connectors into the connector ferrules on the FIM faceplate.

Tip: The fiber optic cable connectors have a small key that you must align with a slot on the FIM connectors. Lock each connector into position by pushing its metal collar forward and clipping it onto the FIM connector.

Install the Interface Assemblies

The DS1 interface assembly provides two filtered DB-15 pin connectors for the external cables required by one DS1 formatter card. You can mount up to four DS1 interface assemblies in the DSU.

The CEPT interface assembly provides four filtered BNC connectors for the external cables required by one formatter card. You can mount up to four CEPT interface assemblies in the DSU. Each interface assembly plugs into a J3 DIN 3x32 pin connector. The connectors are located in a 3.5 inch x 5 inch (9 cm x 12.5 cm) box that projects from the backplane.

To install a DSU Interface Assembly:

1. Attach an anti-static strap to your wrist.
2. Unpack and inspect the interface assembly.
3. If you are installing a CEPT Interface Assembly, set the jumpers to the desired positions.
4. At the rear of the cabinet, locate the slot in the DSU box that corresponds to the DSU slot that you will use for each DSU card.

Tip: When you are facing the rear panel, the DSU box slots (from right to left) correspond to DSU slots 2 through 5.

5. Remove the cover plate from the selected slot by removing the two screws that hold the plate in place.
6. If the interface assembly has an extension bracket, mount the interface assembly extension bracket on the selected slot using the screws that secured the cover plate. The closed side of the extension bracket must be to the left when viewed from the rear of the cabinet.
7. Insert the interface assembly into the empty slot in the DSU box. Ensure that the edge connector on the card aligns with the connector on the backplane of the system.
8. Secure the interface assembly to the DSU cabinet or the extension bracket.

Install the DSU Cards

CAUTION: To prevent static damage to electrical components, ensure that the system is grounded. Whenever you handle circuit cards, wear an anti-static strap.

To install a DSU card:

1. Ensure that the FIMs are installed and cabled.
2. Connect the power cord to the external AC power source.
3. Unpack the card, and verify that it is not damaged.
4. If required, adjust the card switch settings (see page 289 for details).
5. Check the connector pins to be certain that they are straight.
6. Slide the card into the appropriate slot.
7. Push the upper and lower latches away from you until they are vertical and the card is locked in place.
8. Proceed to one of the following tasks to complete the card installation:
   - CEPT or DS1 formatter cards (see page 154)
   - BRI card (see page 152)
   - PRI card (see page 154)
   - R2 card (see page 158)

Install Telephones and Peripherals

This section contains information on installing telephone sets, consoles, and other peripherals.

The 3300 ICP supports a number of IP, DNI, analog and wireless phones, as well as conference units, programmable key modules, and attendant consoles. The CX and CXi controllers support IP and analog phones.

If you have a peripheral cabinet with analog/DNIC phones connected to it, program those telephones using the System Administration Tool.

Tip: You cannot use the Group Administration Tool to modify programming for SUPERSET 400-series telephones.

Installing Telephones, Consoles and Appliances

Refer to each device's Installation Guide (included in the telephone package) to install the devices.

Tip: Connect a printer to the 5550 IP Console RS-232 port to print hotel reports. For Release 6.0 and later, PMS provides for a direct IP connection to the 3300 ICP. See Property Management System in the online help for details.

Note: If you intend to rely on LLDP VLAN Discovery in the network, you must first upgrade the 3300 ICP to Release 7.0 or later and upgrade the IP Phone firmware to version 2.0.0.18 or later.

Note: LLDP-MED non-compliant telephones cannot use LLDP for VLAN discovery. They must use DHCP VLAN discovery. Non-compliant sets are: 5001, 5005, 5010, 5020 IP Phones, 5140 IP Appliance, 5201, 5205, 5207, 5215 (single mode), 5220 (single mode), 5230 IP Phones, 5240 IP Appliance, 5485 IP Pager, and 5550 IP Console keypad.

Upgrading IP Phone Firmware

- Automatically download firmware from the 3300 controller to the IP Phones (requires a DHCP server configured with options 128-133).
- Download firmware by plugging the telephone directly into an Ethernet port on the 3300 controller. The controller must be running Release 7.0 or later to provide LLDP-compliant firmware to the telephone.

Installing Line Interface Modules

The Line Interface Module (LIM) provides analog operation to the 5220 IP Phone (Dual Mode), 5224 IP Phone, 5235 IP Phone, 5330 IP Phone, or 5340 IP Phone in the event of an IP connection failure. Follow the instructions in the Installation Guide that is included in the module package to install a Line Interface Module. Refer to "Program Emergency Services for a Line Interface Module" in the System Administration Tool Help.

Programming Phones

Tip: Refer to the System Administration Tool Online Help for information on programming SpectraLink Wireless Telephones, IP DECT Wireless Phones, and Symbol NetVision MiNET Phones.

To program telephones:

1. Using the System Administration Tool, enter the required programming and registering information in the applicable forms in the **Devices** folder. Refer to the Online Help for details.
2. Program the **User Authorization Profile** form for the IP device users if required. Typically, IP Phone and Appliance users are only given access to the Desktop Tool.

Tip: If you have a large number of new user profiles to add, you can import new user and device data using the Import functionality in the User Configuration form in the System Administration Tool.

Registering IP Devices from the Telephone

Use this procedure to register IP devices with the 3300 ICP database. The procedure will program the 3300 ICP database with the MAC address of the IP device.

Tip: Use the System Administration Tool to program all other set features (for example, Class of Service, Interconnect Restriction, Set Key Assignments, and Class of Restriction).

Before you begin

- Ensure a Set Registration Access Code and a Set Replacement Access Code are assigned in the System Options Assignment form.
- Ensure the directory number and device type is programmed in the Single Line IP Set Configuration form or Multiline IP Set Configuration form.

Register an IP Device

1. Connect the IP device to an RJ-45 Ethernet port on the LAN. For the CXi, connect to a controller Ethernet port.
2. Provide power to the IP device (refer to the Hardware Technical Reference Manual at Mitel OnLine for power option information).
3. Press ***** during power-up (to clear any PIN number in memory).
4. Type the PIN number at the prompt on the IP device. Prompts are:
   - non-display IP Phones: solid message light.
   - display IP Phones and IP Appliances: display shows **Enter the PIN number**.

Tip: The PIN number is the set registration code followed by the set's extension number.

5. Complete one of the following to send the PIN:
   - 5001, 5005, 5201 and 5205 IP Phones: press **Hold**.
   - 5010, 5207, 5215, 5020 and 5220 IP Phones: press **SuperKey**.
   - 5140 and 5240 IP Appliances, 5235 IP Phone: press **OK**.
   - 5230 IP Appliance: press **Send**.
     The set will complete initialization.

Register an IP Device in a Cluster

The registering sequence in a cluster is unchanged provided that:

- the Cluster Element ID programmed in the **Cluster Element Assignment** form matches the ICP/PBX Number programmed in the **ICP/PBX Assignment**.
- each member of the cluster is programmed with the directory numbers of the other controllers. This information must be programmed using OPS Manager.
- the Set Registration Access Codes and Set Replacement Access Codes are the same for each controller in the cluster.
- each IP device is able to retrieve the IP address of one of the controllers in the cluster.

Setting Static IP Address on IP Display Set

The customer may prefer to assign static IP addresses to IP sets rather than using dynamic IP addressing. You cannot set static IP addresses on non-display sets. To set static IP address on the IP telephones:

1. Plug the set cable and power into the set while holding down the **Volume Up** key for 3 seconds to display **Set Static IP (Yes #/No *)**.
2. At the **STATIC IP SETUP MODE**.
   - Use the **Volume Up/Down** keys to navigate
   - Use the ***** key to back up (to correct an error)
   - Use the # key to insert a decimal and move to the next field.
3. At the **USE PRESENT SETTINGS** screen, select **# - ENABLE** to enter a complete set of IP data.

Tip: Select * - DISABLE to revert back to DHCP from static parameters.

4. At **INPUT VLAN ID**, if VLANs are used, enter the VLAN ID that will be inserted into packets sent by the phone. Enter nothing if VLANs are not used.
5. At **INPUT PRIORITY**, enter **6** if priority is used or leave blank.
6. At **INPUT IP ADDRESS**, enter the customer-supplied static IP address (e.g. 10.30.27.191).
7. At **INPUT PDA ADDRESS**, enter the customer-supplied static IP address (not for single line display sets).
8. At **INPUT SUBNET MASK**, enter the subnet mask.
9. At **INPUT DEFAULT GATEWAY**, enter the Router IP address (e.g. 10.30.27.2).
10. At **INPUT RTC ADDRESS** (**SRVR IP** on single line sets), enter the RTC address.
11. At **INPUT TFTP ADDRESS** (**TFTP SRVR IP** on single line sets), enter the address of the TFTP server used to download the main and boot load images.

12. At **INPUT DNS ADDRESS**, you MUST enter the IP address of the server that will be used during Web browsing to resolve host names into IP addresses. Skipping this field will prevent the phone from booting. If you do not have a DNS server, enter any IP address value (for example 10.30.32.3).
13. The following prompts are required fields for IP Appliances, optional for multiline display sets, and do not appear for single line display sets:
    INPUT WINS ADDRESS
    INPUT PROXY ADDRESS
    INPUT PROXY PORT
14. At **USE JITTER BUFFER**, enter **Yes #** or **No ***.
15. At **TECHNICIAN IP ADDR?**, enter the address of the debugging utility, or leave blank.
16. At **STORE IN NVRAM?**, enter **Yes #** to store parameters in non-volatile RAM. This step will ensure that your static setting will be used when the set is powered-up and when the FLASH is upgraded.
17. The set will reboot and will then use the static IP data.

Removing Static IP Addresses on the IP Sets

To return to using dynamic IP addressing when static parameters were previously enabled:

1. Plug the set cable and power into the set while holding down the **Volume Up** key for 3 seconds to display the **STATIC IP SETUP MODE.**
2. At the **USE PRESENT SETTINGS** screen, select *** - DISABLE** to revert back to DHCP from static parameters.

Installing and Configuring Music on Hold

There are three types of Music on Hold available to the system, embedded, analog, and digital.

Embedded Music on Hold is provided by audio files that are imported into a single controller using the System Administration Tool or into multiple controllers using Enterprise Manager.

An Embedded Music on Hold source in use consumes half an E2T resource and each session consumes an E2T resource.

Program Music on Hold in the System Administration Tool:

- System Audio Files Update - download a WAV file (μ-law (G.711), 8 kHz, 8-bit, mono)
- System Options Assignment form - MOH option "Yes"
- Miscellaneous Assignment form - Music Source "Embedded"

Analog Music on Hold is provided by an external music source connected to any one of the following:

- Music on Hold connector (audio jack) on the back of a controller with embedded analog (see Table 43 on page 262)
- Music on Hold connector on the back of a Universal ASU (see Table 66 on page 277)
- Music on Hold connector on a peripheral cabinet E&M trunk card (see Figure 61 on page 281)

Program Music on Hold in the System Administration Tool:

- System Options Assignment form - MOH option "Yes"
- E&M Trunk Circuit Descriptor Assignment form
- E&M Trunk Assignment form
- Miscellaneous Assignment form - Music Source "External"

Digital Music on Hold is provided by an external music source connected to a DNIC Music on Hold/Pager Unit (DMP). The DMP is connected to a peripheral cabinet DNI line card (not supported on the CX/CXi).

Program Music on Hold in the System Administration Tool:

- System Options Assignment form - MOH option "Yes"
- Program the DMP as a single line DNI telephone
- Miscellaneous Assignment form - Music Source "External"

Installing a DNIC Music on Hold/Paging Unit (DMP)

Tip: To reduce the risk of hum or other interference, you should install the DMP close to the music source or paging amplifier and keep the cables to and from the unit as short as possible. If "none" balanced input or output equipment is used, you may need a balancing transformer (not supplied by Mitel).

To install DNIC Music on Hold (not supported on the CX/CXi):

1. Install a DNI line card in a peripheral card slot.
2. Attach the circuit tip and ring leads to the 25th pair of the DMP.
3. Attach the balanced music source to the 7th pair of the DMP via the MDF.

To install a DMP for Paging (not supported on the CX/CXi):

1. Install a DNI line card.
2. Attach the circuit tip and ring leads to the 25th pair of the DMP.
3. Attach the paging adapter interface to the 9th pair of the DMP.
4. If required, attach the page control inputs of the paging adapter via the MDF to the 11th and 12th pair of the DMP.
5. Connect the paging adapter to an appropriate power source (according to the manufacturer’s instructions).
6. Connect the external speakers as required to the paging adapter via the MDF (according to the manufacturer’s instructions).

Chapter 3
Software Procedures

Back Up a Database

Tip: It is very important to maintain current database backups; backups should be done on a regular basis.

Tip: Many of the following procedures assume that you have voice mail. If you don't have voice mail, please disregard voice mail-related steps.

You need the following information and equipment to back up a database:

- ❒ Installation/Maintenance PC (see page 7)
- ❒ IP address of the Controller
- ❒ System Administration Tool username and password

During the first minute of backup, the voice mail system is not accessible (Ring-No Answer). Voice mail will remain in Ring-No Answer state until all voice mail users are disconnected from the system. Ensure that no one is connected to voice mail before you begin your backup.

Verifying if Anyone is Connected to the Voice Mail System

- Ensure that all PLIDs are 'Not applicable' or 'Idle' by using the following maintenance commands in the System Administration Tool: **stat 1 4 27** and **stat 1 4 28**.

Time: The system takes 30 to 90 minutes to back up an average-sized database (50-100 MB), and approximately 4 hours to back up a large voice mail database (600 MB).

To back up the databases:

1. Click **Maintenance and Diagnostics**.
2. Click **Backup**.
3. Copy the **identitydb.obj** file to your PC (required for every user profile on every PC used for backup and restore). Follow the instructions displayed on the screen.
4. Click **Browse** to launch the **Save As** dialog box, then navigate to the location on your local drive where you want to save the backup file (for example C:\3300_ICP\backup).
5. Type a name for your backup file, and then click **Save As**.

6. Select the check box for Call History records and/or Voice mail messages if you want them included in your backup. Each addition can increase the backup time noticeably.
7. Click **Start Backup**. System will display progress and then a backup complete message.

Tip: To perform a backup, your current user account on the computer must have Java™ Plug-in version 1.4.2_06 or later installed. If you do not have the correct version of Java installed, it will be automatically installed when you click Start Backup. The backup will begin after the plug-in is installed.

8. Click **OK**.
9. Verify the presence of the backup file on the local drive.

Tip: During a system backup, no other users can access any of the web-based tools (5140/5240 IP Appliance Online Services, Visual Voice Mail, Desktop Tool, Group Administration Tool, or System Administration Tool), access Visual Voice Mail, or save changes. To avoid blocking other users, we recommended that you perform system backups outside of business hours.

Verifying the Backup

To verify that the backup contains voice mail messages:

1. Add the extension **.tar** to your backup file (for example, change May10 to May10.tar).
2. Use WinZip to open your renamed **.tar** file.
3. Look for the voice mail files:
   - **002Vxxxxxxx.yyy** (where xxxxxxx is a variable, system-generated string) contains all messages.
   - **003msgxxxx.vox** (where xxxx is the extension number) contains the status of messages belonging to that extension.

Restore a Database

Use this procedure to restore a previously saved database.

Tip: The system does not allow you to log in during the restore and reset period. Once the system has completed the restore and reset, you should see "deleting/ipservicesdb.tar" in the RTC. This is a good indication that you can log back in to the System Administration Tool.

CAUTION: You must reboot the controller after restoring a database. Service will be LOST during this reboot.

Tip: You can only restore a Release 3.3 or later database onto a system running Release 4.1 or later software. You may not restore a database saved on software prior to Release 3.3.

Tip: You may not restore an LX or 700-user database onto an MX controller if the database had CIM 3 or 4 configured. You must first delete the unsupported CIM configuration.

Tip: You may not restore an MX database onto an MXe controller if the database had an Analog Option Board (AOB) configured. You must first delete the unsupported AOB configuration.

Tip: You may not restore a database created on one system onto another system if they provide for different numbers of embedded analog circuits. For example, the database from an MX (which provides for 2 ONS and 6 LS) may not be restored onto a CX (which provides for 4 ONS and 6 LS).

You need the following information and equipment to restore a database:

- ❒ Installer PC (see page 7)
- ❒ IP address of the Controller
- ❒ System Administration Tool username and password

To restore a database:

Time: The system takes approximately 30 to 90 minutes to restore an average-sized database, during which time the files are copied to the controller. Once the files have been copied, you must reset the controller. Note that the system can take up to an additional 1 hour to reset.

1. Click **Restore** in the **Maintenance and Diagnostics** menu.
2. Copy the **identitydb.obj** file to your PC (required for every user profile on every PC used for backup/restore). Follow on-screen instructions.

3. Type the location of the database that is being restored, or use the browse facility.
4. Click **Yes** if you want to include Hotel/Motel wake up information in the restore.
5. Prior to Rls 5.1 UR 1:Choose the Dimension Selections (see page 83)
   - accept **Use Dimension Selections from backup file** OR
   - click **Use Current Dimension Selections** if you are restoring the database after programming new Dimension Selection information.
6. Click **Start Restore**.

Tip: To perform a restore, your current user account on the computer must have Java Plug-in version 1.4.2_06 or later installed. If you do not have the correct version of Java installed, it will be automatically installed when you click Start Restore. The restore will begin after the plug-in is installed.

7. Click **OK**. The system will show an "in progress" message.
8. When the status window shows "complete", click **OK**.
9. **Reboot** the controller (see page 99). When the reboot is complete, the database is converted, and the system **automatically resets** (prior to Release 4.0, another manual reboot was required).
   - If you have programmed Dimension Selection, the system reboots automatically one more time.

Tip: While the System Administration Tool is restoring the database, no other users can access any of the web-based tools, access Visual Voice Mail, or save changes. To avoid blocking other users, we recommend that you perform restores outside of business hours.

Verifying the Restore

CAUTION: Do not reset any system components (Controller, NSU, ASU, DSU, Peripheral Cabinet, and so on) while executing the following checks.

CAUTION: Rebooting the controller before the Analog Main Board and Analog Options Board loads can render the boards inoperable.

1. Verify that none of the NSUs are loading. If they are, wait until they have finished loading. To verify that L0/L1 LEDs are not marching, see “Universal NSU LED States” on page 347 and “R2 NSU LED States” on page 348.
2. Log into ESM (using the customer’s username and password), then click **System Administration Tool** and select **Maintenance Commands**.
3. Issue the **dbms stat** maintenance command to check if the DBMS_Initialized flag is ON (look for the line `DBMS info: DBMS_Initialized is ON`).
4. Issue the **Type *.dr.logfile_1** maintenance command to display the log file created during the Data Restore. Wait until the checks are complete, then review the log to ensure there were no errors during the restore procedure.
5. Issue the **message subsystem (me sub)** command to check the programmed NSU links; they should be OPEN. If any programmed links are in SCAN, check the LINK STATUS LEDs; if the amber LEDs are marching, the NSUs are writing to the RAM DISK.

Upgrade/Install System Software

Use the Mitel 3300 ICP Software Installer Tool (latest release) to install or upgrade software or to install a software patch.

Tip: Upgrading to a larger controller or to a faster processor means the replacement of the controller. For example, you cannot upgrade a controller from 300 MHz to 450 MHz, or convert a CX controller to an MX controller.

Tip: When you replace a controller as part of an upgrade, you must move the old hard drive to the new controller, manually install the software, and then use the Software Installer Tool for options and restore.

Software Upgrade Options

Table 2: 3300 ICP Upgrade Options

Upgrade Path	Software Installer Tool
From 3.2 to any later release	Manual install only
From 3.3 to any later release	Full install
From 4.0 to any later release	Full install
4.1.7.6 to 5.x	Upgrade
4.1.7.6 or 5.x to 6.0	Upgrade
4.1.7.6 or 5.x to 7.0.8.4	Full install
6.0 to 7.0.8.4	Upgrade
6.1 to 7.0.8.4	Upgrade

The **Manual install procedure** formats the hard drive and installs new software. Use the manual install procedure to install software:

- on an advanced replacement hard drive
- to rebuild/replace a corrupted database
- to change a hard drive across platforms.

The **Upgrade procedure** upgrades your 3300 ICP controller software.

You must use the Software Installer Tool (always use the latest release) to invoke the upgrade procedure. You may upgrade multiple controllers simultaneously over the LAN. WAN connectivity is not supported.

Tip: Before installing new 3300 ICP software, read the RN for the software you are installing (see “3300 ICP Documentation” on page 9). Verify if any other software/firmware components of the 3300 ICP needs to be upgraded to work with the new software.

CAUTION: If you decrease the number of IP User Licenses or IP Device Licenses, after saving the change, you must perform a backup and restore.

CAUTION: You may not downgrade the CX and CXi controllers to a software version prior to release 6.0. A downgrade would render the controller inoperable.

CAUTION: You may not downgrade the LX controller to a software version prior to release 5.0. A downgrade would render the controller inoperable.

Upgrade/Install Options with Cluster or Dimension Changes

There are install/upgrade requirements to consider when dealing with Maximum Elements per Cluster changes or Dimension Selection changes.

Table 3: Maximum Elements Change or Flexed Dimension Selection

Elements / Dimensions		Software Installer Tool	Notes
From	To		
Prior to Rls 6.0 with Flexed Dimensions	Release 6.0 with Flexed Dimensions	Install only. Do not perform a data restore with the SI Tool. See “Upgrade to Rls 6.0 or later with Flexed Dimensions” on page 84.	After the install is complete, flex the dimensions, reboot, and restore using current dimension selections.
30 or 60 / Flexed Dimension Selection	30 or 60 / Flexed Dimension Selection	Install or Upgrade	Use Dimension Selections from the backup file.
(Page 1 of 2)			

Table 3: Maximum Elements Change or Flexed Dimension Selection (continued)

Elements / Dimensions		Software Installer Tool	Notes
From	To		
30 or 60 / default or Flexed Dimension Selection	250 / default	Install See "To upgrade and change to a default dimension:" on page 83.	Use the existing Dimension Selections. If changing from Flexed Dimensions, it is possible that data may be lost.
30 or 60 / Flexed Dimension Selection	250 / Flexed Dimension Selection	Install only. Do not perform a data restore with the SI Tool. See "To upgrade and change to a flexed dimension:" on page 83.	After the Install and Maximum Element selection, Flex Dimensions, Reboot, and Restore through ESM. Use the existing Dimension Selections.
250 / default	30 or 60 / default	Install See "To upgrade and change to a default dimension:" on page 83.	Use the existing Dimension Selections. It is likely that data will be lost when going from a large database to a smaller one.
250 / default	30 or 60 / Flexed Dimension Selection	Install only. Do not perform a data restore with the SI Tool. See "To upgrade and change to a flexed dimension:" on page 83.	Install, select Maximum Elements, Flex Dimensions, Reboot, and then Restore using ESM. Use the existing Dimension Selections. Data may be lost when going from a large database to a smaller one.

(Page 2 of 2)

Tip: The system software ships with small system dimensions enabled. You enable the large network cluster when you select 250 Maximum Elements per Cluster in the License and Option Selection form. The Default Feature Resources Dimension changes from Dimension 17 to Dimension 19.

Restore Issue - Music on Hold file size

If you restore a pre-Release 6.0 database, with an embedded music on hold file larger than 8 MB (for the MX/LX) or 16 MB (for the LX 512 MB), the file is moved to a temp location and disabled. The following error log is generated: Embedded System Music On Hold Audio source file size exceeds allocated space. It has been disabled and placed in a temporary location: db/temp/system_music_on_hold_tmp.

The relocated file is not backed up and will remain on the hard drive until a full install is performed of until the file is deleted.

To restore music on hold when it is disabled due to file size:

1. Retrieve the **system_music_on_hold_tmp** file from **db/temp/**
2. Reduce the file size.
3. Use the **System Audio Files Update** form, in the System Administration Tool, to restore the smaller music on hold audio file. **OR** create a new audio file within the size limit.

Software Procedure Requirements:

- ❒ Installation/Maintenance PC (see page 7 for requirements)
- ❒ IP address of the 3300 ICP
- ❒ 3300 ICP username and password
- ❒ 3300 ICP software CD
- ❒ Mitel 3300 ICP Software Installer Tool (for a true upgrade)
- ❒ 3300 ICP Mitel Options Password (see page 11)
- ❒ Database backup with voice mail messages (see page 61).

Tip: You need a new password if you have purchased new options. You do not need a new password to change Configuration Options.

Installing the Software Installer Tool

You can install the Software Installer Tool on the Installation/Maintenance PC, or on its own PC (see page 7 for PC requirements).

Tip: Assign a static IP address to the PC running the Software Installer Tool.

Tip: Ports required by the Software Installer Tool and Audio File Manager:
Prior to Release 7.0 - port 2002 and ports 49500-49549
Release 7.0 and later - port 443.

To install the ICP Software Installer Tool:

1. Insert the 3300 ICP software CD-ROM into the Installer PC's CD drive.
2. Open the **Tools** folder, then the **Software Installer** folder.
3. Double-click the **Setup.exe** file. Follow the prompts to install the Tool.

To launch the ICP Software Installer Tool:

1. On the **Start** menu, point to **Programs**, and then click **Mitel 3300 ICP Software Installer**.
2. For ICP Software Installer Tool information, refer to its Online Help.

Tip: Refer to "Requirements for AMC Connection" on page 23 if you wish to manage software licenses online.

Installing System Software on the FTP Server

To install system software on the FTP server:

1. Insert the 3300 ICP software CD-ROM into the installer PC's CD drive.
2. Release 7.0 and later: run the **Mitel_3300ICP_Installation.exe** program from the Software folder on the software CD-ROM.

   Prior to Release 7.0: run the **Setup.exe** program from the Software folder on the software CD-ROM.

   You will see the Installation Wizard Welcome page.
3. Click **Next**, read the License Agreement, and click **Yes** to continue.
4. Choose a location on your local FTP server for the InstallSetup program to install files (default username and password for the controller is ftp and @).
   - Click **Browse** to find the location, and then click **Next** OR
   - Click **Next** to accept the location displayed and continue.

   You will see a read-only list of the configurations you have made.

Tip: If you do not see this list, your FTP server is not installed properly. If the files get installed on the PC's **c:** drive, your FTP server is not installed and you will get a message 'No FTP Server'. Re-install your FTP server.

5. Click **Next**.

Time: The system takes approximately 10 minutes to copy the files.

6. Ensure that the **Read manual instructions to complete the installation** check box is selected, and click **Finish**. The README file opens.

Installing System Software on the Controller

CAUTION: If you have a Universal NSU with a PRI database, you must convert that database before you begin the install (see "Converting a PRI Database on a Universal NSU" on page 76).

To perform a full or new install with the Software Installer Tool:

1. Launch the Software Installer Tool.
2. In the **Identification Screen**, enter the following:
   - 3300 ICP IP Address or DNS Name of the controller onto which you want to install the software
   - System Login ID
   - System Password
3. Click **Configure**. The Full Install Source Definition screen appears.
4. Select **Perform Full Install**. Enter the following information:
   - FTP Server IP Address
   - FTP Account Name
   - FTP Password
5. Click **Next** to open the Define Full Install Options screen.
6. Select the desired upgrade install options. All four options are selected by default.
   - **Backup** to create a Backup File
   - **Install** to Install the Software
   - **Configure** to configure the License and Options
   - **Restore** to restore your Database
7. Click **Next** to launch the License and Option Selection screen.

8. Enter the Purchased Options, Password, and Configuration Options from your Mitel Options sheet.
9. Click **Next**.
10. Click **Start** on the Installation In Progress screen.

Time: This process takes approximately 45 minutes.

Upgrading System Software

Time: This process will take approximately 1 to 2 hours including the backup, restore, and reboot.

CAUTION: If you have a Universal NSU with a PRI database, you may need to convert that database before you begin the upgrade. Refer to page 76 and the RN for conditions.

Tip: To minimize the size of the database, you may want to ask your users to delete any unneeded voice mail messages.

CAUTION: You may not downgrade the LX controller to a software version prior to release 5.0. A downgrade would render the controller inoperable.

CAUTION: You may not downgrade the MXe controller to a software version prior to release 7.0. A downgrade could render the controller inoperable.
PC or Layer2 switch connection must be to Ethernet port 1.

To perform an upgrade with the 3300 Software Installer Tool:

Note: The upgrade requires a change to a different set of DHCP options (43/60 or 124/125) used to configure Mitel IP endpoints. The change is due to reclassification of DHCP options by the Internet Engineering Task Force (see RFC 2133 and RFC 3925). The old options can still be used to provide backward compatibility with IP sets that have yet to be upgraded with firmware that supports the new options. After the upgrade, the old options may be removed to prevent future conflicts with standard use or other vendors' use of these options. The change to the new options is automatic for the internal DHCP server.

Note: If you intend to rely on LLDP VLAN Discovery in the network, you must first upgrade the 3300 ICP to Release 7.0 or later and upgrade the IP Phone firmware to version 2.0.0.18 or later.

Note: LLDP-MED non-compliant telephones cannot use LLDP for VLAN discovery. They must use DHCP VLAN discovery. Non-compliant sets are: 5001, 5005, 5010, 5020 IP Phones, 5140 IP Appliance, 5201, 5205, 5207, 5215 (single mode), 5220 (single mode), 5230 IP Phones, 5240 IP Appliance, 5485 IP Pager, and 5550 IP Console keypad.

1. Ensure that you have an off-board database backup before you begin.
2. Install system software on the FTP server (see page 70).
3. Launch the Software Installer Tool.
4. In the **Identification Screen**, enter the following:
   - 3300 ICP IP Address or DNS Name of the controller to upgrade
   - System Login ID and System Password
5. Click **Configure**. The Upgrade Source Definition Screen appears.
6. Click **Perform Upgrade**. Enter the following information:
   - FTP Server IP Address, FTP Account Name, and FTP Password
7. Click **Next** to launch the Define Upgrade Options screen.
8. Select the desired upgrade options. The options are:
   - **Backup** - select only if you don't already have a backup (this backup is the call control only; not voice mail or Embedded T1/E1)
   - **Upgrade** - not an optional selection
   - **Configure** - select only if you need to add a new option or change existing Licensed Options
   - **Restore** - select to restore Hotel/Motel wake-up messages.
9. Click **Next**.
10. Click **Start** on the Upgrade In Progress screen.
11. Clear your PC's browser cache and distribute new software to all IP Phones when you upgrade a controller in a resilient cluster (page 75).

Tip: After you upgrade the 3300 ICP software, you must reboot the 3300 CITELlink Gateway in order for the gateway to load the new software.

Tip: If the system includes IP DECT wireless phones, reboot each Open Mobility Manager (OMM) in the IP DECT system after the upgrade. Refer to the IP DECT Technical Manual for instructions. When you reboot the OMMs, the Radio Fixed Parts (RFPs) will obtain the latest firmware (iprfp.bin file) from the 3300 ICP controller.

12. After the upgrade, follow the instructions below to reprogram the DHCP server(s) to use the new DHCP options.

Reprogram the internal DHCP server (required for Release 7.0)

1. Check the **DHCP Options** form for previously programmed options 128 - 133 values. Ensure that the values have been correctly converted to Option 125 for all defined scopes in the DHCP server(s) of all upgraded controllers.

Note: DO NOT delete Options 128-133 yet.

2. After the upgraded controllers are returned to service, and all IP Phones have re-homed to them, use the LOAD IP 1-700 maintenance command to force a firmware reload of all devices.

3. Delete old options 128-133 on all controllers.

Reprogram external DHCP servers (required for Release 7.0)

Note: If you intend to rely on LLDP VLAN Discovery in the network, you must first upgrade the 3300 ICP to Release 7.0 or later and upgrade the IP Phone firmware to version 2.0.0.18 or later.

Note: LLDP-MED non-compliant telephones cannot use LLDP for VLAN discovery. They must use DHCP VLAN discovery. Non-compliant sets are: 5001, 5005, 5010, 5020 IP Phones, 5140 IP Appliance, 5201, 5205, 5207, 5215 (single mode), 5220 (single mode), 5230 IP Phones, 5240 IP Appliance, 5485 IP Pager, and 5550 IP Console keypad.

1. Use option pairs 60/43 or 124/125, whichever is most appropriate for the customer's environment.

2. Ensure that previously programmed options 128-133 values are in place for the global scope and any defined sub-scopes in the DHCP server(s).

Note: DO NOT delete Options 128-133 yet.

3. Ensure that the TFTP server pointed to by option 128 corresponds to a server (possibly an upgraded ICP) that contains the new IP Phone software loads.
4. On the DHCP server(s), create a global scope corresponding to option 60 or option 124 (as selected above). Repeat for each sub-scope (if any).
5. On DHCP server(s) define option 43 or option 125 (as selected above) for each newly created scope. See the 3300 System Administration Tool Help for information on formatting the required option strings.

Note: The values used in the option 43 string must correspond exactly to previous option 128-133 values.

6. After the upgraded controllers are returned to service, and all IP Phones have re-homed to them, use the LOAD IP 1-700 maintenance command to force a firmware reload of all devices.
7. Delete old options 128-133 on all DCHP servers.

Distributing New Software to IP Phones

Use this procedure for IP Phone software distribution after you upgrade any controller in a resilient cluster.

1. Update all TFTPs in the scope of the upgraded controller's cluster.
2. Wait for all IP devices to return to their primary ICP (now upgraded).
3. Use the LOAD IP 1-700 maintenance command to force a firmware reload of all devices.

Clearing the Browser Cache

To clear the browser cache in your administration PC:

1. Launch Internet Explorer.
2. Click **Internet Options** in the **Tools** drop-down list.
3. Click **Clear History** and then click **Yes**.
4. Click **Delete Files**, check **Delete all offline content**, and click **OK**.

Converting a PRI Database on a Universal NSU

To convert a Universal NSU PRI database:

1. Install the IMAT that is on the 3300 software CD-ROM (see page 88).
2. Launch the new IMAT and connect to the Universal NSU.
3. Load the database from your previous IMAT backup.
4. Select PRI 8.2 or NSU 1.4 for your new database version.
5. Convert the database and then save the new database into the NSU.
6. Return to step 2 of the upgrade procedure (see page 72).

3300 ICP Software Version	Universal NSU Database Version
Up to release 3.3	PRI 8.0 or NSU 1.1
Release 4.0	PRI 8.1 or NSU 1.2
Release 4.1, 5.0, or 5.1	PRI 8.2 or NSU 1.3
Release 5.1	PRI 8.2 or NSU 1.4
Release 5.2, 6.0, or 6.1	PRI 8.2 or NSU 1.5
Release 7.0	PRI 8.2 or NSU 1.6

Applying a Software Patch

Use the Software Installer Tool to apply a software patch, from Release 4.1 and later. Get the patch (service pack) from Mitel OnLine or from Technical Support.

Time: This process takes approximately 15 to 30 minutes including reboot.

To apply a software patch with the Software Installer Tool:

1. Copy the service pack software to a directory on the FTP Server.
2. Launch the Software Installer Tool.
3. In the Identification Screen, enter the following:
   - 3300 ICP IP Address or DNS Name of the controller to which you want to apply the patch
   - System Login ID
   - System Password

4. Click **Configure**. The Patch Definition Screen appears.
5. Click **Apply Patch**.
6. Specify the path of the patch source by typing a path in the text box or clicking the **Browse** button and navigating to a path.
7. Choose to reboot immediately or to reboot manually later. You must reboot your system for the patch installation to take effect.
8. Click **Next** to view the FTP validation dialog box. This will test the FTP connection credentials. Click **Cancel** in this window to return to the Source Definition Screen.
9. The FTP validation dialog box is displayed. Following successful testing, the Patch Install In-Progress Screen is displayed.

Installing System Software Manually

Use this manual procedure to install software prior to Release 3.3, when a hard drive must re replaced, or to upgrade software prior to Release 4.1.7.5. In all other cases, we recommend that you use the 3300 ICP Software Installer Tool.

Time: The complete manual install procedure takes approximately 2 hours for an average-sized database (50-100 MB) and approximately 4 hours for a large database (600 MB), including the database restore.

CAUTION: The software install procedure will format the controller hard drive and install new software. The procedure will erase all system settings, including voice mail messages, so you must back up your database. If you do not have a database backup to restore, you will have to reprogram the system.

The manual upgrade/install procedure consists of the following sub-procedures, all of which **must be completed in order**:

- ❒ Steps 1-2: Establish a Connection to the Controller (page 78).
- ❒ Step 3: Back up the 3300 ICP database page 78.
- ❒ Steps 5-10: Reboot the Controller (page 79).
- ❒ Steps 11-12: Set Your Purchased Mitel Options (page 81).
- ❒ Step 13: Restore the Database OR Program the System (page 81).

- ❒ Steps 16-20: Perform the Maintenance Checks (page 82).
- ❒ Steps 21-22: Upgrade IP phones and force lease renewals (page 82).

Tip: Ensure that no one else makes changes to the database once you've backed up the database. Any changes not included in your backup will be lost when the system is restored.

Tip: If a Security Information Warning pop-up window appears during this procedure, click **Yes** to continue.

Establish a Connection to the Controller

Tip: You can connect directly to the controller through an Ethernet port. You can also connect to the controller through the LAN. WAN connectivity is not supported.

1. Using an RJ-45 Ethernet cable, connect the Installer PC directly to one of the 3300 ICP Ethernet ports, or through the Layer 2 switch (required for the MX and, 100-user systems). For the CX, use LAN port 17. For the MXe, use LAN port 1.

Tip: The Installer PC must be on the same subnet as the RTC IP address; otherwise, a router will be required on your network, and the gateway IP address of that router must be applied to the RTC setup as well as to the Installer PC. Also make sure that the Installer PC's IP address does not conflict with any other IP addresses.

Tip: Check the FTP site properties and ensure that the FTP username has the proper permissions. If you use another username, make sure that it permits you to access the FTP server in the IIS/PWS-FTP site and also that it is programmed on the RTC (see "Installation and Upgrade" on page 183 for more information).

2. From the Installer PC, PING the 3300 controller to verify that you have established a connection.
3. Back up the 3300 ICP database (including voice mail for an install/restore) to the Installer PC (see page 61).

CAUTION: If you have a Universal NSU with a PRI database, you may need to convert that database before you begin the upgrade. Refer to "Converting a PRI Database on a Universal NSU" on page 76 and the RN for conditions.

Install the Software on the FTP Server

4. Refer to “Installing System Software on the FTP Server” on page 70, Step 1 through Step 6.

Reboot the Controller

5. Launch your VT100 emulator communications program.
6. Type **appShutdown**, and press ENTER. The controller reboots.
7. The communication program will instruct you to **Press <SPACE><SPACE><SPACE> to stop auto-boot AFTER countdown starts** (Release 5.2 and later) or **Press any key to stop auto-boot** (prior to Release 5.2). You have 7 seconds to press a key or the system will auto-boot.

Tip: If you miss the 10-second timeout, manually reboot the controller by pressing the **Reset** button. The RTC opens, and you once again have 10 seconds to complete Step 7.

8. At [VXWorks Boot] type **c**, and press ENTER.
9. For each setting shown in **bold** (see Table 4 below), type the table value, then press ENTER. For all other settings, press ENTER to accept the default value.

Tip: The VXWorks parameters are case-sensitive.

Table 4: VxWorks Settings

Prompt	Value	Note
boot device	**motfcc**	Boot device is Network.
processor number	0	Not used.
host name	bootHost	
file name	**Boot_Install**	Boot location and file name.
inet on ethernet (e)		IP address and subnet mask (hex) for controller RTC (for example, 134.199.63.11:ffffff00). Obtain it from your IT administrator.
inet on backplane (b)		
host inet (h)		IP address of Installer PC. Used for software upgrades.
gateway inet (g)		IP address of the end user's default gateway for the 3300 ICP (must be outside the DHCP range).
user (u)	ftp	
ftp password (ftp)	ftp	
flags (f)	0x0	Uses host inet IP address.
target name (n)		
startup script (s)		
other (o)	motfcc	

10. At [VXWorks Boot], type @, or press the controller **Reset** button.

Time: The system takes approximately 30 minutes to format the hard drive and install the software.

Tip: If you get an error message see "Installation and Upgrade" on page 183. After the software install is complete, the file name for all platforms, for Release 6.0 and later will be: /partition1/Rtc8260.

Tip: Prior to Release 6.0: LX, 250/700-user: /partition1/Rtc8260; MX: /partition1/Lite200UP; 100-user: /partition1/Lite8260.

Tip: Continue with Step 11 by using the **System Administration Tool**, or you can continue by using the **Software Installer Tool** (see "Installing System Software on the Controller" on page 71).

Log into the 3300 ICP ESM

11. Launch Internet Explorer, and type the IP address of the controller (for example, http://<RTC IP address>). Log into the 3300 ICP ESM using the default username (**system**) and password (**password**).

Tip: The Installer PC must have the same subnet address as the RTC IP (for example, 192.168.1.n) to launch ESM.

Tip: If your login fails, it may be because the system is not finished loading. Log in when you see the message "**Voice Mail Successfully Started"**.

Set Your Purchased Mitel Options

12. Set the options in the **License and Option Selection** form according to your purchased Mitel options (refer to your records or go to AMC (see page 26)).

Tip: Since the installation of new software erases all of your system settings, you must complete this form even if you have not purchased any new options.

a. In the **All forms (alphabetical)** list, click **License and Option Selection**. Click **Change** in the top right corner.

b. Enter the information for the system options you purchased.

c. Enter your Mitel Options Password in the **Password** field.

d. Change the **Configuration options** as needed.

Tip: We recommend that you enable **Networking Option** and **Mitai/Tapi Computer Integration**.

e. Click **Save**. A pop-up window instructs you to restore or reboot. Click **OK** to close the window.

Restore the Database OR Program the System

13. To restore a database, refer to page 63, and continue with Step 15.

14. If you do not have a database backup:

- **Reboot** the controller (see page 99).
- Program the system using the System Administration Tool.
- Issue the **dbms save** maintenance command.
- Enter the **dbms stat** command to verify the DBMS save, and that the **DBMS_Initialized** flag is on.

Perform the Maintenance Checks

Tip: Complete the following Maintenance Checks only after a restore.

CAUTION: Do not reset system components while executing the following checks.

15. Verify that none of the NSUs is loading. If they are, wait until they have finished loading (L0/L1 LEDs are not marching).
16. When the system has finished resetting, log back into ESM.
17. In the **All forms (alphabetical)** list, click **Maintenance Commands**.
18. Enter the **dbms stat** command to verify the DBMS save, and that the **DBMS_Initialized** flag is on.
19. Issue the **Type *.dr.logfile_1** command to display the log file created during the Data Restore. When the checks are complete, review the log to ensure there were no errors during the restore procedure.
20. Issue the **mess sub** command to check the programmed NSU links; they should be OPEN. If any programmed links are in SCAN, check the LINK STATUS LEDs; if the amber LEDs are marching, this means that the NSUs are writing to the RAM DISK.
21. Upgrade the IP telephones and force lease renewals. Issue the **LOAD IPDevice 1 to X** maintenance command (where X represents the last IP device number) to upgrade the IP phones.
22. If the system has a peripheral cabinet with DNI line cards, enter the **Load x x x** command to load the DNI cards and the latest DNI line load.

Tip: If you have an IP console, you must:

- Cycle the power on the IP TKB (key pad).
- Upgrade the IP Console software (if required).
- Renew the IP address for the console PC (if required). Power down or at the DOS prompt enter **ipconfig /release** and then **ipconfig /renew**.

23. Back up the database (see "Back Up a Database" on page 61).

Upgrading/Installing with Maximum Elements Change

The following options have some impacts to the upgrade/install procedure that you need to be aware of:

To upgrade and change to a default dimension:

- **30/60** maximum elements per cluster (with **default or flexed** dimensions) to **250** maximum elements(with **default** dimensions)
- **250** maximum elements per cluster (with **default** dimensions) to **30/60** maximum elements per cluster (with **default** dimensions)

1. Back up the database (see page 61).
2. Follow the standard full install procedure (see page 71) using the Software Installer Tool.
   - In the **License and Options Selection** form change **Maximum Elements per Cluster** to or from **250**. The Software Installer Tool will reboot the controller.
3. **Restore** the database (see page 63). Click the **Use the existing/current Dimension Selections** radio button.
4. When prompted, **reboot** the controller (see page 99).
5. Back up the database (see page 61).

To upgrade and change to a flexed dimension:

- **30/60** maximum elements per cluster (with **default or flexed** dimensions) to **250** maximum elements per cluster (with **flexed** dimensions)
- **250** maximum elements per cluster (with **default or flexed** dimensions) to **30/60** maximum elements per cluster (with **flexed** dimensions)

1. Back up the database (see page 61).
2. Print the **Dimension Selection** form if you have flexed dimensions.
3. Follow the standard full install (see page 71) procedure using the Software Installer Tool, but do not Restore; **clear the Restore button**.
   - In the **License and Options Selection** form, change **Maximum Elements per Cluster** to or from **250**. The Software Installer Tool will reboot the controller.

4. Complete the remaining steps in this procedure using the System Administration Tool. Log into ESM using the customer's username and password (see page 8), then click **System Administration Tool**.
5. Program **Dimension Selections** to modify Dimension 19. If you had flexed dimension 17, program **Dimension Selections** using the printed dimensions from step 2 (see Change the Resource Dimension in the online help for details).
6. **Reboot** the controller (see page 99).
7. **Restore** the database (see page 63). Click the **Use the existing/current Dimension Selections** radio button.
8. When prompted, **reboot** the controller (see page 99).
9. Back up the database (see page 61).

Upgrade to RIs 6.0 or later with Flexed Dimensions

Use the Software Installer Tool to install the Release 6.0 or later software and then use the System Administration Tool to restore your database.

To upgrade to Release 6.0 or later with flexed dimensions:

1. Print the Dimension Selection form.
2. Launch the Software Installer Tool.
3. In the **Identification Screen**, enter the following:
   - 3300 ICP IP Address or DNS Name of the controller onto which you want to install the software
   - System Login ID
   - System Password
4. Click **Configure**. The Full Install Source Definition screen appears.
5. Select **Perform Full Install**. Enter the following information:
   - FTP Server IP Address
   - FTP Account Name
   - FTP Password
6. Click **Next** to open the Define Full Install Options screen.
7. Clear the Restore radio button. All four options are selected by default.
   - **Backup** to create a Backup File
   - **Install** to Install the Software

- **Configure** to configure the License and Options
- **DO NOT** select **Restore**

8. Click **Next** to launch the License and Option Selection screen.
9. Click **Next** to accept options without modification. DO NOT change the Maximum Elements.
10. Click **Next**.
11. Click **Start** on the Installation In Progress screen.

Time: This process takes approximately 45 minutes.

12. After the installation is complete, log into the System Administration Tool.
13. In the **Dimension Selection** form, change dimensions to match the quantities in the form that you printed in step 1 and click **Save**.
14. Reboot the system.
15. Launch the System Administration tool.
16. In the **Restore** form, select **Use current Dimension Selections (*select if Dimensions were modified*)**.
17. Click **Start Restore**.
18. Reboot the system.
19. Back up the database.

Programming Overview

- ❒ Optional: use the ICP Software Installer Tool to restore a saved database or, from 3300 Release 7.0 UR1, to migrate a database (from SX-2000 LIGHT, SX-2000 MicroLIGHT, 3200 ICP, or 3800 WAG systems). Prior to Release 7.0 UR1, use the 3300 Configuration Tool to migrate a database from legacy systems. Refer to the ICP Software Installer help system for programming information.
- ❒ Use the System Administration Tool to program the 3300 ICP. See the System Administration Tool online help for programming information.
- ❒ Optional: Use the System Administration Tool to program networks or clusters of 3300 ICPs. Refer to the Voice Clustering (Portable Directory Number) Guide on Mitel OnLine for planning information. Refer to the System Data Synchronization book in the System Administration Tool online help for programming instructions.
- ❒ Use IMAT to program PRI/QSIG and R2 NSUs (does not apply to Embedded T1/E1).
- ❒ Use the System Administration Tool to program the required voice mail settings in the Voice Mail folder. Refer to the Online Help for more information.

Tip: These settings will not take effect until you reboot the system.

Tip: If you have not already done so, perform a DBMS Save (Step 4 on page 26) or verify that the DBMS_Initialized flag is on (Step 5 on page 26).

Basic Hardware Programming

Refer to the System Administration Tool Online Help for programming.

- "Basic Programming and Data Save" on page 25
- "Programming DHCP" on page 29
- "Programming the Controller DHCP Server Settings (for Release 7.0 and later)" on page 31
- "Configuring the Layer 2 Switch" on page 35
- "Programming the Peripheral Cabinet" on page 45
- "Programming Phones" on page 52.

Install 6000 MAS Software

You will need this procedure only if you have to replace the Application Processor Card (APC) hard drive. When you purchase the APC, with it's hard drive, the 6000 Managed Application Server (MAS) software is already on the hard drive.

Refer to "APC Hard Drive (CXi)" on page 121 to install the hard drive.

To install the 6000 MAS software:

1. Insert the 6000 MAS software CD into a portable CD-ROM drive attached to a USB connector located on the front panel of the 3300 ICP.
2. Power down the 3300 controller (see page 99).
3. Power up the 3300 controller.
4. Launch the secure telnet client.
   - Enter open <RTC IP address> using port <2005> (command with example IP address, **open 192.168.1.2 2005**).
   - Enter the 3300 username and password.
5. Follow on-screen instructions to configure the 6000 MAS and blades. Refer to the 6000 Managed Application Server documentation on Mitel OnLine.

Install and Use IMAT

The ISDN Maintenance and Administration Tool (IMAT) software is used to program PRI and R2 cards and Network Services Units. IMAT is also used to install PRI card and R2 card software.

Tip: IMAT is not applicable for the CX and CXi controllers.

Tip: IMAT is not needed to program Embedded PRI, T1/D4, and QSIG (dual T1/E1 framer module or T1/E1 combo module in the controller).

Tip: You must have IMAT software version 7.3 or greater to use with Release 4.1 or greater of the 3300 ICP software. Use IMAT version 7.4 with Release 5.1 of the 3300 ICP software.

Installing IMAT on the PC

You can install IMAT on the Maintenance PC or on its own PC (IMAT PC).

Tip: We recommend using an Ethernet connection from the IMAT PC when running Windows NT 4.0, Windows 2000 Professional, Windows XP, or Windows 98. For Windows 95/98 (without a NIC), use Dial-up Networking.

To install IMAT on the PC:

1. Close all the applications running on the PC.
2. Insert the 3300 ICP software CD-ROM in the CD drive.
3. Open the **Tools** folder, then the **Disk 1** folder.
4. Double click the **Setup.exe** file. The installation program starts. Follow the prompts to install IMAT.
5. Connect the NSU Ethernet port directly to the NIC of the PC using a crossover cable or connect the NSU Ethernet port to the network.

Tip: Refer to the IMAT online help for LAN connection details. If you're using a dial-up connection, see "Connect a Windows 95/98 PC to the NSU via Dial-Up" on page 90.

Programming an IP Address into the NSU

You must change the IP and gateway addresses to match an available address on the LAN.

To program the IP address that IMAT will access:

1. Program the PC's serial port with a baud rate of **38400**.
2. Connect the IMAT PC to the NSU serial port.
3. Establish a terminal session with the NSU card.
4. Reboot the NSU.
5. Press any key during auto-boot to halt the boot process.
6. At the **[MC269AA Boot]-**: prompt enter **C**.
7. Change the boot parameters, **inet on ethernet (e) : 192.168.1.1:ffffff00** and for **gateway inet (g) : 192.168.1.251** default values to the values provided to you by your LAN administrator.
8. For all other settings, press ENTER to accept the default.

```
boot device          : flash
unit number          : 0
processor number     : 0
host name            : pc5147
file name            : vxworks
inet on ethernet (e) : 192.168.1.1:ffffff00
gateway inet (g)     : 192.168.1.251
ftp password (pw)    : vxworks
flags (f)            : 0x0
target name (tn)     : dass2
other (o): flash,c:/,xqt,b_loader.cmd
```

9. At [VXWorks Boot], type @, or press the **Reset** button on the controller.
10. Connect the NSU Ethernet port to the LAN.

Dial-up Connection of the IMAT PC to the NSU

For Windows 95 and Windows 98, refer to "Connect a Windows 95/98 PC to the NSU via Dial-Up" on page 90.

For Windows 4.0, Windows 2000 Professional, or Windows XP without a NIC, refer to IMAT Online Help for Dial-up connection details.

Using IMAT

For more information, refer to the IMAT online help.

To log onto an IMAT computer:

1. Launch IMAT from the **Start** menu or the desktop (ignore any message about username configuration error).
2. On the **File** menu, select **Connect to Remote Site.**
3. Click to select **Ethernet Network Card** in the Connection Medium field.

To exit the IMAT application:

1. **Save** any open databases.
2. On the **File** menu, click **Exit**.

Connect a Windows 95/98 PC to the NSU via Dial-Up

Tip: You can also connect the PC to the NSU via a modem (remote connection). For more information, see the IMAT Online Help.

Tip: Refer to the IMAT online help for dial-up connection details when your PC is running on Windows NT 4.0, Windows 2000 Professional, or Windows XP without a NIC.

By default, Windows does not support a direct cable connection. You must add a device driver. Windows takes the information from a Mitel file and creates the driver called NT Direct Connection.

To install a Direct Connection Device Driver (Windows 95/98):

1. On the **Start** menu, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Modems** icon.
3. In the **Modem Properties** window, click **Add**.
4. In the **Install New Modem** screen, click **Other**.
5. Select **Don't detect my modem, I will select from a list**, then click **Next**.
6. Click **Have Disk**.
7. Type **c:\Program Files\Mitel\Imat** in the **Copy manufacturer's files from** field, then click **OK**.
8. In the **Install from Disk** window, click **OK**.

9. Click **Next** to select the NT Direct Connection.
10. Select **COM 1** or **COM 2**, and then click **Next**.
11. Click **Finish**.
12. In the **Modem Properties** window, select **NT Direct Connection**, then click **Properties**.
13. Set the following parameters:
    - Maximum speed: **38 400**
    - Check: **Only connect at this speed**
    - Data bits: **8**
    - Parity: **None**
    - Stop bits: **1**
    - Mode: **Auto Answer**

    In **Advanced Settings** window, do the following for a direct connect cable:
    - Turn off: **Error control**
    - Turn off: **Flow Control**
14. Click **OK** and close the Control Panel window.

Physically Connecting the PC to an NSU

- Connect an RS-232 straight DTE serial cable between the NSU's serial port and the PC's serial port.

Tip: If you are connecting through a modem, use a null modem adapter on the NSU side.

Creating a Dial-Up Network Connection on Windows 95/98

Typically, you need to follow this procedure twice to create two Dial-up Networking connections, one for on-site direct access, and one for remote modem access.

1. On the **Start** menu, point to **Programs**, point to **Accessories**, and then click **Dial-Up Connections**.
2. Double-click **Make New Connection**.
3. Enter an appropriate name for the connection (for example, Direct for direct connections, Remote or a customer's name for remote connections) and click **Next**.

Tip: If you are creating a direct connection, make sure NT Direct Connection is listed in the drop-down list in the **Make a New Connection** window.

4. Enter an **Area Code** and **Telephone Number** and select a **Country Code** from the drop-down list. Click **Next**. Click **Finish**.
5. Right-click your new connection icon and click **Properties**.
6. Click **Configure**. Ensure the fields are set as follows:
   - Data bits: **8**
   - Parity: **none**

   For a direct connection:
   - Maximum speed: **38400**
   - Check: **only connect at this speed**
   - Select: **wait for dial tone before dialing**
   - Select: **cancel the call time at 60 sec**
   - Click **Advanced** and turn off **error control** and **flow control**

   For a remote connection:
   - Stop bits: **1**
   - Click **Advanced** and turn on **error control** and select Compress data.
   - Turn on **flow control** and select Hardware.
7. Click **OK**.
8. Select **Server Types** tab and make sure that PPP: Windows, WindowsNT3.5, Internet or PPP:Internet appears in the Type of Dial-Up Server field.
9. In the **Advanced Options** field, select **Log onto Network and Enable software compression**.
10. Make sure that only **TCP/IP** is selected in the **Allowed network protocols** field.
11. Select the **Scripting** tab and enter:
    - for a 3300 Universal NSU: **c:\program files\mitel\ Imat\pridun.scp**.
    - for an R2 NSU: **c:\program files\mitel\Imat \r2dun.scp**.
12. Click **OK**.

Install the Java Plug-In

The Java plug-in comes with the 3300 ICP software and must be installed on the Installer PC for every user profile. During backup/restore procedures, the software detects whether the proper version of Java Plug-in has been installed. If not, it will prompt you to install the correct version with the installation wizard. You need Java version 1.4.2_06 for 3300 ICP Release 4.0 and later.

The **identitydb.obj** file must be present on every profile for every computer that will be used for a database backup or restore. Installation instructions are on the Backup and Restore screen in the System Administration Tool.

Tip: We recommend that you avoid running multiple versions of the Java plug-in. If you are running the incorrect version for the upgrade, you should uninstall it from every PC used as a 3300 ICP administrator, and allow the software to install the correct version, during the next backup/restore, on each PC.

Chapter 4
Upgrades and FRUs

About this Chapter

This chapter contains the following sections:

Tip: For information on installing the 3300 ICP, see Chapter 2: “Installation” on page 13. For information on upgrading the system software, see “Upgrade/Install System Software” on page 66.

Safety Considerations

WARNING: READ THE SAFETY INSTRUCTIONS BEFORE PERFORMING THE PROCEDURES IN THIS CHAPTER (SEE "SAFETY INSTRUCTIONS" ON PAGE 3).

WARNING: FAILURE TO FOLLOW ALL INSTRUCTIONS MAY PRESENT A RISK OF ELECTRICAL SHOCK.

CAUTION: To prevent ESD damage to the equipment: (1) Ensure that the system is grounded before you install a card. (2) Whenever you handle cards, wear an anti-static strap (always attach the wrist strap from the cabinet). (3) When removing cards from the cabinet, immediately place them in an anti-static bag.

CAUTION: All installation, field replacement, and servicing procedures must be carried out by service personnel who have successfully completed the Mitel Installation and maintenance training course.

CAUTION: Hardware is sensitive to shock and vibration; handle hardware with care.

Upgrade a 3300 ICP

Use Table 1 on page 18 for a view of controller component options. See page 235 to view the controller speed. Refer to page 66 for software upgrade options.

Tip: Upgrading to a larger controller or to a faster processor means the replacement of the controller. For example, you cannot upgrade a controller from 300 MHz to 450 MHz, or convert a CX controller to an MX controller.

Adding Resiliency

For information on upgrading to a resilient system, refer to the 3300 ICP Resiliency document on Mitel OnLine.

Power Down the Controller

To power down the controller, Release 7.0 and later:

1. In the System Administration Tool, navigate to Maintenance Commands.
2. Enter the **Shutdown** command.
3. Remove power:
   - for the MXe, set both power switches to OFF
   - for all other controllers, remove the power cord.

To power down the controller, prior to Release 7.0:

1. Type **appShutdown** at the RTC shell.
2. When the controller boots up, the communication program will instruct you to **Press <SPACE><SPACE><SPACE> to stop auto-boot AFTER countdown starts** (Release 5.2 and later) or **Press any key to stop auto-boot** (prior to Release 5.2).

Tip: Prior to Release 7.0, complete steps 1 and 2 to stop the system from auto-booting.

3. Remove the power cord.

Perform a System Reset

To reset the system, Release 7.0 and later:

1. In the System Administration Tool, navigate to Maintenance Commands.
2. Perform a system reboot by using the **reset system** command.

To reset the system prior to Release 7.0:

1. In the System Administration Tool, navigate to Maintenance Commands.
2. Perform a system reboot by using the **LOAD 1** c

Removing/Replacing LX/700-User Controller Cover

To remove the LX/700-user controller cover:

1. Power down the controller (page 99).
2. Disconnect all cables.

3. Remove the controller from the rack (if applicable) and place it on a suitable work area.
4. Remove the front faceplate (clip it off).
5. Turn the controller over gently, keeping the front panel facing forward.
6. Remove the two screws from the underside of the controller.
7. Turn the controller the right side up and rotate it until the back panel unit is facing you.
8. Remove the two screws from the back panel.
9. Slide the cover forward until it catches, then tilt the cover up to remove.

To install the LX/700-user controller cover:

1. Turn the controller until the back panel is facing forward.
2. Lift the lock for the AC power cord and place the cover at an angle to hook onto the back of the unit.
3. Straighten and slide the cover forward as far as it will go.
4. Secure the shell by inserting and snugly securing the two screws on the back panel.
5. Turn the controller gently upside down.
6. Secure the screws on the bottom front of the unit.
7. Turn the controller right side up.
8. Clip on the front face-plate taking care not to damage the protruding FIM connectors.
9. Reinstall the controller into the rack (if applicable).
10. Reconnect all cables.
11. Power on the unit.

Removing/Replacing MX/100-User Controller Cover

To remove the MX/100-user controller cover:

1. Turn off the power to the unit.
2. Disconnect all cables.
3. Remove the controller from the rack and place it on a suitable work area.

4. Remove the four screws from the top of the controller.
5. Slide the cover back and tilt up to remove.

To install the MX/100-user controller cover:

1. Tilt and slide the cover forward under the front faceplate.
2. Secure the four screws on the top of the unit.
3. Reinstall the controller into the rack (if applicable).
4. Reconnect all cables.
5. Power on the unit.

Removing/Replacing CX/CXi/MXe Controller Cover

To remove the CX/CXi and MXe controller cover:

1. Unplug the power cord from the controller and disconnect all cables.
2. Remove the controller from the rack and place it on a suitable work area.
3. Loosen the captive screw at the back panel of the controller (1).
4. Grip the handle on the plastic trim plate and pull back about 1/2” until the cover catches (2).
5. Lift the cover upward to remove it (3).

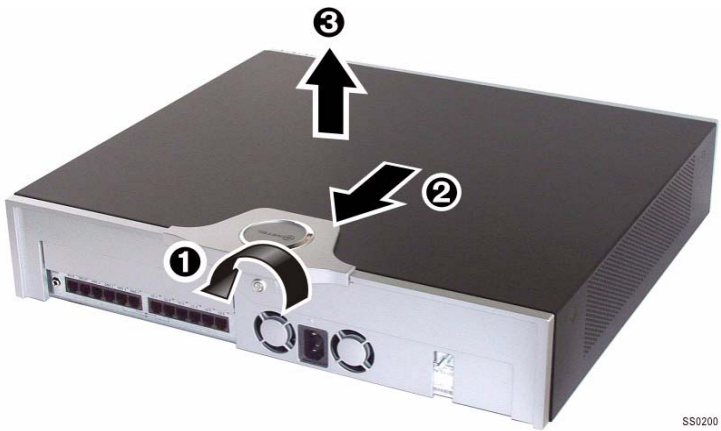


Figure 9: CX/CXi Controller - Removing the Cover

To install the CX/CXi and MXe controller cover:

1. Turn the controller until the front panel is facing forward.
2. Align the pins inside the cover with the corresponding slots on the controller, and then, with the cover about half an inch from the back, lower the cover to seat it.
3. Slide the cover toward the back of the controller as far as it will go.
4. Tighten the screw on the back panel.
5. Reinstall the controller into the rack (if applicable).
6. Reconnect all cables.
7. Power on the unit.

Upgrading to a 300 or 450 MHz Controller

If you have a 133 MHz controller, you can replace it with a 300 MHz controller. You can replace a 700-User 300 MHz controller with 450 MHz controller. 64 compression channels requires a minimum 300 MHz controller.

WARNING: TO UPGRADE TO A 300 OR 450 MHZ CONTROLLER, MOVE THE HARD DRIVE FROM THE OLD CONTROLLER TO THE NEW CONTROLLER. MANUALLY INSTALL THE RELEASE 5.0 SOFTWARE (SEE "INSTALLING SYSTEM SOFTWARE MANUALLY" ON PAGE 77) AND RESTORE THE DATABASE.

To upgrade a 133 MHz controller to a 300 or 450 MHz controller:

1. Power down the old controller (see page 99).
2. Disconnect all cables from the old controller.
3. Move the hard drive from the old controller to the new controller (see "Hard Drive Replacement Overview" on page 125).
4. Remove each controller's cover (see page 99).
5. Move the System ID module from the old controller to the new controller (see "System ID Module" on page 133).
6. Connect the cables to the new controller.
7. Power up the new controller.

Upgrading to a 700-User Controller

You can increase the capacity of a 250-user controller to that of a 700-user controller by adding the following modules:

- One DSP module for telecom support (21061/21161 based).
- One Dual FIM module.
- One 64-Channel echo canceller.

Tip: A second 64-channel echo canceller can be added, or the existing 64-channel echo canceller can be replaced by a 128-channel echo canceller.

Tip: To add compression channels to the upgraded system, see “DSP Module” on page 105.

Refer to "Install Controller Components" on page 15 for module slot locations.

To upgrade a 250-user controller to a 700-user controller:

1. Power down the controller (see page 99).
2. Disconnect all cables from the controller.
3. Remove the controller cover (see page 99 or page 100).
4. Install the Dual FIM module if you are adding peripheral cabinets or NSUs (see “Dual Fiber Interface Module (FIM)” on page 104).
5. Install the DSP module in Slot 7 (see “DSP Module” on page 105).
6. Install the 64 echo canceller module in Slot 6 (see “Echo Canceller” on page 112).
7. Replace the controller cover (see “Removing/Replacing LX/700-User Controller Cover” on page 99).
8. Reconnect the cables to the controller.
9. Power up the controller (see page 22).

Add or Replace Controller FRUs

This section contains detailed information on adding or replacing the 3300 ICP Field Replaceable Units (FRUs). See page 365 for part numbers.

The section is organized as follows:

Tip: See also "Add Controller FRUs" on page 116 and "Replace Controller FRUs" on page 125.

Dual Fiber Interface Module (FIM)

Tip: You may not install a FIM in a CX or CXi controller.

Tip: Ensure that the type of the optical interface matches that of the mating unit (820nm single-mode, 1300nm single-mode, or 1300mn multi-mode).

To add or replace a Dual FIM:

1. Power down the controller (see page 99).
2. Remove the dual FIM from its packaging.
3. Remove a blank module cover. See the Figures on page 15 for slot locations.
4. Line up the connectors and firmly seat the FIM onto the main board.
5. Secure the Dual FIM module onto the main board using the screws and lock washers provided.
6. Replace the controller cover and secure it with its screws (see "To install the LX/700-user controller cover:" on page 100, "To remove the MX/100-user controller cover:" on page 100, or "Removing/Replacing CX/CXi/MXe Controller Cover" on page 101).

DSP Module

You may have to add additional DSP modules to:

- increase the number of voice mail ports
- add compression channels
  - LX/MXe expanded/700-user: up to 64
  - MX/MXe base/100-user: up to 32
  - CX/CXi: up to 16
- increase telephony resources to support more TDM devices.

Tip: Refer to Table 7 on page 108 to calculate DSP requirements for the CX and CXi controllers. You may replace two Dual DSPs with one Quad DSP.

This section contains DSP tables for:

- “Calculating DSP Usage (MXe)” on page 105
- “Calculating DSP Usage (LX/MX)” on page 105
- “Calculating DSP Usage (CX/CXi)” on page 108.

Calculating DSP Usage (MXe)

The embedded DSP resources on the MXe are sufficient to support telephony services, conferencing and voice mail. Additional DSPs are required to support G.729a compression.

Table 5: MXe DSP Requirements Example

MXe configuration	Embedded DSP	Quad DSP MMC
Standard MXe	√	—
MXe with 32 channels G.729a	√	1
MXe with second processor and 64 channels G.729a	√	2

Calculating DSP Usage (LX/MX)

Enter your system parameters in Table 6 (see Table 5 for MXe, Table 7 on page 108 for CX/CXi), to determine the number of Quad DSP modules required. Other features in a system which can affect the DSP usage are ACD, external applications, and heavy or light traffic.

Table 6: Quad DSP Requirement Calculator (LX/MX

Basic Requirements	1.77	=	1.77
IP Lines		× 0.0012 =	
TDM Lines		× 0.0025 =	
IP networking (enter total users in above equation, if IP networking is enabled, otherwise enter zero)		× 0.002 =	
FAX detection (Note 1)		× 0.003 =	
Voice Mail Ports:		÷ 15 =	
Subtotal (Note 2)	minimum = 4		
Required telephony devices	subtotal minus embedded		
Compression Channels: (round up result to next integer)		÷ 8 =	
Total DSP Devices =			
Quad DSP modules = Total DSP devices ÷ 4 (round up result to next integer)			
Note 1. FAX detection only applied when IP trunks are active. Note 2. Every system allocates a minimum of 4 DSP devices to telecom applications.			

The result of this calculation gives a reasonable estimate of the number of DSP devices and modules required to support the system configuration. If the total number of DSP devices is very close to a Quad module boundary, or if there are other issues with a complex system, contact Professional Services for a detailed analysis of system resources and performance.

Voice mail notes:

- Program the additional voice mail ports, then add the DSP MMCs if necessary (for the MXe, you need to add DSPs only for compression).
- With Release 5.0, voice mail ports support G.729a compression. When you increase the number of ports you may also have to add DSPs to handle the increased demand for compression.

Compression notes:

- Compression resources are assigned to the first DSP devices found starting at the **lowest-numbered available slot**.

- You must purchase compression licenses before adding a DSP module for compression.
- Upgrading to 64 compression channels requires a minimum 300 MHz controller (see “Upgrading to a 300 or 450 MHz Controller”, page 102).
- If you are adding compression to a **100-user** controller with a Single or Dual Telecom DSP in slot 3, you must first move the Telecom DSP to slot 4.

Telecom notes:

- Telecom resources are assigned from the **highest-numbered slot**. The first Telecom DSP in an MX or 100-user controller is in slot 4. The first Telecom DSP in an LX or 700-user controller is in slot 8.

Perform this step if the system needs compression channels and/or 30 voice mail ports and/or increased telephony resources to support more TDM devices (see “Hardware Part Numbers” on page 365 for the part numbers of the DSP modules).

To determine the number of DSP modules required in a system, use the formula in Table 5 on page 105 or Table 6 on page 106 Table 7 on page 108.

- LX controller ships with two Quad DSP modules
- MX controller ships with one Quad DSP module
- MXe controller ships with embedded DSP equivalent to two Quad DSP modules (sufficient to support a 400-user system).
- CX and CXi controllers ship with a Dual Embedded DSP on the main board. The T1/E1 Combo also includes DSP resources.

Tip: Voice mail ports support G.711 and G.729a compression. This applies to all types of voice mail ports, including RAD, Music on Hold, Auto Attendant, and Record-a-call.

Tip: Make sure you have the appropriate compression license before installing DSP modules for compression.

Tip: In the following scenario, the call will not be compressed when going through the second controller: a call originates in a Release 5.0 or later controller with compression OFF, through a Release 4.1 controller with compression ON, and terminates at a Release 5.0 or later controller.

Calculating DSP Usage (CX/CXi)

Table 7: CX/CXi DSP Configurations

Base System (2 total)	Base + T1/E1 Combo (3 total)	Base + Dual DSP (4 total)	Base + T1/E1 Combo + Dual DSP (5 total)
3 3-party conf. 4 voice mail ports 0 G.729a channels 24 IP phones 8 ONS phones 12 LS/CLASS trunks	10 3-party conf. 16 voice mail ports 0 G.729a channels 64 IP phones 8 ONS phones 12 LS/CLASS trunks 24 T1 trunks	10 3-party conf. 16 voice mail ports 0 G.729a channels 40 IP phones 8 ONS phones 12 LS/CLASS trunks	10 3-party conf. 16 voice mail ports 16 G.729a channels 64 IP phones 8 ONS phones 12 LS/CLASS trunks 24 T1 trunks
		3 3-party conf. 4 voice mail ports 8 G.729a channels 40 IP phones 8 ONS phones 12 LS/CLASS trunks	

Notes:

1. The number of conference, voice mail, and compression resources is fixed by the purchased option and the number of DSP devices available; the other values are adjustable. Compression alters the number of resources available for the system. For example, by adding 8 compression resources to a system with 4 DSPs total, the maximum number of three-party conferences drops to 3 and the maximum number of voice mail ports drops to 4.

2. The controller supports the G.711 and G.729a audio codecs.
- The G.711 PCM audio codec for 56/64 kbps generally provides the best voice quality and is comparable to TDM-type connections.
- The G.729a audio codec for 8/13 kbps provides a good reduction in bandwidth with only minor loss in voice quality.
- A purchasable MOSS option (Option 120, Number of Compression Resources) controls the number of G.729a codecs available to IP devices in the system. Compression enables more devices to share the available bandwidth. The option is purchasable in multiples of 8 to a maximum of 16. The default value is 0. The quantity entered must exactly match the quantity on the MOSS sheet.

3. A hard drive is strongly recommended for systems that have more than eight voice mail ports or when Record a Call is frequently used.

4. The base CX contains an Analog Main Board (AMB) that supports 4 ONS and 6 LS circuits. By installing an Analog Option Board (AOB), capacity doubles to 8 ONS and 12 LS circuits. The AOB does not require extra DSP resources.

Adding or Replacing a DSP Module

To add or replace a DSP module:

1. Power down the controller (see page 99) and disconnect all cables.
2. Remove the controller cover (see page 99 or page 101).
3. Remove the DSP module from its packaging.
4. Remove a blank module cover if necessary. For installation in a rear slot, internal site in the MXe, or Slot 3 in the CX and CXi controllers, skip to Step 8. See the Figures on page 15 for slot locations.
5. If you are replacing a defective DSP, remove the screws and lock washers and pull up on the module to remove it.
6. Remove the small PCB (or the defective DSP module) from the blank module cover (1 in Figure 10).
7. Install the module cover on the new DSP module (2 in Figure 10).
8. Insert the DSP module in the appropriate slot, firmly seat it onto the main board, and secure using the screws and lock washers provided.
9. Put the controller's top cover back on, and secure it with its screws (see page 100, page 100, or page 101).
10. Reconnect the cables to the controller.
11. Power up the controller (see page 22).

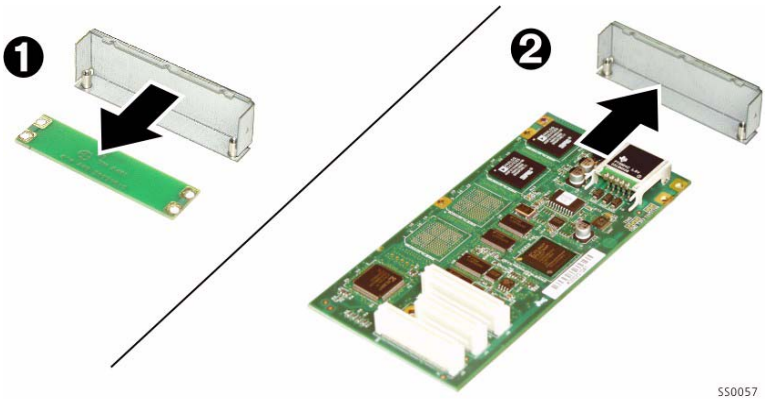


Figure 10: Attaching Cover Plate to the DSP Module

Programming the Additional Voice Mail Ports

To program the additional voice mail ports:

1. In the System Administration Tool, change the number of voice mail ports. In the **All forms (alphabetical)** list, click the **Voice Mail Port Capacity** form.
2. In the **Voice Mail Port Assignment** form, program the extension and interconnect numbers for each new voice mail port.
3. **Reboot** the controller (see page 99).

Framer (Dual T1/E1, T1/E1 Combo, Quad BRI)

Embedded T1/E1 (for PRI or T1/D4) or BRI

You can add embedded T1/E1 (for PRI, T1/D4, or MSDN/DPNSS) or embedded BRI to a controller by adding one to three framer modules (Dual T1/E1, or Quad BRI) in the controller (see "Hardware Part Numbers" on page 365 for the part number of the Framer Modules). The CX controller does not support the Dual T1/E1 Framer. The BRI Framer is not supported in North America.

Tip: Upgrading to embedded PRI, T1/D4, MSDN/DPNSS, or BRI requires a minimum 300 MHz controller (see "Upgrading to a 300 or 450 MHz Controller", page 102). To determine the speed of your processor, see "Checking Controller Hardware Profile" on page 235.

Tip: The Dual T1/E1 Framer does not support XNET, Min/Max, or NFAS.

Dual T1/E1 Framer

Each Dual T1/E1 Framer has 2 ports (RJ-45 connectors), each of which can be used for T1/E1 ISDN or T1/D4. The two protocols can operate in tandem on the same Dual T1/E1 Framer with any ISDN variant, i.e. PRI and QSIG.

T1/D4 provides for digital E&M, digital DID, or digital CO protocols. T1/E1 ISDN provides for DMS-100, DMS-250, NI-2 (Bellcore National ISDN, 5ESS, GTD5), Euro ISDN, 4ESS, Euro-ISDN (CTR4), and QSIG protocols.

T1/E1 Combo

The T1/E1 combo module, available only for the CX and CXi controllers at Release 6.0, combines trunking (T1D4 and PRI ISDN/QSIG) and DSP functionality in a single card. The Release 6.0 version of the combo contained a single T1/E1 framer. The module also includes 32-channel Echo Cancellation.

At Release 7.0 the combo has a resilient connection added. You can connect T1/E1 Combo cards in a primary and a secondary controller, for resilient operation, with a one-to-one RJ-45 cable. Enable the resilient feature in the Digital Link Assignment form. Refer to the Resiliency document on Mitel OnLine for instructions on how to configure T1/E1 resiliency.

Tip: Resilient operation requires that both the primary and secondary controllers are running Release 7.0 software. The secondary controller may be configured with the new or old version T1/E1 Combo card or a Dual T1/E1 Framer module.

Quad BRI Framer

BRI (Basic Rate Interface) is a basic ISDN service consisting of two 64 Kbps channels and a single 16 Kbps channel (see page 261 in the Hardware Reference chapter for connection details). The Quad BRI Framer is not supported in North America.

To add or replace a framer module:

1. Power down the controller (see page 99).
2. Disconnect all cables from the controller.
3. Remove the controller cover (see page 99, page 100, or page 101).
4. Remove the module from its packaging. DO NOT move LT/NT jumpers.
5. Remove the blank module cover at the front of the controller, and insert the module in an appropriate slot (see page 15).
6. If you are replacing a defective module, remove the screws and lock washers and pull up on the module to remove it
7. Secure the module to the controller using the screws and pillars provided with the module.
8. Put the controller's top cover back on, and secure it with its screws (see page 100, page 100, or page 101).

9. Reconnect the cables to the controller. Power up the controller.

Tip: For the T1/E1 Combo, connect the T1 line from the service provider to the RJ45 connector on the T1/E1 combo module. See Table 40 on page 260 for connector pinouts.

Tip: The Quad BRI Framer allows a 1:1 connection to a BRI Central Office or a crossover connection to a BRI telephone. The shielded, twisted pair ISDN cable is connected on either end with pins 3-4, and 5-6. The straight-through cable is used for "T" interfaces to the Central Office and the crossover (with 3-4 and 5-6 crossed at one end) for "S" interfaces to sets.

Echo Canceller

Tip: The CX, CXi, and MXe controllers contain echo cancellers on the main board sufficient to handle normal traffic conditions.

To add or replace an echo canceller:

1. Power down the controller (see page 99).
2. Disconnect all cables.
3. Remove the cover (see page 99, page 100, or page 101).
4. Remove the echo canceller module from its packaging.
5. If you are replacing a defective echo canceller module, remove the screws and lock washers and pull up on the module to remove it.
6. Line up the connectors of the new echo canceller module and firmly seat it onto the main board in an appropriate slot (see page 15).
7. Secure the module onto the main board using the screws and lock washers provided.
8. Replace the controller top cover and secure it with its screws (see "To install the LX/700-user controller cover:" on page 100, "To remove the MX/100-user controller cover:" on page 100, or "Removing/Replacing CX/CXi/MXe Controller Cover" on page 101).
9. Reconnect the cables to the controller.
10. Power up the controller (see page 22).

Analog Option Board (MX Controller)

Install an AOB to increase LS CLASS circuits from 6 to 12 and ONS CLASS circuits from 2 to 4 (see page 262).

To add or replace an AOB in an MX:

1. Power down the controller (see page 99).
2. Remove the cover (see page 100).
3. Remove the four screws from the back portion of the Analog Main Board (AMB) (see Figure 23 on page 136).
4. Install and secure the standoffs that ship with the Analog Option Board.
5. Insert the Analog Option Board onto the AMB. Ensure it is well-seated in its socket.
6. Attach the four screws that you removed from the AMB.
7. Replace the top cover (see page 100).
8. Power up the controller.
9. In the System Administration Tool, go the **Analog Services Unit Configuration** form.
10. Select Unit 4 and click **Modify**.
11. Select **3300 Expanded Analog** and click **Save**.

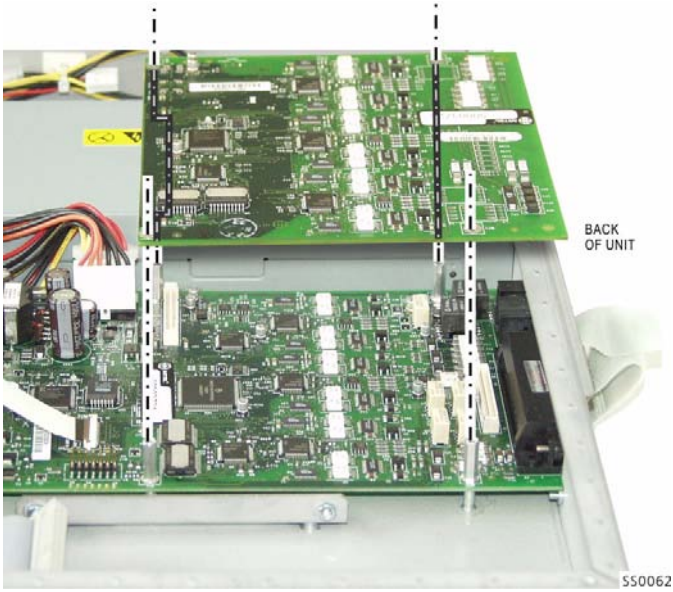


Figure 11: Screws and Standoffs on the Analog Option Board

Analog Option Board (CX/CXi Controller)

CX controller: to increase LS CLASS circuits from 6 to 12 and ONS CLASS circuits from 4 to 8 (see page 264).

To add or replace an AOB in a CX/CXi:

1. Power down the controller (see page 99).
2. Remove the cover (see page 101).
3. Remove the blanking panel from the back of the controller.
4. Insert the replacement faceplate into the back of the controller and attach it with screws (1).
5. Place the AOB on a flat surface.
6. Attach the flex and power cables. To attach the flex cable, lift up on the tabs at the end of the connector to loosen it, insert the cable label side down, and then press down on the tabs to tighten connector (2).
7. Lower the AOB into place and attach it with the supplied screws (3).

8. Connect the other ends of the flex cable and power cable where indicated in Figure 12. The horizontal flex cable connector is hinged: flip up to loosen it, insert the cable, and then press down to tighten (4).
9. Replace the top cover (see page 101).
10. Power up the controller.
11. In the System Administration Tool, go the **Analog Services Unit Configuration** form.
12. Select Unit 4 and click **Modify**.
13. Select **3300 Expanded Analog** and click **Save**.

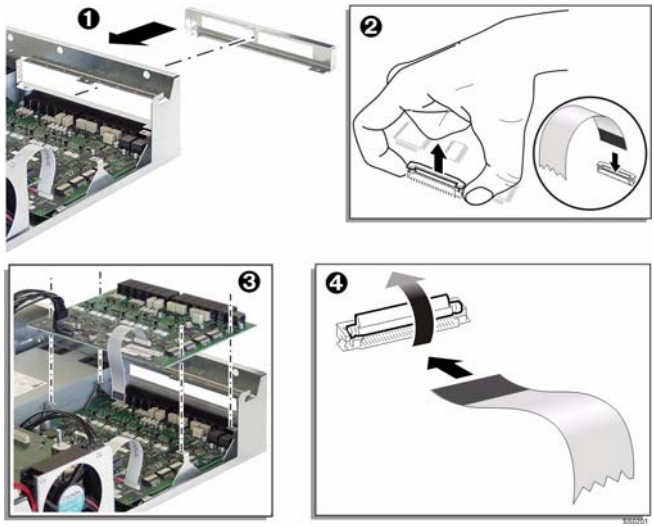


Figure 12: Screws and Standoffs on the Analog Option Board

Add Controller FRUs

This section contains detailed information on adding the 3300 ICP Field Replaceable Units (FRUs). See Appendix E FRU Part Numbers beginning on page 365 for a list of FRU part numbers.

The section is organized as follows:

Tip: The CX/CXi/MXe controllers are shipped with the **Analog Main Board** installed. If you receive a CX/CXi/MXe and the AMB is not installed, refer to page 136 for installation instructions.

Tip: See also "Add or Replace Controller FRUs" on page 104 and "Replace Controller FRUs" on page 125.

MXe RAID Controller

The RAID (redundant array of independent disks) controller will mirror all data on two hard drives. In the event that one drive fails, the system will continue to operate on the remaining drive. Refer to Knowledge Base Article 06-2806-00012 "RAID Controller Operations Manual" for RAID operation details.

CAUTION: The RAID controller does not protect against loss of data as a result of a power outage. You must provide an Interruptible Power Supply (UPS) to protect your system data from an electrical disturbance.

Tip: It is very important to maintain current database backups; backups should be done on a regular basis even when you have disk redundancy.

To add a RAID controller:

1. Remove the controller, hard drives, and RAID controller card from their packaging.
2. Remove the top cover of the controller (see page 101).
3. Remove the indented portion of the plastic bezel, above the hard drive position, to expose the RAID controller LEDs and mirror buttons.
   - At the rear of the cover, insert a sharp object through a LED hole. Push the bezel cover out far enough to grasp the top and bottom edges and pull that portion of the bezel off.
4. Remove the ribbon cable from the HD1 position on the interconnect card and remove the power cable.
5. Remove the standard hard drive interconnect card from the top of the hard drive carrier.
6. Install the RAID controller card.
7. Attach the ribbon cable and power cable to the RAID card.
8. Replace the top cover (page 101).
9. Continue with the “Redundant Hard Drive (MXe)” procedure, below.

Redundant Hard Drive (MXe)

After the RAID controller has been installed, perform the following steps to install the two hard drives, one at a time.

CAUTION: Both hard drives must have the same part number.

CAUTION: You must install only the first hard drive, with the installed software, before you boot the system.
After the system is fully booted, slide the second hard drive into the HD2 position.

Tip: We recommend that you perform a replacement with rebuild outside of business hours.

To install a redundant hard drive in an MXe:

1. Remove hard drive carriers from the controller.
2. Install hard drives onto the hard drive carriers.
3. Ensure that the hard drive jumpers are set to master (see page 256).
4. Slide the first hard drive, with installed software, into the HD1 position. DO NOT INSTALL the second hard drive at this time.
5. Push to seat the hard drive into the hard drive back plane.
6. Tighten the thumb screw.
7. Power up the controller (page 22). The HD1 access LED should be green and the activity LED flashes orange and green.
   - The HD1 access LED should be green HD2 fault LED should be orange and the activity LED flashes orange and green
   - Once the system is booted, the activity LED will be green most of the time.
8. After the system is fully booted, slide the second hard drive into the HD2 position.
9. Push to seat the hard drive into the hard drive back plane.
10. Tighten the thumb screw.
11. Press the HD2 mirror control (ctrl) button for 5 to 10 seconds to mirror the drives.
12. Release the mirror button when the fault LED flashes green twice per second. The Activity LED will go solid green, occasionally flash amber.
13. The rebuild process will take more than two hours to complete. After the rebuild is complete, the HD2 fault LED will be off and the access LED will be on solid green.

Application Processor Card (CXi)

The optional Application Processor Card (APC) allows the system to host the Mitel 6000 Managed Application Server (MAS) that can run 6040 Office Server, Live Business Gateway, Mobile Extension, and Teleworker Solution. Each of the applications will be released with guidelines defining conditions, performance, and installation combinations. For information on how to program and use software blades and services, refer to the 6000 MAS documentation at http://edocs.mitel.com.

After you install the APC, continue by installing the APC hard drive (page 121) and configuring for 6000 MAS (page 122).

To install the APC in a CXi:

1. Remove the controller, hard drives, and APC from their packaging.
2. Remove the top cover of the controller (see page 101).
3. Remove the Stratum Clock module if installed.
4. Place the APC on the main board connectors. The connectors are spaced irregularly to assist in alignment (see Figure 13).
5. To seat the connectors, grasp the main board with your fingertips and press down firmly on the middle of one side of the APC with your thumbs as shown. Repeat for the other side of the APC next to the fan (Figure 14). You should hear and feel the connectors seating themselves.

Tip: To ensure that the APC is seated securely, press down on the APC over each of the four connectors, one at a time. Once the APC is properly installed, the four corners of the APC will rest against the standoffs located at each corner of the APC.

6. Prepare the heat spreader for installation by removing the protective strips from the adhesive heat pads (see Figure 15).
7. Place the four screws (supplied) in the heat spreader, and lower the heat spreader onto the APC. Align the cutout on the heat spreader above the memory modules on the APC.
8. Tighten the screws in an alternating pattern until they are snug. Do not over-tighten.
9. Replace the Stratum Clock module.
10. Continue with the “APC Hard Drive (CXi)” procedure on page 121.

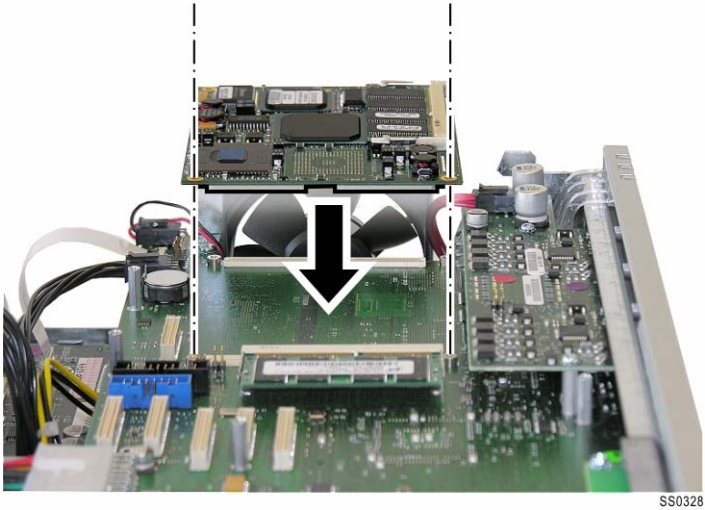


Figure 13: APC module on the main board - CXi

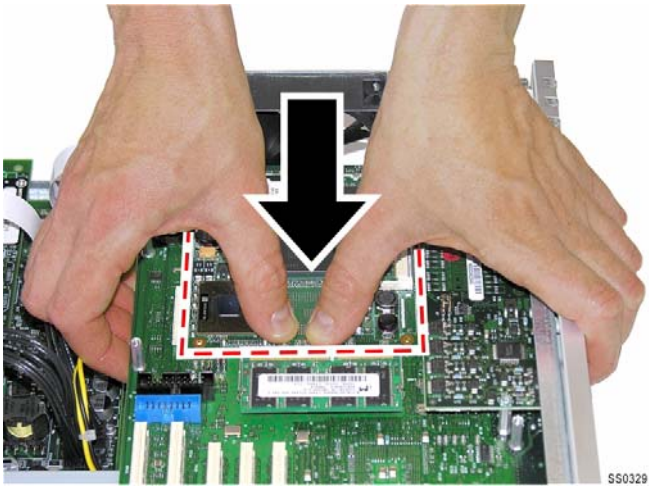


Figure 14: Seat the APC

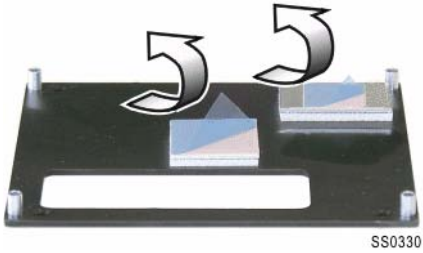


Figure 15: Remove protective strips from APC heat pads

APC Hard Drive (CXi)

If you are installing the optional Application Processor Card, then you must also install a hard drive to support the APC's operating system and applications. If you are replacing an APC hard drive with one that does not have the 6000 MAS software installed, refer to “Install 6000 MAS Software” on page 87.

To install the APC hard drive in a CXi:

1. Unplug the ribbon cable and the power cable from the old hard drive.
2. Remove the screws connecting the bracket to the back of the controller, then slide the bracket forward and remove it.
3. If a System hard drive is already installed in the upper bracket position, unscrew it from the bracket and move it to the lower bracket position. The power and IDE cables can remain connected.
4. Lower the APC hard drive into the upper bracket position. Ensure that the hard drive jumpers are set to master.
5. Secure the hard drives to the bracket with the screws provided.
6. Connect the power and IDE cables to the corresponding connectors on the hard drive and main board. The cables are keyed for proper connection (see Figure 16).

Tip: Connect the System hard drive IDE cable to the main board connector labeled MPC8270 HARDDRIVE. Connect the APC hard drive IDE cable to the main board connector labeled ETX HARDDRIVE.

7. Slide the bracket back into the chassis, then fasten the screws connecting the bracket to the back of the controller.

8. Replace the top cover (page 101).
9. Power up the controller (see page 22).

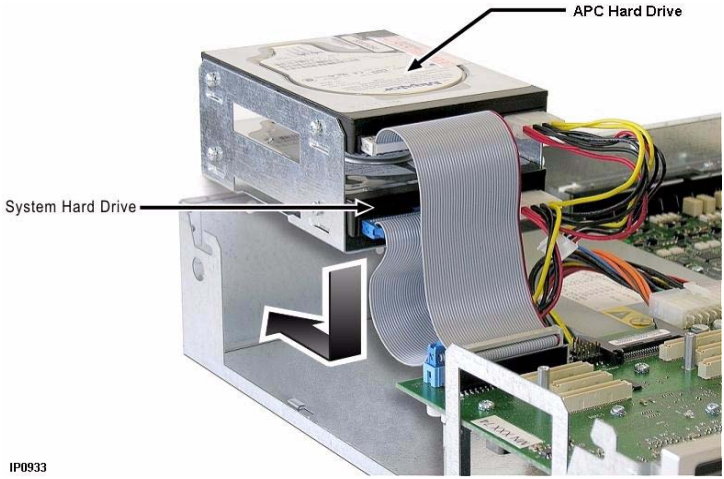


Figure 16: Connecting cables to APC - CXi

Configure the System for 6000 MAS

To configure the 3300 and APC to support MAS:

1. Power down the 3300 controller.
2. Install the Application Processor Card in the 3300 controller.
3. Install the APC hard drive (on which the software is preloaded) in the 3300.
4. Power-up the 3300.
5. Program the WAN Settings form, in the 3300 System Administration Tool, to support APC.
6. Launch the secure telnet client.
   - Enter open <RTC IP address> using port <2005> (command with example IP address, **open 192.168.1.2 2005**).
   - Enter the 3300 username and password.
7. Follow on-screen instructions to configure the 6000 MAS and blades. Refer to the 6000 MAS documentation on Mitel OnLine.

Redundant Power Supply (MXe)

To add a redundant power supply in an MXe:

Tip: It is not necessary to power down the controller to add a power supply.

1. Remove the power supply unit blanking panel.
2. Slide the new power supply unit into the power supply carrier on the rear of the controller.
3. Push to seat the power supply into the power supply back plane.
4. Secure the thumb screw and connect the power cord.
5. Set the AC power switch to ON. AC and DC LEDs will illuminate.

To replace a power supply:

1. Set the AC power switch to OFF.
2. Remove the power cord from the AC receptacle on the power supply.
3. Loosen the thumb screw on the power supply.
4. Slide the power supply unit out of the power supply carrier on the rear of the controller.
5. Continue with the “To add a redundant power supply in an MXe:” procedure, above, beginning with step 2.

E2T Processor (MXe)

Tip: Refer to Engineering Guidelines to determine when a second processor is necessary.

To add an E2T processor in an MXe:

1. Power down the controller (see page 99).
2. Remove the controller cover (see page 101).
3. Disconnect cables from the main board.
4. Disconnect ribbon cable from the interconnect card or RAID controller.
5. Remove the single captive screw that secures the main board to the chassis.
6. With the rear of the controller facing you, slide main board towards the front of the chassis and pull it up.

7. Set the main board on a flat surface with the under side facing up.
8. Seat the E2T onto the main board and secure with four screws.
9. Set the main board on the chassis and attach to the chassis with the captive screw.
10. Attach the cables to the main board.
11. Connect the ribbon cable to the interconnect card or RAID controller.
12. Replace the cover and reconnect the cables to the controller.
13. Power up the controller (see page 22).

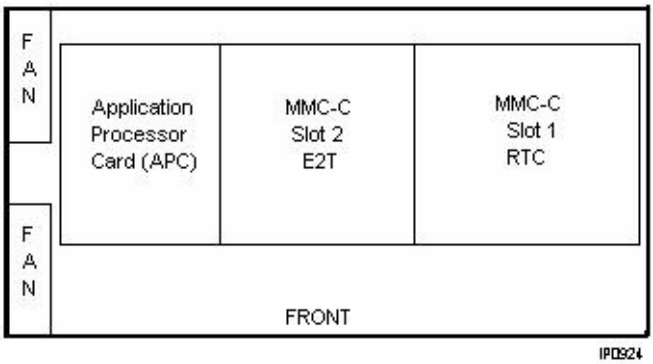


Figure 17: MXe: RTC / E2T/ APC on the Main Board, bottom view

Replace Controller FRUs

This section contains detailed information on replacing the 3300 ICP Field Replaceable Units (FRUs) (see page 363 for part numbers).

The section is organized as follows:

Tip: See also “Add or Replace Controller FRUs” on page 104 and “Add Controller FRUs” on page 116.

Hard Drive Replacement Overview

CAUTION: If you move a programmed hard drive from one controller type to another (for example, an MX system to an LX or CX system), you MUST manually install the software (see page 77) and restore the database. A new hard drive purchased from Mitel is configured for installation in any system.

CAUTION: Both hard drives in a redundant hard drive MXe must have the same part number.

CAUTION: If you install a new hard drive, with Release 6.0 or later software, in a system running older software, you must change the RTC file name (see page 300).
The file name for all platforms, for Release 6.0 and later is: /partition1/Rtc8260.
Prior to Release 6.0: LX, 250/700-user: /partition1/Rtc8260; MX: /partition1/Lite200UP; 100-user: /partition1/Lite8260

LX, 100, 250, 700-User Hard Drive

To replace the hard drive in the LX, 100, 250, or 700-user controller:

Tip: Use this procedure only to replace a controller hard drive in a system that's already installed. To install a hard drive in a new system, see page 19.

1. If possible, back up your database (or locate the most recent backup).
2. Power down the controller (see page 99) and disconnect all cables.
3. Place the controller on the work area with the bottom facing up.
4. Remove the hard drive backing plate from the controller by removing the six (6) small border screws (the four large screws secure the hard drive to the backing plate). Keep the screws.
5. Unplug the ribbon cable and the power cable from the old hard drive.
6. Connect the ribbon cable and power cable to the new hard drive.

Figure 18: LX and 700-User Controller Hard Drive Installation

7. Secure the new hard drive backing plate with the hard drive attached, to the controller cover using the screws provided.
8. Remount the controller.
9. Restore the connections to the Maintenance PC.
10. Return power to the controller, but do not connect to the network.
11. Manually install the software on the hard drive (see page 77).
12. Reconnect the controller to the network.
13. If you backed up your database in Step 1, restore the database (see page 63).

MX Hard Drive

To replace the hard drive in an MX controller:

Tip: Use this procedure only to replace a controller hard drive in a system that's already installed. To install a hard drive in a new system, see page 19.

1. If possible, back up your database (or locate the most recent backup).
2. Power down the controller (see page 99) and disconnect all cables.
3. Remove the controller cover (see page 100).
4. Remove the four screws that secure the hard drive to the controller.
5. Remove the old hard drive (behind slot 4).
6. Unplug the ribbon cable and the power cable from the old hard drive.

Figure 19: MX Controller Hard Drive Installation

7. Connect the ribbon cable and power cable to the new hard drive.
8. Install the new hard drive (remove and discard the backing plate).
9. Secure the hard drive plate to the controller using the screws provided.
10. Replace the controller cover (see page 100).
11. Remount the controller.
12. Restore the connections to the Maintenance PC.
13. Return power to the controller, but do not connect to the network.
14. Manually install the software on the hard drive (see "Installing System Software Manually" on page 77).
15. Reconnect the controller to the network.
16. If you backed up your database in Step 1, restore the database (see "Restore a Database" on page 63).

MXe Hard Drive, Single

To replace the hard drive in a single hard drive MXe:

Tip: Use this procedure only to replace a controller hard drive in a system that's already installed. To install a hard drive in a new system, see "Hard Drive" on page 19.

Tip: In a redundant hard drive system, each of the hard drives is hot-swappable. In a single hard drive system, you must power down the controller to replace the hard drive.

1. If possible, back up your database (or locate the most recent backup).
2. Power down the controller (see page 99).
3. Loosen the captive screw and slide the defective hard (HD1) drive from the hard drive carrier.
4. Slide the new hard drive into the hard drive carrier and tighten the screw.
5. Push to seat the hard drive into the hard drive back plane.
6. Tighten the thumb screw.
7. Return power to the controller, but do not connect to the network.

8. Manually install the software on the hard drive (see “Installing System Software Manually” on page 77).
9. Reconnect the controller to the network.
10. If you backed up your database in Step 1, restore the database (see “Restore a Database” on page 63).

MXe Hard Drive, Redundant

CAUTION: Both hard drives must have the same part number.

Refer to “MXe Hard Drive, Both Redundant Drives” on page 130 when you have **to replace both hard drives** under the following conditions:

- both of the hard drives have failed OR
- the replacement hard drive part number is different from that of the defective hard drive.

To replace a hard drive in a redundant hard drive MXe:

Tip: Refer to Table 96: RAID Fault and Access LEDs p.(337) for a complete description of LED activity.

Tip: We recommend that you perform a replacement with rebuild outside of business hours.

1. If the hard drive is already off-line (normally or faulted) go to step 4.
2. Using a small pointed object (paper clip), press the mirror control (ctrl) button, for less than five seconds, of the hard drive to be removed.
   - Release the button when the Access LED starts flashing once per second.
   - Hard drive is off-line when the Access LED is off and the fault LED is orange.
3. Release the retaining screw securing the hard drive carrier to the controller.
4. Slide the defective hard drive out of the hard drive carrier.
5. Remove the four screws securing the hard drive to the hard drive carrier.

6. Install the new hard drive in the hard drive carrier with the four screws.
7. Slide the hard drive into the controller.
8. Push to seat the hard drive into the hard drive back plane.
9. Tighten the thumb screw.
10. To copy data onto the new drive, press the mirror control button for the new hard disk for 5 to 10 seconds.
    - Release the button when the Access LED starts flashing twice per second.
    - The rebuild process is indicated by the Access LED solid green and the Fault LED flashing green.
    - The rebuild is complete when the Fault LED is off (approximately two hours).

MXe Hard Drive, Both Redundant Drives

CAUTION: Both hard drives must have the same part number.

CAUTION: You must install only the first hard drive before you boot the system.
After the system is fully booted, slide the second hard drive into the HD2 position.

Use this procedure when both drives have failed or when you need to replace both drives because replacement hard drive part number is different from that of the defective hard drive.

To replace both hard drives in a redundant hard drive MXe:

1. Ensure that you have a database backup.
2. Power down the controller (see page 99).
3. Loosen the captive screws and slide the hard drives from the hard drive carrier.
4. Clear the sockets (refer to Knowledge Base Article 06-2806-00012).
5. Replace the old hard drive with the new hard drive, in the hard drive carrier, with the four screws.

- Slide the first hard drive into the HD1 position. DO NOT INSTALL the second hard drive at this time.

6. Push to seat the first hard drive into the hard drive back plane.
7. Tighten the thumb screw.
8. Return power to the controller, but do not connect to the network.
9. Manually install the software on the hard drive (see “Installing System Software Manually” on page 77).
10. Reconnect the controller to the network.
11. Replace the second old hard drive with the second new hard drive in the hard drive carrier with the four screws.
12. Slide the second hard drive into the HD2 position.
13. Push to seat the hard drive into the hard drive back plane.
14. Tighten the thumb screw.
15. To copy data onto the new drive, press the HD2 mirror control button for the new hard disk for 5 to 10 seconds.
    - Release the button when the Access LED starts flashing twice per second.
    - The rebuild process is indicated by the Access LED solid green and the Fault LED flashing green.
16. The rebuild is complete when the Fault LED is off (approximately 20G per hour).

CX/CXi Hard Drive

To replace the hard drive in a CX or CXi:

Tip: Use this procedure only to replace a controller hard drive in a system that’s already installed. To install a hard drive in a new system, see “Hard Drive” on page 19.

1. If possible, back up your database (or locate the most recent backup).
2. Power down the controller (see page 99).
3. Disconnect all cables.
4. Remove the controller cover (see page 101).
5. Unplug the ribbon cable and the power cable from the old hard drive.

6. Remove the screws connecting the bracket to the back of the controller, then slide the bracket forward and remove it. (Removal is unnecessary if the drive is installed in the upper bracket position).
7. Replace the drive with the new one (1) and secure it to the bracket (2). (If the bracket was removed, re-install it and secure it to the back of the controller). Ensure that the jumpers on the new drive are set to the Master setting.
8. Connect the power and IDE cables to the corresponding connectors on the hard drive and main board (3). The cables are keyed for proper connection.

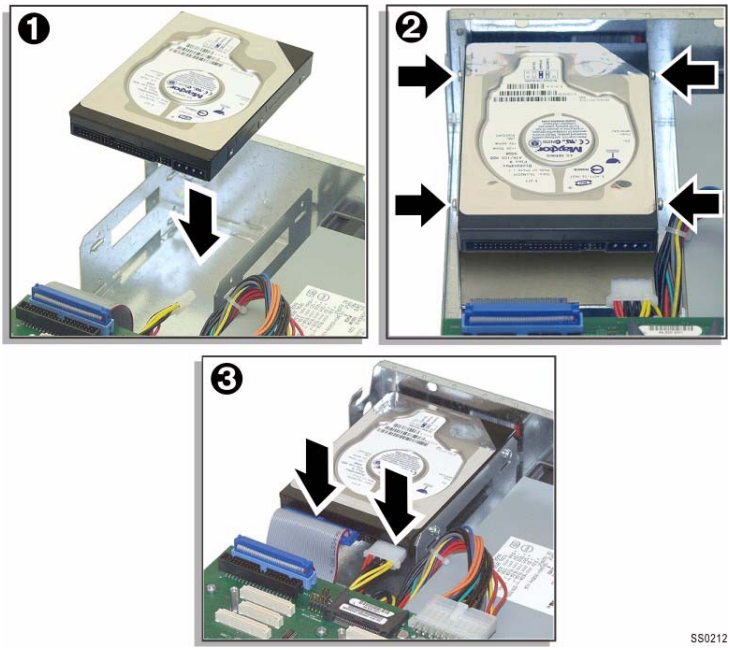


Figure 20: CX Controller Hard Drive Installation

9. Replace the controller cover (see page 101).
10. Remount the controller.
11. Restore the connections to the Maintenance PC.
12. Return power to the controller, but do not connect to the network.
13. Manually install the software on the hard drive (see "Installing System Software Manually" on page 77).

14. Reconnect the controller to the network.
15. If you backed up your database in Step 1, restore the database (see “Restore a Database” on page 63).

System ID Module

To replace the system ID module:

1. Power down the controller (see page 99).
2. Disconnect all cables.
3. Remove the controller cover (see page 99 or page 100).
4. Remove the old System ID module from the main board:
   - **100-user** controller: behind slot 2.
   - **MX** controller: behind slot 4.
   - **LX, 250, or 700-user** controller: between slots 1 and 8.
5. Remove the cover from the new System ID module’s connector.
6. Install the new System ID module and secure with the screw provided.
7. Replace the controller cover (see page 99 or page 100).
8. Reconnect all the cables to the controller.
9. Power up the controller (see page 22).

Tip: If you replace with a new System ID, you must program the options (see page 25) and then restore the database (see page 63).

System i-Button (CX/CXi and MXe)

To replace the system i-button in a CX, CXi, or MXe:

1. Power down the controller (see page 99).
2. Disconnect all cables.
3. Remove the controller cover (see page 101).
4. Remove the old system i-button from the main board. Slightly pull out the metal clips holding the i-button in place.
5. Insert the system i-button in the twin tab connector located on the main board (see Figure 21 on page 134).
6. Replace the controller cover (see page 101).

Tip: If you replace with a new System ID, you must program the options (see page 25) and then restore the database (see page 63).

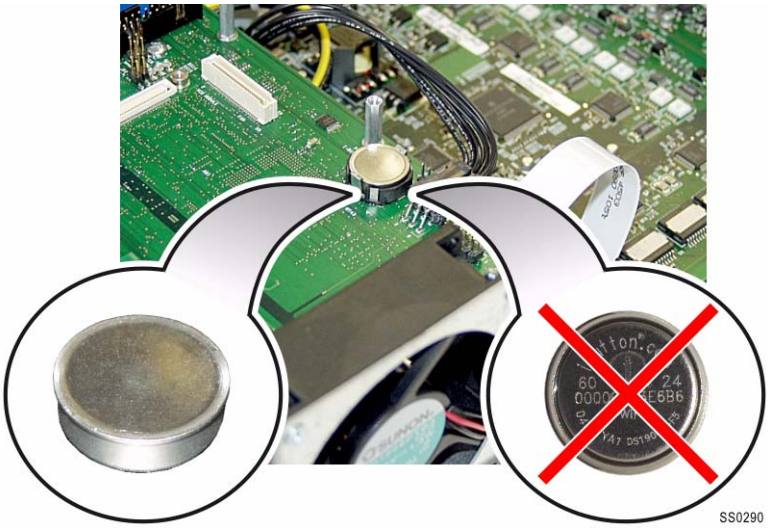


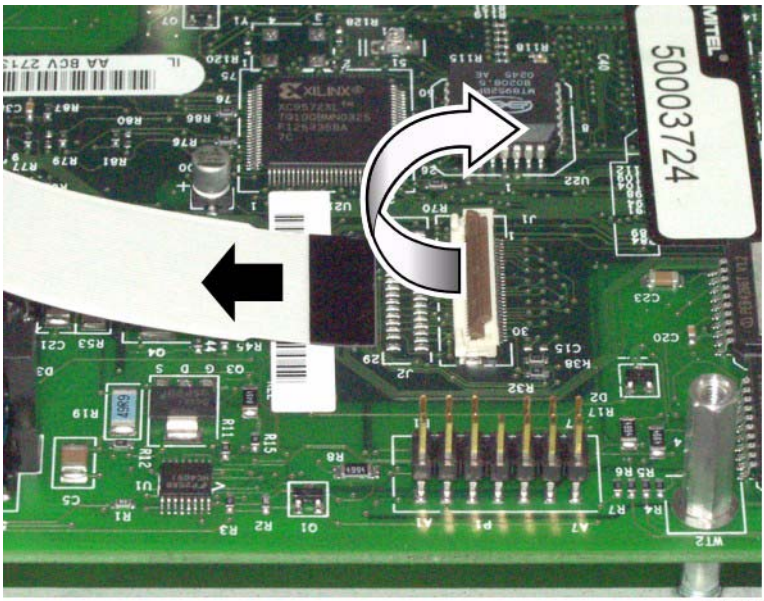
Figure 21: Installing the System i-Button

Analog Main Board (MX Controller)

To replace the analog main board in an MX:

1. Power down the controller (see page 99).
2. Remove the cover (see page 100).
3. Remove the Analog Option Board, if one has been installed, by reversing the installation procedure (page 113).
4. Disconnect the three power supply connectors.
5. Remove the ribbon cable by flipping up the clip on the connectors at each end of the cable (see Figure 22 on page 135).
6. Remove the four standoffs and the two screws at the front of the board (refer to Figure 23 on page 136).

7. Remove the two screws from the hold-down for the Amphenol cable assembly on the back of the unit.
8. Remove the clock module, behind MMC Slot 2.
9. Remove the Analog Main Board.
10. Insert the new Analog Main Board.
11. Replace the two screws in the hold-down for the Amphenol cable assembly on the back of the unit.
12. Replace the two screws at the front of the board and the four standoffs.
13. Replace the ribbon cable by sliding it under the guides on the side and up into the connector. Flip the clip down to secure the cable.
14. Replace the three Power Supply connectors.
15. Replace the top cover.
16. Power up the controller (see page 22).



SS0064

Figure 22: Analog Main Board Ribbon Cable

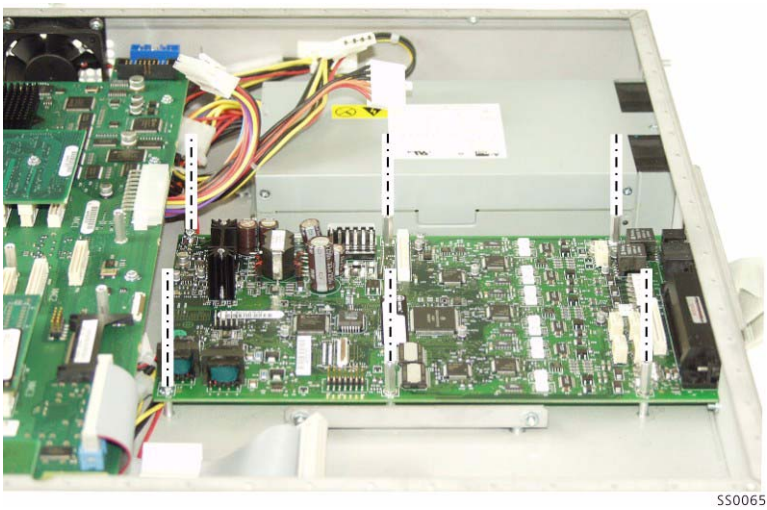


Figure 23: Screws and Standoffs on the Analog Main Board

Analog Main Board (MXe Controller)

To replace the analog main board (AMB) in an MXe:

1. Power down the controller (see page 99).
2. Disconnect the power supply cable.
3. Remove the top cover (see page 101).
4. Disconnect the power cable and remove the ribbon cable on the AMB by flipping up the clip on the connectors at each end of the cable.
5. Remove the Analog Main Board.
6. Place the new AMB on the power supply carrier and slide the port interfaces through the slots at the rear of the controller.
7. Secure the AMB to the carrier with the captive screw provided.
8. Attach the ribbon cable to the controller by lifting up the clip and inserting the cable vertically into the connector. Push the clip down to secure the cable.
9. Attach the power supply cable.
10. Replace the top cover and power up the controller (see page 22).

Analog Main Board (CX/CXi Controller)

To replace the analog main board (AMB) in a CX or CXi:

1. Power down the controller (see page 99).
2. Remove the cover (page 101).
3. Remove the screw that secures the faceplate to the back panel.
4. Remove the Analog Option Board, if one has been installed, by reversing the installation procedure (page 114).
5. Disconnect the power supply cable on the AMB.
6. Remove the ribbon cable on the AMB (not from the main board) by flipping up the clip on the connectors at each end of the cable.
7. Remove the Analog Main Board.
8. Insert the new Analog Main Board.
9. Replace the ribbon cable by sliding it under the guides on the side and up into the connector. Flip the clip down to secure the cable.
10. Replace the power supply cable.
11. Replace the Analog Option Board (if previously removed).
12. Replace the top cover and power up the controller (see page 22)..

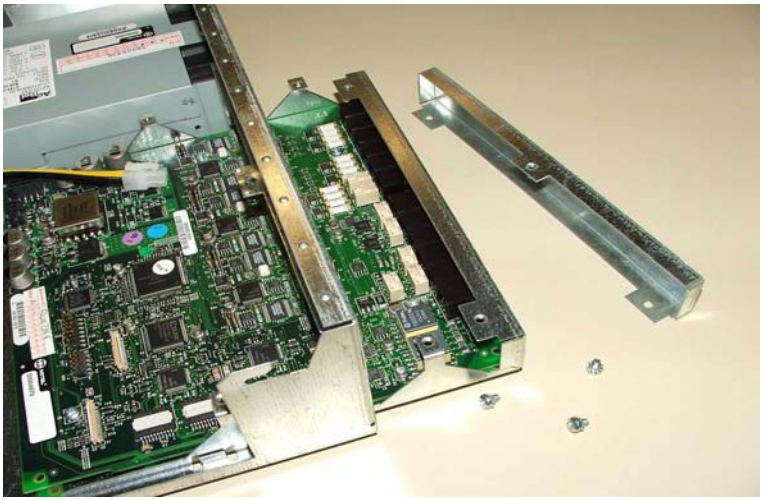


Figure 24: CX/CXi, Insert the Analog Main Board

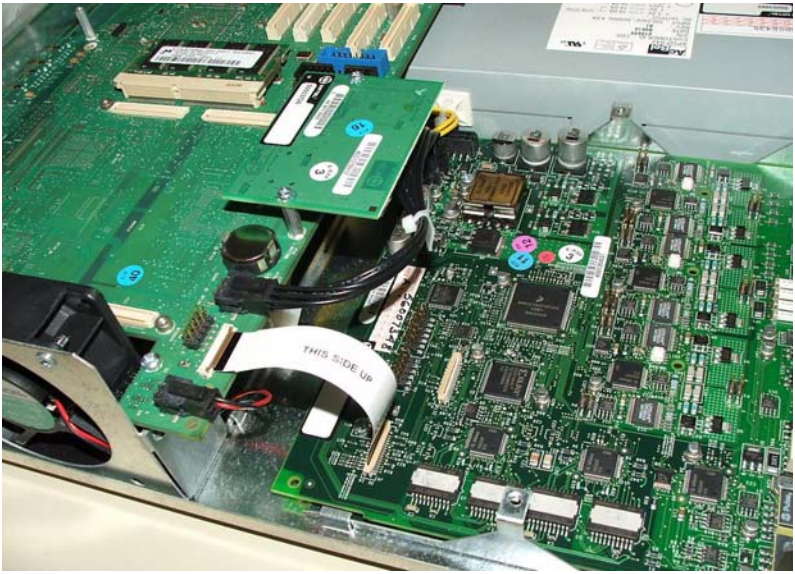


Figure 25: CX/CXi, AMB ribbon cable

RTC Processor (MXe)

To replace the RTC processor in an MXe:

1. Power down the controller (see page 99).
2. Remove the controller cover (see page 101).
3. Disconnect cables from the main board.
4. Disconnect ribbon cable from the interconnect card or RAID controller.
5. Remove the single screw that secures the main board to the chassis.
6. With the rear of the controller facing you, slide main board towards the front of the chassis and pull it up.
7. Set the main board on a flat surface with the under side facing up.
8. Remove four screws and pull off the old RTC.
9. Seat the new RTC onto the main board and secure with four screws.
10. Attach the cables to the main board.

11. Set the main board on the chassis and attach to the chassis with the captive screw.
12. Attach the cables to the main board.
13. Connect the ribbon cable to the interconnect card or RAID controller.
14. Replace the cover and reconnect the cables to the controller.
15. Power up the controller (see page 22).

Cooling Fan (MXe)

To replace the cooling fan in an MXe:

1. Power down the controller.
2. Remove the controller cover (see page 101).
3. Remove the two fan screws above the edge of the controller chassis.
4. Disconnect the cable and lift out the fan unit.
5. Set the new fan unit in place.
6. Secure the unit with two screws and connect the cable.
7. Replace the top cover.
8. Power up the controller (see page 22).

Power Supply Unit (MXe)

To replace a power supply unit in a single power supply MXe:

1. Set the AC power switch to OFF.
2. Remove the power cord from the AC receptacle on the power supply.
3. Loosen the thumb screw on the power supply.
4. Remove the defective power supply unit from the rear of the controller.
5. Slide the new power supply unit into the controller.
6. Push to seat the power supply into the system power connector.
7. Secure the thumb screw and connect the power cord.
8. Set the AC power switch to ON.

Stratum 3 Clock Module

To replace the clock module in all controllers:

1. Power down the controller (see page 99).
2. Remove the cover (see page 99, page 101, or page 101).
3. Remove the screws from the clock module.
4. Remove the clock module.
5. Seat the new clock module onto the main board.
6. Replace the screws that you removed from the clock module.
7. Replace the top cover.
8. Power up the controller (see page 22).

Install ASU II FRUs

The ASU II can be configured with one or two line cards. You can install one or two 16 port ONS cards, one or two 4 + 12 port combo cards (4 LS trunks and 12 ONS lines), or one of each.

Line Card (16 Port ONS / 4+12 Port Combo)

To install a 16 port ONS or 4 + 12 port combo card:

1. If necessary, loosen the thumb screw and remove the blanking plate from the cabinet rear.
2. Slide the card into the slot, with the lock latch open, and seat it securely.
3. Close the lock latch and tighten the thumb screw with a Phillips screwdriver.
4. Connect the Amphenol cable and secure the strap.

Power Supply

To replace the ASU II AC power supply:

1. Remove the power cord from the power supply AC receptacle.
2. Loosen the thumb screw on the power supply.
3. Open the lock latch and slide the card out of the slot.
4. Slide the new power supply into the slot on the rear of the ASU II, with the thumb screw on the right.
5. Push to seat the power supply into the system power backplane.
6. Secure the thumb screw and tighten it with a Phillips screwdriver.
7. Insert the AC power cord into the power supply AC receptacle.

Install Peripheral Cabinet FRUs

Tip: The CX and CXi controllers do not support Peripheral Cabinets.

The peripheral cabinet has the following Field Replaceable Units (FRUs):

- Circuit card (page 143)
- Power converter (page 144)
- Power distribution unit (page 145)
- Cooling fan (page 146)
- Expanded peripheral cabinet (page 149)
- FIM (page 147)
- Peripheral switch controller card (page 150)

Removing/Replacing the Front Panel of a Peripheral Cabinet or DSU

To remove the front panels:

1. Insert a slot screwdriver in the slot on the right side of the front grill and pry it open.
2. Loosen the two screws on the front cover and lift the cover up and away from the cabinet.

To replace the front panels:

1. Align the front panel screws with the holes in the cabinet and tighten the two screws.
2. Insert the left front grill into the slot and snap it closed.

Powering Down the Peripheral Cabinet

To power down the peripheral cabinet:

1. Remove the front panels.
2. Switch off the power converter.
3. Set the power switch on the rear of the unit to '0' (OFF).
4. Unplug the external power cord at the rear of the unit.

Powering Up the Peripheral Cabinet

To power up the peripheral cabinet:

1. Ensure the voltage selector switch is set to the required setting for your country.
2. Connect the external power cord at the rear of the unit.
3. Set the power switch on the rear of the unit to "I" (ON).
4. Switch on the power converter.
5. Replace the front panels.

Replacing Circuit Cards

Refer to “Safety Considerations” on page 98.

WARNING: HAZARDOUS VOLTAGES CAN EXIST ON INSTALLED PERIPHERAL CARDS EVEN WHEN POWER IS REMOVED FROM THE SYSTEM. GRASP CARDS BY THE LOCK LATCHES ONLY. DO NOT TOUCH THE SIDES OF CARDS.

CAUTION: To prevent static damage to electrical components, wear the anti-static wrist strap whenever you handle circuit cards.

Tip: You can replace peripheral interface cards or DSU cards while the unit is operating.

To remove a circuit card from a peripheral or DSU cabinet:

1. Log into the System Administration Tool (see page 8).
2. In the **All forms (alphabetical)** list, click **Maintenance Commands**.
3. Enter BUSY <PLID of faulty card> and enter CD (courtesy down).
4. Enter STATE <PLID of faulty card> to confirm that all circuits are busy.
5. Pull the upper and lower latches outward until they are both in the horizontal release position.
6. Draw the card toward you.
7. Immediately place the card in an anti-static bag.

To install a circuit card in a peripheral or DSU cabinet:

1. For cards that have switches, refer to the card's hardware description for information about switch settings (see page 289).
2. Check that the connector pins are straight.
3. Slide the card into the slot.
4. Move the card latches to the vertical position to secure the card.
5. In the **All forms (alphabetical)** list, click **Maintenance Commands**.
6. Enter RTS <PLID> to return the circuits to service.

Replacing a Power Converter

To replace a power converter in a peripheral cabinet:

1. Remove the front panels of the peripheral cabinet (see page 142).
2. Power down the peripheral cabinet (see page 142).
3. Disconnect the internal AC power cord:
   a. Unscrew and remove the AC power cord access cover plate on the rear of the unit (see Figure 26 on page 145).
   b. Unplug the internal AC power cord from the rear of the AC power converter (accessed through a cutout in the backplane).
4. Remove the converter:
   a. Move the card latches on the converter to the horizontal position.
   b. Carefully withdraw the converter unit from the shelf.
5. Unpack and inspect the new converter.
   a. Unpack the converter and remove all packing materials.
   b. Inspect the converter to ensure that the unit is not dented or scratched, and that all fittings are secure.
6. Install the new converter:
   a. Slide the replacement converter into position (slots 13 - 15).
   b. Move the card latches to the vertical position to secure the converter.
   c. Plug the internal AC power cord from the Power Distribution Unit into the AC power converter, through the cutout in the backplane.

d. Replace the cover plate over the access cutout in the backplane, and fasten in place with the screws removed in step 3.

7. Power up the peripheral cabinet (see page 142).

8. Replace the front panels on the peripheral cabinet (see page 142).

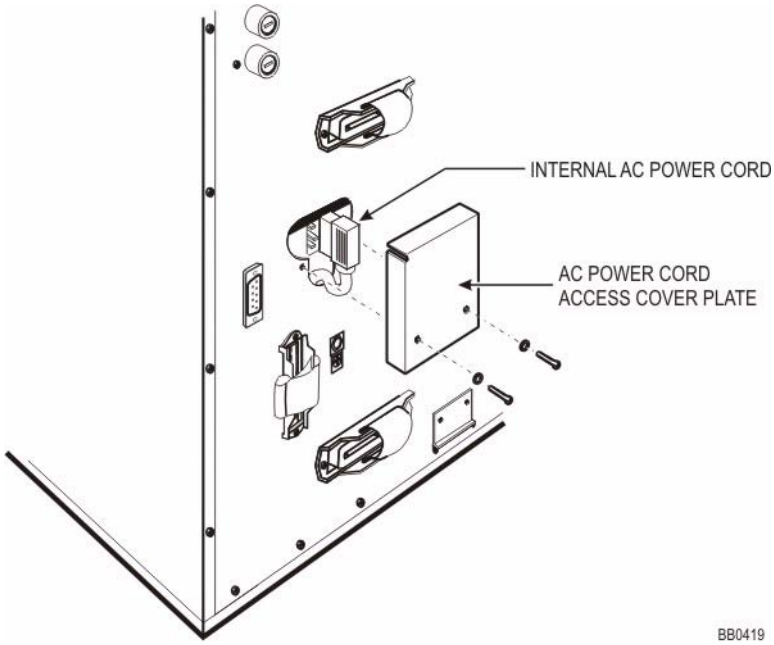


Figure 26: Peripheral Cabinet Power Converter Connections

Replacing the Power Distribution Unit (PDU)

Refer to “Safety Considerations” on page 98.

To replace a PDU in a peripheral cabinet:

1. Power down the unit (see page 142).

2. Remove the front panels (see page 142).

3. Remove the PDU:

a. Unplug the external power cord from the PDU.

b. Remove the PDU internal power cover plate.

c. Unplug the PDU internal power cord from the power converter.

d. Remove the outer screws on the PDU faceplate.

e. Pull the PDU out until you can access the fan power connector at the rear of the PDU.

f. Disconnect the fan power connector and remove the PDU.

4. Install a new PDU:

a. Unpack and inspect the new PDU for damage.

b. Set the power switch on the new PDU to off (O).

c. Connect the fan power connector at the rear of the PDU.

d. Insert the PDU and replace the outer screws on the PDU faceplate.

e. Plug the PDU internal power cord into the power converter.

f. Replace the internal power access cover plate.

g. Plug the external power cord into the PDU.

5. Power up the unit (see page 142).

6. Replace the front panels (see page 142).

Replacing a Cooling Fan

Refer to "Safety Considerations" on page 98.

To replace a cooling fan in a peripheral cabinet:

1. Power down the unit (see page 142).

2. Remove the front panels (see page 142).

3. Disconnect the fan assembly.

4. Remove the defective fan.

5. Insert the new fan.

6. Replace the fan assembly.

7. Replace the front panels (see page 142).

8. Power up the unit (see page 142).

Replacing the Fiber Interface Module (FIM)

WARNING: POWER MUST NOT BE APPLIED TO THE PERIPHERAL CABINET WHILE THE FIM IS REPLACED.

To replace a FIM in a peripheral cabinet:

1. Power down the unit and remove the front panels (see page 142).
2. Attach the anti-static strap to your wrist.
3. If you need more room, remove the power converter and the peripheral switch controller (PSC).
4. Disconnect the fiber cables from the FIM.
   - Place dust caps on the cable and on the FIM connectors.
5. Pull the FIM out gently from slot 17, unplugging it from the backplane.
6. Unpack the new FIM, and inspect it to ensure that it is not damaged.
7. Slide the new FIM into the bottom of slot 17 until it connects with the backplane firmly.
8. Fasten the new FIM in place with the two screws provided or the latch on the card guides.
9. Attach the FIM cable by following the steps in Connect the Fiber Optic Cable (see page 42).
10. If the PSC and power converter were removed, replace them.
11. Power up the unit and replace the front panels (see page 142).

Expanding a Peripheral Cabinet II

Tip: A Peripheral Expansion Node II is no longer an orderable item. Instead, a Peripheral Node II is ordered and converted to an Expansion Node by using the Peripheral Node Expansion Kit.

To convert a peripheral cabinet II to an expanded peripheral cabinet II:

1. Unpack, position, and ground the new cabinet. This cabinet will be used as the slave cabinet.
2. Unpack the peripheral node expansion Kit. It contains 2 interconnect cards, 1 interconnect cable, and 2 EMI filter kits.
3. Remove the front panel from the slave cabinet.

4. Remove the PSC from slot 16 in the slave cabinet, and replace it with a peripheral interconnect card. The PSC is not required.
5. Attach an EMI Filter Kit to the back of the slave cabinet:
   a. Remove the sliding door from the back of the cabinet.
   b. Attach the filter kit using the screws from the sliding door.
   c. Route the attached filter cable through to the front of the cabinet.
   d. Attach the cable to the front of the peripheral interconnect card.
6. Install up to 12 peripheral interface cards in slots 1 through 12 of the slave cabinet (as required for your system).
7. Proceed to connect an expanded peripheral node II to a peripheral node II (see steps below).

To connect an expanded peripheral cabinet II to peripheral cabinet II:

1. Convert a peripheral cabinet II to an expanded peripheral cabinet II (see steps above).
2. Unpack, position, and ground the master cabinet.
3. Remove the front panel from the master cabinet.

Tip: The master cabinet includes a power converter in slots 13 through 15, a PSC in slot 16, and a FIM in slot 17. The slave cabinet includes a power converter in slots 13 through 15 and a peripheral interconnect card in slot 16. An additional peripheral interconnect card and EMI filter are also available from the peripheral node expansion kit.

4. Detach the fiber cables from the FIM in the master cabinet, and remove them through the cable port on the back of the cabinet.
5. Install the additional peripheral interconnect card in slot 16B of the master cabinet.
6. Attach an EMI filter kit to the back of the master cabinet:
   a. Remove the sliding door from the back of the cabinet.
   b. Attach the filter kit using the screws from the sliding door.
   c. Route the attached filter cable through to the front of the cabinet.
   d. Attach the cable to the front of the peripheral interconnect card.
   e. Loosen the door screws on the back of the filter kit and slide the door up.
   f. Follow the steps in Connect the Fiber Optic Cable.

g. Tighten the door screws on the back of the filter kit to hold the FIM cables securely in place.

7. Install up to 12 peripheral interface cards in slots 1 through 12 of the master cabinet (as required for your system).
8. Cable the master cabinet to the MDF, and power it up to ensure that it works properly.
9. Attach the cabinet interconnect cable to the EMI filter kit on each cabinet.
10. Power up the slave cabinet to ensure that it works properly.
11. Replace the front panels on both cabinets.

Installing an Expanded Peripheral Cabinet

Tip: The peripheral expansion node II is not orderable. Instead, a peripheral node II is ordered and converted to an expansion node by using the peripheral cabinet expansion kit (see page 147).

The expanded peripheral cabinet II consists of the following components:

- Peripheral node II - peripheral cabinet II, power converter, peripheral switch controller II card, fiber interface module.
- Peripheral expansion node II - peripheral cabinet II, power converter, peripheral interconnect cards (2), EMI filter kits (2), cabinet interconnect cable.

Review “Safety Considerations” on page 98 before installing an expanded peripheral cabinet.

To install an expanded peripheral cabinet:

1. Unpack, position, and ground both cabinets (see page 40).
2. Remove the front panels from both cabinets (see page 142).
   - The master cabinet includes a power converter in slots 13 to 15, a peripheral switch controller (PSC) in slot 16, and a fiber interface module (FIM) in slot 17.
   - The slave cabinet includes a power converter in slots 13 to 15, a peripheral interconnect card in slot 16, and an additional peripheral interconnect card with the package.
3. Install the additional peripheral interconnect card in slot 16B of the master cabinet.

4. Install up to 12 peripheral interface cards in slots 1 to 12 of each cabinet, as required for your system.
5. Attach an EMI filter kit to the back of the master cabinet:
   a. Remove the sliding door from the back of the cabinet and attach the filter kit using the screws from the sliding door (route the attached filter cable through to the front of the cabinet).
   b. Attach the cable to the front of the peripheral interconnect card.
   c. Loosen the door screws on the back of the filter kit and slide the door up. Follow the steps in Connect the Fiber Optic Cable.
   d. Tighten the door screws on the back of the filter kit to hold the FIM cables securely in place.
6. Cable the cabinet to the MDF (see page 45) and power it up to ensure it works properly.
7. Repeat step 5, attaching the remaining EMI filter kit to the slave cabinet (skip steps c and d since there is no FIM installed in the slave cabinet).
8. Attach the cabinet interconnect cable to each EMI filter kit, connecting the two cabinets together.
9. Power up the slave cabinet and ensure it works properly.
10. Replace the front panels of each cabinet (see page 142).

Replacing a Peripheral Switch Controller Card

CAUTION: Wear an anti-static strap whenever you handle circuit cards.

To replace a peripheral switch controller card:

1. Power down the peripheral cabinet (see page 142).
2. Replace the faulty peripheral switch controller card with the new peripheral switch controller card.
3. Power up the peripheral cabinet (see page 142).

Install Digital Service Unit FRUs

Tip: The CX and CXi controllers do not support Digital Service Units.

The DSU has the following Field Replaceable Units (FRUs):

- Circuit card (page 143)
- BRI card (page 152)
- BRI interface assembly (page 153)
- Formatter cards (CEPT, DS1) (page 154)
- PRI card (page 154)
- Peripheral resource card (page 156)
- FIM (page 157)
- R2 card (page 158)

Removing/Replacing the Front Panel

See “Removing/Replacing the Front Panel of a Peripheral Cabinet or DSU” on page 142.

Powering Down the DSU Unit

To power down the DSU:

1. Set the power switch on the rear of the unit to ‘0’ (OFF).
2. Unplug the external power cord at the rear of the unit.

Powering Up the DSU Unit

To power up the DSU:

1. Connect the external power cord at the rear of the unit.
2. Set the power switch on the rear of the unit to "I" (ON).

Replacing Circuit Cards

See “Replacing Circuit Cards” on page 143.

Installing a BRI Card

Before you install the BRI card, ensure that:

- The configuration includes a CEPT formatter card that has an unused hybrid circuit (one Rx/Tx pair) configured with DPNSS protocol.
- The system has a free DSU slot for the BRI card.
- The wiring from the network termination terminal equipment (NTTE), network termination 1 (NT1), or terminating equipment is CAT 5 UTP.
- A computer is available for use as a BRI maintenance terminal (see "BRI Network Services Unit" on page 37 for details).

To install a BRI card:

1. Program the customer data using the System Administration Tool (see the Online Help for details).
2. Install the BRI interface assembly (see Figure 27 below). For details, see "Install the Interface Assemblies" on page 49.

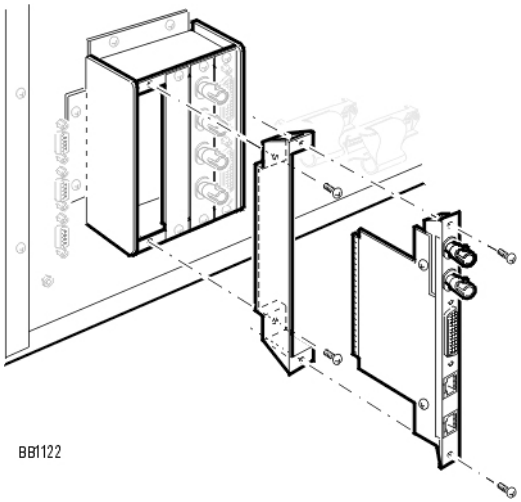


Figure 27: BRI Interface Assembly Installation

3. Install the BRI card. For details, see page 50).
4. Using a BNC to BNC cable, connect the Rx port on the BRI interface assembly to the Tx port on the CEPT interface assembly (see Figure 28 on page 153).

5. Using a BNC to BNC cable, connect the Tx port on the BRI interface assembly to the Rx port on the CEPT interface assembly.
6. Using the 44-pin D-type to Amphenol cable, connect the ISDN BRI port on the BRI interface assembly to the distribution frame, RJ-45 patch panel, or network terminating rack. Refer to the Hardware Technical Reference Manual for BRI Card cable pinouts.
7. Connect the BRI card to the maintenance PC (see “BRI Network Services Unit”, Step 4, a and b on page 38).
8. On the BRI maintenance PC, program the BRI card using the VT100 emulator. See Technical Bulletin 58004741 (*Basic Setup Guide for the MC268 BRI Card*) for more information.

Tip: Even though the Technical Bulletin is written for the SX-2000 system, the parameters described are also applicable to the 3300 ICP system.

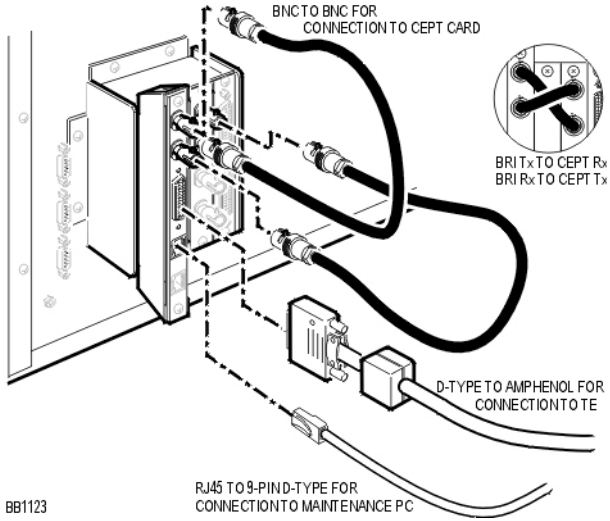


Figure 28: BRI Card Connections

Next: After installing the BRI card, go back to page 49.

Installing a Formatter Card (CEPT, DS1)

The CEPT and DS1/T1 formatter cards are installed in any empty DSU slot. The DSU cabinet supplies the power for the card and provides a message interface back to the controller through the FIM interface and the fiber optic cable.

Tip: Before you install the card, ensure that you have programmed the card using the System Administration Tool (see the Online Help for details) and installed the interface assembly (see "Install the Interface Assemblies" on page 49).

To install a formatter card:

1. Install the formatter card. For details, see "Install the DSU Cards" on page 50.
2. If you are installing a CEPT card, connect the cables from the external network to the BNC connectors on the CEPT interface assembly.
3. If you are installing a DS1 card, connect the 22 AWG (22 IWG) shielded twisted pair cables from the external network to the DB-15 pin connectors on the DS1 interface assembly (see Table 72 on page 290 for the DB-15 connector pinout and Table 73 on page 291 for the pinouts for line/network termination).

Next: Go to "To test a formatter card:" below.

To test a formatter card:

If the installation is successful, the card will boot up.

1. Inspect the LEDs on the faceplate to verify that the card is functioning (see "BRI Card" on page 356 for details).
2. Log into the System Administration Tool (see page 8).
3. In the **All forms (alphabetical)** list, click **Maintenance Commands**.
4. Enter STATE <PLID of the card> to verify that the trunks associated with the corresponding channels are all in IDLE state.

Next: Go back to "Install the Interface Assemblies" on page 49.

Installing a PRI Card

Before you install the PRI card, ensure that:

- The system has a free DSU slot for the PRI card.
- The PRI card has been upgraded to use ISDN 7.0 (LW31.1+).

- A computer is available to connect to the PRI card as a maintenance PC. IMAT provides the communication between the card and the computer. Refer to page 7 for PC requirements.
- Install IMAT on the maintenance PC (see page 88).

Installation Sequence

Install the PRI card in the following sequence:

- Program the card using the System Administration Tool (see the Online Help for details)
- Install the interface assembly (see page 49)
- Install the PRI card
- Save the IMAT database onto the PRI card
- Connect the PRI card to the ISDN network
- Test the PRI card

Install the PRI Card

The PRI card is installed in any empty DSU slot. The DSU cabinet supplies the power for the card and provides a message interface back to the control cabinet through the FIM interface and the fiber optic cable.

Save the IMAT Database onto the PRI Card

Before you save the IMAT database onto the PRI card, you need to configure the PRI database and connect the computer to the PRI card. For more information, refer to the IMAT online help.

Connect the PRI card to the ISDN network

To connect the PRI card to the ISDN network:

1. Unpack and inspect the ISDN PRI cables. Retain the original package.
2. Plug the ISDN PRI cable into the PRI port(s).
3. Plug the ISDN PRI cable(s) into the network terminating equipment.

Tip: A dual-port card needs two ISDN PRI cables when using both ports.

Test the PRI Card

If the installation is successful, the PRI card will boot up, configure itself with the default database, and communicate with the system.

To test the PRI card:

1. Inspect the LEDs on the faceplate to verify that the card is functioning. See Faceplate LEDs on page 356.
2. Log into the System Administration Tool (see page 8).
3. In the **All forms (alphabetical)** list, click **Maintenance Commands**.
4. Enter STATE <PLID of the card> to verify that the trunks associated with the PRI channels are all in IDLE state.

Installing a Peripheral Resource Card (PRC)

Each FIM in the DSU must have a peripheral resource card (PRC) installed above it.

WARNING: POWER MUST NOT BE APPLIED TO THE PERIPHERAL CABINET WHILE YOU ARE INSTALLING THE PERIPHERAL RESOURCE CARD.

To install a peripheral resource card:

1. Unpack the PRC.
2. Slide the PRC into the top of slot 1 until it connects firmly with the backplane (see Figure 69 on page 292).
3. Fasten the PRC in place using the two screws provided, or use the latches on the card guides.
4. If a second PRC is required, install it in the same manner in the top of slot 6 (see Figure 69 on page 292).

Next: After installing the PRC, go back to "Install the Interface Assemblies" on page 49.

Replacing a DSU FIM

Refer to “Safety Considerations” on page 98.

To replace a DSU FIM:

1. Power down the unit (see page 151).
2. Remove the front panels (see page 142).
3. Attach an anti-static strap to your wrist.
4. Remove adjoining DSU cards.
   a. Pull out the 2 DSU cards next to the FIM being replaced in order to access the FIM slot.
5. Remove the FIM.
   a. Disconnect the internal optical fiber cables from the FIM faceplate. Mark the cable connectors so they are replaced correctly on the new FIM.
   b. Remove the screws or release the latches on the FIM.
   c. Pull the FIM out gently from slot 1 or 6, unplugging it from the backplane.
6. Install a new FIM.
   a. Slide the new FIM into the bottom slot 1 or 6, making sure it is firmly connected to the backplane DIN connector.
   b. Fasten the screws or release the latches on the FIM.
   c. Remove the plastic caps from the cable connectors on the FIM faceplate and connect the optical fiber cables to those connectors.
7. Replace the DSU cards.
8. Power up the unit (see page 151).
9. Replace the front panels (see page 142).

Installing a DSU FIM

WARNING: FIBER OPTIC SOURCES EMIT INFRARED LIGHT INVISIBLE TO THE HUMAN EYE THAT CAN DAMAGE THE RETINA. NEVER LOOK DIRECTLY INTO A SOURCE OR INTO THE END OF A FIBER ENERGIZED BY A SOURCE. WHEN WORKING WITH RAW FIBER OPTIC CABLE, BE CAREFUL OF FIBER ENDS OR SLIVERS THAT CAN PUNCTURE THE SKIN AND CAUSE IRRITATION.

To install a DSU FIM:

1. Attach the anti-static strap to your wrist.
2. Unpack the FIM. Inspect the FIM to ensure that it is not damaged.
3. Remove the DSU unit front door
   a. Pry open the two latches on the right hand side of the black cover panel on the front door, and swing the cover panel off to the left.
   b. Loosen the two screws under the black panel to release the front door.
   c. Pull the top corners of the front door out and lift it off the lip at the bottom front of the unit.
4. Remove the DSU cards from the cabinet. Insert each circuit card in a separate anti-static bag.
5. Slide the FIM into the bottom slot 1 or slot 6 until it connects with the backplane firmly. Fasten the FIM in place with the two screws provided or use the latch on the card guides.
6. Remove the anti-static strap from your wrist.

Installing an R2 Card

Before you install the R2 card, ensure that:

- The system has a free DSU slot for the R2 card
- A computer is available to connect to the R2 card as a maintenance PC. IMAT provides the communication between the card and the computer. Refer to page 7 for PC requirements.
- Install IMAT on the maintenance PC (see page 88).

Installation Sequence

Install the R2 card in the following sequence:

- Program the card using the System Administration Tool (see the Online Help for details)
- Install the interface assembly (see page 49)
- Install the R2 card
- Save the IMAT database onto the R2 card
- Connect the R2 card to the PSTN network
- Test the R2 card

Install the R2 Card

The R2 card is installed in any empty DSU slot. The DSU cabinet supplies the power for the card and provides a message interface back to the control cabinet through the FIM interface and the fiber optic cable.

Save the IMAT Database to the R2 Card

Before you save the IMAT database to the R2 card, you need to configure the R2 database and connect the computer to the R2 card. For more information, refer to the IMAT online help.

Connecting the R2 Card to the PSTN Network

To connect the R2 card to the PSTN network:

1. Unpack and inspect the R2 coaxial cables. See “R2 Card Connections” on page 160. Retain the original package.
2. Plug the R2 cable(s) into the R2 port(s).
   See Table 74 on page 292 for the R2 card RJ-45 connector pinout.

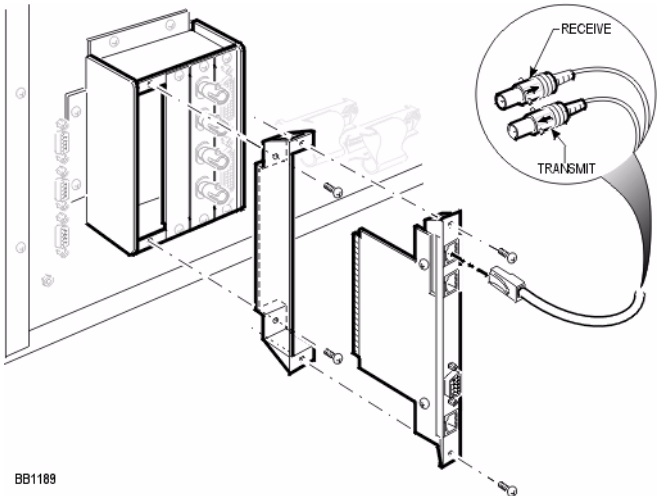


Figure 29: R2 Card Connections

3. Plug the R2 cable(s) into the network terminating equipment. See Table 74 on page 292 for the R2 card RJ-45 connector pinout.

Tip: A dual-port card needs two coaxial cables if you are using both ports.

Tip: The R2 coaxial cables have both transmit (arrow pointing away from cable) and receive (arrow pointing towards cable) connectors. When you set the card for trunk side termination (jumper at **NT** position), connect the R2 coaxial cable transmit lead to the network receive connector, and the R2 coaxial receive lead to the network transmit connector. When you set the card for line side termination (jumper at **LT** position), connect the R2 coaxial cable transmit lead to the network transmit connector, and the R2 coaxial receive lead to the network receive connector.

Testing the R2 Card

If the installation is successful, the R2 card will boot up, configure itself with the default database and communicate with the system.

To test the R2 card:

1. Inspect the LEDs on the faceplate to verify that the card is functioning. See Faceplate LEDs on page 359.
2. Log into the System Administration Tool (see page 8).

3. In the **All forms (alphabetical)** list, click **Maintenance Commands**.
4. Enter STATE <PLID of the card> to verify that the trunks associated with the R2 channels are all in IDLE state.

Next: After installing the R2 card, go back to “Install the Interface Assemblies” on page 49.

Install SUPERSET HUB FRUs

Installing a Fiber Interface Module

To install a FIM in a SUPERSET HUB:

1. Power down the SUPERSET HUB unit by disconnecting the power cord.
2. Disconnect the fiber optic cables from the fiber interface module.
3. Remove the two screws which secure the FIM to the unit and remove the FIM.
4. Replace the FIM. Ensure that the edge connector on the FIM is correctly located in the socket inside the unit.
5. Replace the two screws which secure the FIM to the unit.

Migrate an SX-2000 PBX

Only the MicroLight can be migrated using this procedure. To migrate an SX-2000 Light Non-redundant system simply replace the control cabinet with a 3300 controller. Similarly replace a 3200 ICP controller with a 3300 controller. You cannot migrate the SX-2000 Light redundant control system to an equivalent 3300 ICP.

To upgrade SX-2000 MicroLIGHT hardware for 3300 ICP control:

1. Remove the Main Controller (MMC) from slot 1/1/1.
2. Install a triple FIM in that slot.
3. Remove any FIM carrier cards in the DSU slots.
4. Do NOT remove any other cards.

Tip: Refer to Knowledge Base Article 04-1000-00068 (TB 58005193) for Migration procedure details.

An SX-2000 MicroLIGHT system converted to 3300 control uses fiber interface modules (FIM) of the triple FIM carrier card as required:

- One triple FIM carrier card
- One control resources card
- One peripheral switch control (PSC) Card
- One to eight peripheral interface cards (PIC)
- Optionally, one to four DSU cards 0 DSU1 through DSU4.

Triple FIM Carrier Card Port	When connected, support
Circuit 1 (bottom)	PER cards
Circuit 2	DSU in slots 2 and 3
Circuit 3 (top)	DSU in slots 4 and 5

Any DSU or peripheral cabinets that were connected to the MicroLIGHT, must now be connected by fiber directly to the 3300 ICP controller.

Figure 30: SX-2000 MicroLIGHT under 3300 control

Chapter 5
Troubleshooting

About this Chapter

This chapter provides standard procedures to troubleshoot the most common problems and is organized as follows:

- IP Phone Boot Sequence (page 225)
- Checking the IP Phone Progress Display (page 230)
- IP Console (page 231)

IMPORTANT: Please see "Before You Contact Technical Support" on page 179 before contacting Mitel Technical Support.

Tip: Maintenance and troubleshooting of your LAN/WAN network is the responsibility of your network provider. Mitel Technical Support can help you isolate minor network problems; Technical Support will escalate complex network problem to Professional Services, a billable service.

Tip: For information on troubleshooting resiliency problems, refer to the **Mitel 3300 ICP Resiliency** document on Mitel OnLine.

Troubleshooting Tools

Table 8 below lists the tools available to help you troubleshoot a 3300 ICP system.

Table 8: Troubleshooting Tools

Tool Name	Location	Function	Applies to
Alarms Detail Form	System Administration Tool (Maintenance and Diagnostics).	Provides the definition and location of the alarms.	3300 ICP system.
Logs	System Administration Tool (Maintenance and Diagnostics).	Provides a history of the software logs.	3300 ICP software.
Device Connectivity Form	System Administration Tool (Maintenance and Diagnostics)	Reports previous and latest Layer 2 MAC and port number.	IP Phones.
L2 STAT commands	System Administration Tool (Maintenance and Diagnostics)	Provides L2 switch ports details: MAC address, status, Spanning Tree information	CXi and MXe internal L2 switch.
IMAT	Maintenance or IMAT PC.	Allows you to load databases on the NSU PRI.	PRI/QSIG and R2 NSUs.

(Page 1 of 3)

Table 8: Troubleshooting Tools (continued)

Tool Name	Location	Function	Applies to
IP Phone Analyzer	IP Phone Analyzer PC	Supports IP Phone troubleshooting.	IP Phones.
Java Console	Console PC	To troubleshoot IP Consoles (see Note).	5550 IP Console.
LEDs	Front of each unit.	To provide overall status of unit.	3300 ICP hardware.
	Back of MXe.	To provide status of power supplies and RAID controller.	3300 ICP hardware.
NSU Shell	NSU Maintenance Port.	Lists NSU error messages.	All NSUs.
Logviewer (see page 237)	FTP Logs on controller (ftp from Maintenance PC)	Provides a history of software logs (pstswlog, xrtc, xe2t, premortem).	3300 ICP software.
RTC Shell	Controller Maintenance Port	Shows error messages during the installation of the 3300. Monitors the boot sequence.	3300 ICP software.
Phone Debug Option	IP Phones with display.	Allows you to • Monitor the phone settings • Program a static IP address (see page 54) • Hard code connection speed and duplex mode (reboot while pressing 9) **Auto-negotiation is preferred.**	IP Phone with display.

(Page 2 of 3)

Table 8: Troubleshooting Tools (continued)

Tool Name	Location	Function	Applies to
Dual Mode Phone Debug Option	5215 IP Phone (Dual Mode), 5220 IP Phone (Dual Mode, 5330 IP Phone, and 5340 IP Phone.	Allows you to configure/view: • Network parameters • Hardware components • Set the phone mode • PIN, IP address, DHCP, Video.	Dual Mode IP Phones
SMDR	Controller (telnet from Maintenance PC).	Provides the call paths (call logs).	3300 ICP system.
Note: To turn on the Java console: at the IP Console PC, select **Start/Settings/Control Panel**, and launch **Java Plug-in**.			
			(Page 3 of 3)

Using the Phone Debug Option

You can use the debug function on display IP Phones and Appliances, excluding the Dual Mode IP Phones (see below). Press the Up/Down volume keys, or softkeys (if available) to navigate the options.

To use the phone debug option:

1. Hold down both volume keys at the same time.
2. Enter **debug** (33284) on the telephone key pad (handset on hook).
3. On a 5020/5010 IP Phone, press **Superkey** to display categories.
4. View detail for the following categories:
   - **Version info** (Main and Boot loads)
   - **Network** (IP information, such as the telephone's IP Address, Subnet Mask, ICP List, DHCP Server Address, TFTP Server Address, Gateway IP (Router) VLAN/Priority, DSCP)
   - **Telephony/DSP** (Telephone Directory Number and other design information)
   - **Connection** (Link Reset; Hard Reset; Toggle ERROR persistence; CDP Support; Port Settings; Static Settings)

- **Browser Config** (Proxy Server Configuration, Debug Stream On/Off, etc.)
- **Memory Stats** (Various design memory details)

5. Press **Phone View** to exit the debug menu, or Press **Cancel** on the 5020 IP Phone.

Using the Dual Mode Phone Debug Option

On the 5215 IP Phone (Dual Mode), press ***** (yes), **0** (default), and # (no); on the 5220 IP Phone (Dual Mode), press the three softkeys to select menu items.

Accessing the Configuration Menu

Method A: To access the menu during the phone boot sequence:

- Hold down both volume keys until NETWORK PARAMETERS? appears.

Method B: If the phone is up and running with the MiNet main load:

1. Hold down both volume keys at the same time.
2. Continue to hold the down volume key and release the up volume key.
3. Press 234 on the telephone key pad and then release the down key.
   - NETWORK PARAMETERS? appears.
4. Proceed to “Viewing/Modifying Network Parameters” on page 172, “Configuring Hardware Components” on page 173, “Setting the Phone Mode” on page 173, or “Using Tools and Features” on page 173.

Method C: Using hotkeys, at power up, press and hold the following key combinations:

Key Sequence	Function
* and 6 (M)	Change mode to MiNet
* and 7 (S)	Change mode to SIP
7	Jump to “Config Teleworker” menu
*	Erase the PIN and VCON configuration
any other keypad keys	Display “Configure Phone” prompt
Note: Hotkeys access provides limited access. Methods A and B provide full access	

Viewing/Modifying Network Parameters

You can view and modify the following network parameters on the phone:

- Phone IP address (current and static)
- Gateway IP address (current and static)
- Subnet mask (current and static)
- Current controller IP address
- TUG1, TUG2, TUG3, and TUG4 IP addresses (current)
- TFTP server IP address (current)
- VLAN ID and priority (current and static)
- DSCP value
- IPA IP address (current and static)
- TUG IP address (static)
- TFTP SVC IP and port (static).

To view and modify network parameters:

1. Access the Configuration Menu (see page 171).
2. At NETWORK PARAMETERS?, press **Yes**. VIEW CURRENT VALUES? appears.
3. Do one of the following:
   - Press **Yes**, and then press the Up/Down volume keys to view each setting. When you return to VIEW CURRENT VALUES?, press **No**. VIEW STATIC VALUES? appears.
   - Press **No**. VIEW STATIC VALUES? appears.
4. Do one of the following:
   - Press **Yes**, and then press the Up/Down volume keys to view each setting. When you return to VIEW STATIC VALUES?, press **No**. MODIFY STATIC VALUES? appears.
   - Press **No**. MODIFY STATIC VALUES? appears.
5. Do one of the following and then reboot the phone:
   - Press **Yes**, and then press the Up/Down volume keys to scroll through each setting. Use the keypad to modify parameter(s), and then follow the prompts to store the changes and reboot the phone.

- To reset the factory defaults, press **Default**, and then follow the prompts to set and store the factory defaults and reboot the phone.

6. To exit the current menu without a reboot:
   - To return to the main menu, press **Yes** at EXIT MENU?
   - To return to the default display, press **Superkey**.

Configuring Hardware Components

You can configure the speed and duplex for the LAN and PC ports.

To manually configure hardware components:

1. Access the Configuration Menu (see page 171).
2. Press **No** until HARDWARE CONFIG? appears, and then press **Yes**. MODIFY SETTINGS? appears.
3. Do one of the following and then reboot the phone:
   - To modify the current hardware components, press **Yes**, and then follow the prompts to modify each setting and store the changes.
   - To reset the factory defaults, press **Default**, and then follow the prompts to set and store the factory defaults.
4. To exit the current menu without a reboot:
   - To return to the main menu, press **Yes** at EXIT MENU?
   - To return to the default display, press **Superkey**.

Setting the Phone Mode

You can program the 5215 or 5220 IP Phone (Dual Mode) to use MiNET or to work remotely using either SIP or Teleworker Solution (6010).

For SIP configuration information, refer to the 5207/5215/5220 IP Phone Installation Guide (56006499, Rev A) packaged with the phone, and to the 5215/5220 IP Phone SIP User Guide available at www.mitel.com.

Using Tools and Features

- “Erasing the Registration PIN” on page 174
- “Pinging IP Addresses” on page 174
- “Conducting a DHCP Trace” on page 174
- “Configuring Video Conferencing Parameters” on page 175
- “Restoring Factory Default Settings” on page 176.

Erasing the Registration PIN

1. Access the Configuration Menu (see page 171).
2. Press **No** until TOOLS AND FEATURES? appears, and then press **Yes**. ERASE PIN? appears.
3. Press **Yes**, and then follow the prompts to erase the PIN and to store the changes and reboot the phone.
4. To exit the current menu without a reboot:
   - To return to the main menu, press **Yes** at EXIT MENU?
   - To return to the default display, press **Superkey**.

Pinging IP Addresses

1. Access the Configuration Menu during the phone boot sequence.
2. Press **No** until TOOLS AND FEATURES? appears.
3. Press **Yes**, and then press **No** until PING TEST? appears.
4. Press **Yes** and then follow the prompts to conduct the PING test.
5. To exit, do one of the following:
   - To return to the main menu, press **Yes** at EXIT MENU?.
   - To return to the default display, press **Superkey**.

Conducting a DHCP Trace

There is a delay while the phone performs DHCP discovery. The result of the trace displays the following information:

- Phone and Gateway IP addresses
- Subnet mask
- WINS, DNS, TFTP, ICP and Video servers
- DHCP server and Mitel IDs
- Lease
- T1 and T2
- VLAND ID and priority
- HTTP proxy
- IPA address.

To conduct a DHCP trace on the Dual Mode phone:

1. Access the Configuration Menu (see page 171).
2. Press **No** until TOOLS AND FEATURES? appears.
3. Press **Yes**, and then press **No** until DHCP Trace? appears.
4. Press **Yes**, and press the Up/Down volume keys to view the results of the DHCP trace.
5. To exit, do one of the following:
   - When you return to DHCP TRACE?, press **No**.
   - To return to the default display, press **Superkey**.

Configuring Video Conferencing Parameters

To configure video conferencing on the 5220 IP Phone (Dual Boot):

1. Access the Configuration Menu (see page 171).
2. Press **No** until TOOLS AND FEATURES? appears.
3. Press **Yes** and then press **No** until VIDEO CONFIGURATION? appears.
4. Press **Yes**. VIEW PARAMETERS? appears.
5. Do one of the following:
   - Press **Yes** and then follow the prompts. When you return to VIEW PARAMETERS?, press **No**. MODIFY PARAMETERS appears.
   - To continue, press **No**. MODIFY PARAMETERS appears.
6. Do one of the following:
   - Press **Yes** and follow the prompts to modify the video conferencing parameters, store the changes, and reboot the phone.
   - To set the factory default settings, press **Default** and follow the prompts to set and store the factory defaults and reboot the phone.
7. To exit the current menu without a reboot:
   - To return to the main menu, press **Yes** at EXIT MENU?
   - To return to the default display, press **Superkey**.

Restoring Factory Default Settings

Tip: Restoring the factory default settings on the 5215 or 5220 IP Phone (Dual Mode) will erase the static network parameters.

1. Access the Configuration Menu (see page 171).
2. Press **No** until TOOLS AND FEATURES? appears.
3. Press **Yes** and then press **No** until RESTORE DEFAULTS? appears.
4. Press **Yes** and then follow the prompts to set and store the factory defaults and reboot the phone.
5. To exit the current menu without a reboot:
   - To return to the main menu, press **Yes** at EXIT MENU?
   - To return to the default display, press **Superkey**.

IEEE 802.1X Authentication for IP Phones

The 5215 Dual Mode, 5220 Dual Mode, and 5235 IP Phones support IEEE 802.1X Extensible Authentication Protocol (EAP) -Message Digest 5 (MD5) Challenge authentication protocol. Refer to the 3300 ICP Engineering Guidelines for more information about this protocol.

If the network switches and their ports support 802.1.x authorization, the Remote Authentication Dial-In User Service (RADIUS) server checks the username and password of the IP phones against the entries in the database:

- If the username and password of the IP phone match the username and password on the RADIUS server, the IP phone is granted access to the port services. The IP phone boots up.
- If the username and password don't match, the IP phone is denied port access. The IP phone does not boot up.
- If a username and password are not configured for the IP phone, you are prompted to enter them.

Configuring an Authentication Username and Password

1. Power up or reboot the 5215 Dual Mode, 5220 Dual Mode, or 5235 IP Phone.
2. Wait for the prompt: PORT ACCESS CONTROL
   PRESS # TO CONTINUE.

3. Press #.
4. Enter a username of up to 20 characters in length. This username must match a name that is programmed on the RADIUS server. Use the phone keys in the table below to enter the characters:

DTMF Key	Alphanumeric Characters (in order)
1	,&$!?%"'-_1
2	abc2
3	def3
4	ghi4
5	jkl5
6	mno6
7	pqrs7
8	tuv8
9	wxyz9
*	Backup and edit previous char
0	./:@0
#	Commit entered data

   By default, the user name and password are entered in upper case letters. However, you can use both upper and lower case. To change to lower case, press the Volume Down key while entering a letter. All subsequent letters will be in lower case. To return to upper case, press the Volume Up key while entering a letter.

5. Press # to commit the username.
6. Enter a password from 1 to 20 alphanumeric characters in length. This password must match the password that you have programmed on the RADIUS server for the user.
7. Press # to commit the password. The message, “Waiting for 802.1X authentication” appears in the phone display.
   After the server authenticates the username and password, the IP phone boots up.

Erasing an Authentication Username and Password

1. Access the configuration menu on the 5215 Dual Mode, 5220 Dual Mode, or 5235 IP Phone. See "Accessing the Configuration Menu" on page 171.
2. From NETWORK PARAMETERS? press **No** until on the telephone keypad until TOOLS AND FEATURES? appears.
3. Press **Yes**.
4. Press **No** until EDIT 8021X SETTINGS appears.
5. Press **Yes**. ERASE 8021X DATA? appears in the display.
6. Press **Yes** to erase the current username and password.
7. Press **Yes**. The phone erases the data from its flash and then reboots.

Tip: The IP phone usernames and passwords that you configured for EAP-MD5 Challenge Authentication do not need to be reprogrammed if power to the phone is lost.

Enabling or Disabling 802.1X Authentication

By default, EAP- MD5 Challenge Authentication Protocol is enabled on 5215 Dual Mode, 5220 Dual Mode, and 5235 IP Phones. If your network does not use this protocol, you do need to disable support for it on these phones.

1. Access the configuration menu. See "Accessing the Configuration Menu" on page 171.
2. From NETWORK PARAMETERS? press **No** until on the telephone keypad until TOOLS AND FEATURES? appears.
3. Press **Yes**.
4. Press **No** until EDIT 8021X SETTINGS appears.
5. Press **Yes**. ERASE 8021X DATA? appears in the display.
6. Press **No**. If currently enabled, you are prompted to disable 8021X. If currently disabled, you are prompted to enable 8021X.
7. Press **Yes**.
8. Press **Yes**. The phone erases the data from its flash and then reboots.

Before You Contact Technical Support

If you cannot find the source of the problem in this chapter, please collect the required information listed in the applicable section(s) **before** calling Mitel Technical Support (see “Technical Support” on page 11 for the number to call).

You also need the following information when calling Technical Support:

- ❒ Serial number(s) of your equipment and software.
- ❒ Nature of the problem.
- ❒ What you were doing when the problem occurred.
- ❒ Troubleshooting steps taken.
- ❒ Troubleshooting results.
- ❒ Your network diagram.
- ❒ DHCP server configuration and settings.
- ❒ Layer 2 switch configuration and settings.
- ❒ Whether the problem is between IP and IP, IP and remote IP, remote IP and TDM, etc.
- ❒ Alarm log details.
- ❒ NSU Maintenance log details (if applicable).
- ❒ IP Phone information (refer to the table).

Table 9: Collecting IP Phone Information

Question	Comment
Note: There are several new L2 maintenance commands that are useful for collecting details: l2_poe_satus; l2_stat_maclist; l2_stat_port; l2_stat_spanning_tree; l2_stat_sw	
Is there a PC attached to the IP Phone?	If yes, please have the Network Interface Card (NIC) settings of the PC ready. It is recommended that NO power saving options and NO flow control options be enabled.
Have there been broadcast storms?	Look for a broadcast storm in a Sniffer trace.
Is your cabling CAT 5 or better?	None.
Do your L2 or L3 switch statistics show any issues such as Runs, etc.?	Runs/Collision/Frame error may indicate an issue with NIC or a duplex mismatch.
	(Page 1 of 2)

Table 9: Collecting IP Phone Information (continued)

Question	Comment
What is the L2 port setting for IP phone and controller?	For IP phones, we recommend Trunk Port.
Does your L2 switch have CDP enabled, spanning tree enabled, or Port Fast enabled?	None.
What is your speed setting? (10/100, Full/Half, Auto, Fixed?)	None.
Do the symptoms improve if the IP phone is set to "auto and lock"?	For controllers, we recommend Access Port. Mitel recommends setting "Auto" on phones. In some unique PC/network, the IP phone may require to hard coding or setting to "auto and lock" mode.
Do you have the assert information from the debug menu?	Assert value is saved in the debug mode and reports the last reason that the phone rebooted.
What phone set are you using (5020, 5220, 5220 Dual Mode)?	None.
Is there a pattern? For example, does the problem follow the phone? Can you ping the IP phone?	None.
Have you noted any display information?	None.
Have you tried increasing keepAlives up to 1 minute via the System Administration tool registry entries?	None.
Do you have a complex network?	If yes, a network topology diagram is required.
Can you obtain a packet capture via Ethereal at the phone level?	Packet capture helps us to analyze the state of the network and the condition of the phone.
Can you obtain an IP Phone Analysis (IPA) for the phone in question?	IPA provides crucial information about how the phone is reacting
	(Page 2 of 2)

General Troubleshooting Steps

Follow the steps below if you can't find the problem when using the troubleshooting tables in this chapter.

1. Verify the status of the LEDs (see page 331 for more information).
2. In the System Administration Tool, review the **Alarm Details** form (**Maintenance and Diagnostics**). Identify and fix each alarm.
3. For IP Phone and physical network connectivity problems:
   - Verify that the device has power.
   - Verify the status of the port link integrity LEDs at each end of the cable.
   - Verify that each device transmits a link integrity pulse (LINK LED on).
   - If the link is down, try with another port.Verify that proper cabling is installed between the end devices.
   - Verify that a crossover cable was not installed instead of a straight-though cable, and vice-versa.
4. For network media problems:
   - If there is excessive noise, check for cabling problems.
   - If there are excessive collisions, check for duplex mismatch problems.
   - For Cyclic Redundancy Check (CRC): check if there is a faulty NIC card or flow-control.
   - If there are excessive runt frames, check for bad cables, duplex mismatches or bad PC NIC.
5. For network connectivity problems, identify the path between two end devices by doing the following PING test (in order):
   - Local
   - Local gateway
   - Remote gateway
   - Remote IP.

View Alarms

Alarms indicate the functional state of the system.

An alarm state can be viewed on either the front panel of the controller (see LEDs—Appendix D: Status LEDs on page 331) or on the attendant console.

Alarm Levels

- **No alarm:** The system is functioning properly.
- **Minor:** The system has detected a minor problem that may affect service.
- **Major:** The system has detected a problem that is causing a serious degradation of service.
- **Critical:** The system has detected a serious loss of call processing capability. System Fail Transfer is invoked by a Critical Alarm.

View Alarms

To view alarms, go to the **Alarms Details** form in the **Maintenance and Diagnostics** section of the System Administration Tool.

To view more information on an alarm, use the **show fault <alarm category>** maintenance command.

Alarm Categories are defined in the System Administration Tool online Help.

Troubleshoot Software

Embedded System Management (ESM)

Table 10: ESM Troubleshooting

Symptom	Probable Causes	Corrective Action
ESM Tool does not launch	Cookies are disabled in Internet Explorer.	Enable cookies (see Internet Explorer Online Help for more information).
	Proxy server is enabled on your PC.	Disable proxy server in Internet Explorer (Tools, Internet Options, Connection, LAN settings).

Installation and Upgrade

Table 11: Software Installation and Upgrade Troubleshooting

Error message on RTC shells	Probable Causes	Corrective Action
Fail to load file Fail to log in	IIS/PWS/FTP server is not running or not installed.	Go to your FTP site properties and re-start FTP services (see “Network Configuration Examples” on page 317 for information on Windows 2000 FTP site properties). *OR* Re-install your FTP server.
	The installation files are not in the home directories of the FTP server.	1. Check and identify the home directory of your FTP site properties (default is c:/inetpub/ftproot), and ensure that **boot_install**, **sysro.tar** is there. 2. If the files are not there, run the **setup.exe** again to ensure that all these files are copied to this home directory (not the 3300 directory).
		(Page 1 of 2)

Table 11: Software Installation and Upgrade Troubleshooting (continued)

Error message on RTC shells	Probable Causes	Corrective Action
	FTP user (3300) cannot log in FTP server (by default, the FTP user defined in Vxworks is **ftp** and the password is **ftp**).	1. Check the security tab of your FTP site and ensure that your FTP site allows "anonymous" connection. 2. Verify if there is an FTP username defined in your FTP server's user domain. If there is, ensure that the username and password are correct, OR delete the user from user domain in order to allow "anonymous" login. 3. Confirm that the FTP user name and password in Vxworks are **ftp** and **ftp**. You may change them to match those defined on your server's user domain (or vice versa). **Tip:** You may ftp from a computer into the FTP server and login as user defined in Vxworks to confirm ftp user can access FTP server
	No network connectivity between your FTP server and the 3300 controller	1. Ensure that your FTP server and the controller are on the same subnet. 2. If not, verify if the gateway IP addresses are defined, and that the router is able to route between two subnets. 3. If you changed the IP address on the FTP server, ensure that in "FTP site properties" you select the corresponding IP address on the FTP site tab. Typically, "unassigned". 4. Verify that the Host IP address in Vxworks is pointing to your FTP server, and **bootdevice** is set to **motfcc**. **Tips:** To avoid troubleshooting router related issue, you should connect your FTP server directly to the controller (FTP server and controller on the same subnet).
	The Firewall application on the FTP server is running.	Disable the Firewall application.

(Page 2 of 2)

Table 12: SysID or Password Error

Symptom	Probable Causes	Corrective Action
License and Option Selection error: “Password does not match the purchased options you selected”.	The System ID or i-Button has not been installed.	Install the SysID module or i-Button.

If you still can’t fix the problem, call Technical Support. Make sure you have the following information on hand before calling:

- ❒ The controller’s VxWorks parameters (bootdevice, host file, inet on ethernet, host IP address).
- ❒ The FTP site properties (home directory, IP address of FTP site, user defined in user domain).
- ❒ The error message(s) in the RTC shell.

Downgrading to a Previous Software Release

If it becomes necessary to downgrade the system software:

- ensure that you have an off-board database backup that was created in the software version that you are going back to
- use the “Installing System Software Manually” procedure on page 77.

WARNING: YOU MAY NOT DOWNGRADE THE LX CONTROLLER TO A SOFTWARE VERSION PRIOR TO RELEASE 5.0. A DOWNGRADE WOULD RENDER THE CONTROLLER INOPERABLE.

Backup and Restore

Table 13: Software Backup and Restore Troubleshooting

Symptom	Probable Causes	Corrective Action
Backup/restore failure (only fail to FTP files between PC). **Note:** If Java Plug-in console view is enabled, you should see the security warning.	Java version is not correct. *OR* higher version of Java is installed.	1. Verify that the correct version of Java is installed (see "Install the Java Plug-In" on page 93). 2. If another version is installed, remove it, re-install the correct version, and reboot the PC.
	Backup/restore applet is not trusted (identitydb.obj not on PC).	1. Go to the Backup or Restore form in System Administration Tool (Maintenance and Diagnostics). 2. Click the link to download the **identitydb.obj** file to the Maintenance PC. Save the file in: For Windows NT: WINNT/Profile/ <username>. For Windows 2000: Documents and Settings/<username>
	Backup/restore applet is not trusted (identitydb.obj not in right directory.	Verify the file is in the correct <username> profile (the profile used to log onto the PC).
	Backup/restore applet is not trusted (identitydb.obj has wrong extension).	Verify that the extension of the file is **.obj** (not .obj.obj, or .obj.txt, or anything else). **Tip:** Disable the Hide file extensions for known file types option to see the complete extension of the file. In the folder window, select: For Windows NT: View/Options/View. For Windows 2000: Tools/Folder Options/View.

(Page 1 of 2)

Table 13: Software Backup and Restore Troubleshooting (continued)

Symptom	Probable Causes	Corrective Action
Backup procedure repeats on its own	Internet Explorer timeout	Execute timeout.reg or timeout_4.reg from software CD/ Product_Support/Registry. (See README_for_timeout_reg_files.doc in Product_Support/Registry)
Database backup, with voice mail messages included, fails	Lack of free space in the db partition	Determine the amount of free space in the db partition and if there is enough space for voice mail messages. You can see the free space and required space by entering commands in the RTC window: • dosFsShow "/vmail" • debugVolInfo = 1 • debugVolInfo = 0 Refer to Troubleshooting Guide 04-2806-00011 for detailed instructions.
		(Page 2 of 2)

If you still can't fix the problem, call Technical Support. Make sure you have the following information on hand before calling:

- ❒ Java plug-in version
- ❒ Maintenance PC username
- ❒ Maintenance PC IP address
- ❒ Location of identitydb.obj file on the Maintenance PC
- ❒ Logs from the Maintenance Port (RTC Shell).

Audio File Downloads

Table 14: Audio File Downloads Troubleshooting

Symptom	Probable Causes	Corrective Action
Audio File cannot be located	Corrupted file	Verify that the audio file is not corrupted.
Audio File is rejected	Incorrect audio file specifications	Verify that the audio file meets the required specifications (see System Audio File Updates form in the System Administration Tool).
System Greeting is in the wrong language	Incorrect language file downloaded	Download a file in the correct language using the System Audio File Updated form or Enterprise Manager.
System error log is generated	Downloading file when system is unavailable	Verify that you are not downloading a file during a backup, restore or upgrade, or while someone is recording the same greeting from a telephone.

Troubleshoot Hardware

Alarms

Table 15: Alarm Troubleshooting

Alarm	Probable Cause	Corrective Action
E2T ICP Com	E2T card has no IP address.	**If you are using the controller's internal DHCP server for the E2T**: ensure you assigned a static IP address to the E2T using the correct MAC address (see Step 3 in page 29). **If you are using an external DHCP server for the system:** verify that options are programmed correctly (see page 307).
	DHCP is corrupted.	Rebuild the DHCP scope.
	Incorrectly programmed E2T IP address or setup using a debug cable.	Verify that E2T VxWorks parameters are correct (see "Controller Configuration Settings (RTC)" on page 300). (No debug cable on MXe).
DSP Status	Compression channels or 30 voice mail ports programmed but DSP module not installed (voice mail DSP requirement does not apply to LX or 700-user controller).	Use the **Show Status Dsp** maintenance command to identify status of DSPs in the controller. Install required DSP module(s) ("DSP Module" on page 105).
	DSP module(s) for compression installed, but license not enabled.	Enable compression license in System Administration Tool in the License and Option Selection form.

(Page 1 of 2)

Table 15: Alarm Troubleshooting (continued)

Alarm	Probable Cause	Corrective Action
DSP Card Status	DSP card is defective.	For a defective DSP module, ensure that the module is seated securely. For an embedded DSP failure, replace the controller. Use **Show Status Dsp to identify the location of the defective module.**
Fan	Fan is defective (MXe).	Replace the fan (see page 139). See note.
One PSU	Power supply unit is defective (MXe).	Replace the PSU (see page 139). See note.
Two PSU	Power supply unit is defective (MXe).	Replace the PSU (see page 139). See note.
RAID Hard Disk	Hard disk has a fault (MXe).	Replace the hard disk (see page 128). See note.
Note: Enter the **Show Status Redundant** maintenance command to identified the failed component. A minor Fan, Power Supply, or RAID alarm in the MXe means that only one of the components has failed. A major alarm means that both have failed.		
(Page 2 of 2)		

Embedded T1/E1 (PRI, T1/D4, or MSDN/DPNSS)

Table 16: Embedded PRI Troubleshooting

Symptoms	Probable Cause	Corrective Action
Embedded PRI calls fail and all Status LEDs on the Dual T1/E1 Framer are dark	Configuration	Verify that embedded PRI is programmed properly in the following forms (see also Program Embedded PRI/Q.SIG in the Online Help): • Controller Module Configuration • Dual T1/E1 Framer Configuration • Link Descriptor Assignment • Digital Link Assignment After the Digital Link Assignment form is completed, the T1/E1 Framer status LEDs should come on. This takes about 15 seconds.
Embedded PRI Links are “not seizable”, Status LEDs show RED alarm	Configuration or Wiring	Ensure that the ISDN cable is plugged into the correct RJ-45 port on the Dual T1/E1 MMC. Verify that the ISDN cable is correctly wired. Change the “Termination Mode” setting in the Link Descriptor Assignment form - either LT or NT. This change takes about 30 seconds to take effect.
Embedded PRI links are “not seizable”, Status LEDs show flashing GREEN	Configuration	Verify the “Network Side/QSIG Master” setting in the Protocol Assignment form. Check the “Inverted D-Channel” setting in the Link Descriptor Assignment form - normally it is set to “No”. Each of these changes takes approximately 30 seconds.
Embedded DPNSS links are “not seizable”, Green LED is ON	Configuration	Ensure that the “Address for Message Control” field in the Link Descriptor Assignment form is set appropriately (“A” or “B” depending on the far end. If the configuration is correct, wait for about one minute until every circuit has finished negotiation with the far end.

(Page 1 of 2)

Table 16: Embedded PRI Troubleshooting (continued)

Symptoms	Probable Cause	Corrective Action
Distorted voice or loud noise over PRI/QSIG call	Voice Encoding is not set properly	In the Link Descriptor Assignment for the PRI/QSIG trunk, set the "Voice Encoding" to Nil for T1 on NA or E1 on Euro controller. Note: You cannot use the same Voice Encoding settings as a PRI NSU.
High number of slips	Configuration of Network Synchronization form	Ensure that the synchronization source being selected is to a digital PSTN trunk (like PRI or T1/D4)
Outgoing calls fail with reorder tone	Configuration of ARS or Protocol Assignment	Enter the CCS TRACE maintenance command to ensure that the proper digits are being sent out. Check the Digit Modification with the Per-Call programming for PRI to make sure digits are not being inserted or absorbed unnecessarily. Ensure that the "Protocol" field in the Protocol Assignment form is correct for the PSTN link (not for DPNSS).
Incoming calls fail	Configuration of Trunk forms	Verify in the Trunk Service Assignment form that there is an Answer Point set up for non-DID trunks for Day and Night services. For dial-in trunks, verify that the "Dial in Trunks Incoming Digit Modification - Absorb" field is set to 0 and that the "Dial In Trunks - Incoming Digit Modification - Insert" field is set appropriately for dial in trunks.

(Page 2 of 2)

Embedded BRI

Table 17: Embedded BRI Troubleshooting

Symptoms	Probable Cause	Corrective Action
Embedded BRI calls fail and all Status LEDs on the Quad BRI Framer are dark	Configuration	Verify embedded BRI is programmed properly in the following forms (see also Program Embedded BRI in the online Help): • Controller Module Configuration • Quad BRI Framer Configuration • Link Descriptor Assignment • Digital Link Assignment • Protocol Assignment After the Digital Link Assignment form is completed, the red Quad BRI Framer status LED should come on. This takes about 15 seconds.
Embedded BRI Links are “not seizable”, Status LEDs show RED alarm	Configuration or Wiring	Ensure that the ISDN cable is plugged into the correct RJ-45 port on the Quad BRI MMC. Verify that the ISDN cable is correctly wired (straight through for trunk interface, crossover for terminal). Note that 3-4 and 5-6 are the relevant pins for the cable. Toggle the “Bus Type” setting in the Protocol Assignment (either S or T). This change takes about 30 seconds to take effect. Ensure that the Manual TEI value is correct (if required).
High number of slips	Configuration of Network Synchronization form.	Ensure that the synchronization source being selected is not connected to a BRI terminal. If there is a digital E1 trunk, that should be used as the first synchronization choice.

(Page 1 of 2)

Table 17: Embedded BRI Troubleshooting (continued)

Symptoms	Probable Cause	Corrective Action
Outgoing calls fail with reorder tone	Configuration of ARS or configuration of Per Call Capabilities	Enter the CCS TRACE maintenance command to ensure that the proper digits are being sent out. Check the Digit Modification with the Per-Call programming for BRI to make sure digits are not being inserted or absorbed unnecessarily.
Incoming calls fail	Configuration of Trunk forms	Verify in the Trunk Service Assignment form that there is an Answer Point set up for non-DDI trunks for Day and Night services. For dial-in trunks, verify that the "Dial-in Trunks Incoming Digit Modification - Absorb" field is not left blank and that the "Dial In Trunks - Incoming Digit Modification - Insert" field is set appropriately for dial-in trunks.

(Page 2 of 2)

Network Services Units (NSUs)

Table 18: NSU Troubleshooting

Symptoms	Probable Cause	Corrective Action
NSU fails to come up after upgrade or new installation (Both the red and amber LEDs, or just the amber LED, are marching between L0/L1)	Automatic NSU upgrade is in progress	Wait 15–20 minutes for the NSU upgrade to complete. **CAUTION: Do not power down when the amber LED is marching between L0/L1. Powering down the NSU may corrupt the NSU software.**
NSU keeps resetting with **no IMAT db** error message	No IMAT database is saved to the NSU (PRI/QSIG).	Use IMAT to save the corresponding database to NSU (PRI/QSIG).

(Page 1 of 3)

Table 18: NSU Troubleshooting (continued)

Symptoms	Probable Cause	Corrective Action
Changing NSU from T1 to E1, NSU remains unassigned	NSU does not reflash	• Flash the NSU (refer to Technical Bulletin 58004932) *OR* • Delete datetag.txt via ftp *OR* • From the debug terminal, issue force dl for the NSU.
The LEDs are marching green and amber for more than 30 minutes during an NSU upgrade	Corrupted NSU software.	Refer to Technical Bulletin 58004932 for information on flashing the NSU.
NSU fails to boot, with an error message. Boot line timeout	No fiber connection between the controller and NSU.	Fix the fiber connection, and ensure that the LEDs of both FIMs are solid green.
	Universal NSU programming is not complete.	1. Ensure that the NSU is programmed as a Universal T1 or E1 (not T1 or CEPT). 2. Program the proper link descriptor with the proper integrated access, and assign to the corresponding NSU unit (for example: ISDN node for PRI protocol, T1D4 for T1D4, DPNSS for MSDN). 3. Program at least one trunk.
PRI/QSIG NSU fails to boot	Database not compatible with new load.	1. Connect IMAT to the PRI NSU and start IMAT. 2. Download the database from the NSU to IMAT. 3. Save the database from IMAT to the NSU. 4. A message appears asking if you want to convert the database. Select **Yes**. 5. When the database has finished saving, reset the NSU.

(Page 2 of 3)

Table 18: NSU Troubleshooting (continued)

Symptoms	Probable Cause	Corrective Action
FTP into the NSU fails.	Release 4.1 and later requires a username and password to login	Enter: username, **mitel** password, **passwd1**
NSU is up, but L0 or L1 LED is solid red	No physical connection to far end.	1. Verify and fix wiring. 2. Check DIP Switch 6. If it is UP, set it to DOWN to see if this makes any difference (see Table 53 on page 268).
NSU is up, but L0/L1 LED is flashing green	Layer 2 is not up. Layer 2 protocol mismatch.	1. Check your IMAT database and verify with your Telco which protocol you should use. 2. Check the DSU wiring.
Distorted voice or loud noise on NSU	Voice Encoding is not set properly.	Change Voice encoding in the link descriptor to **invert** for **T1**, and **ADI invert** for **CEPT** (this does not apply to Embedded PRI).
		(Page 3 of 3)

If you still can't fix the problem, contact Technical Support. Make sure you have the following information on hand before calling:

- ❒ Error message from NSU Maintenance port.
- ❒ Boot sequence from NSU Maintenance port.
- ❒ Symptom appears in Troubleshooting table?
- ❒ PRI: can access IMAT database?

Analog Services Units (ASUs)

- Verify the status of the LEDs (see "Analog Services Unit LEDs" on page 351).
- Verify that the IP addresses reserved for the ASUs are not used elsewhere on the system (see "Analog Services Unit" on page 38).

In-Line Power

Use this section to troubleshoot problems with in-line powering of IP devices.

1. Verify the following:
   - Ensure power is applied to the power unit.
   - Ensure you are not using crossover Ethernet cables.
   - Ensure that the input Ethernet cable is connected to the **Data In** port of the power unit.
   - Ensure that the output Ethernet cable is connected to the **Data and Power Out** port of the power unit.
   - Ensure that the input and output cables of a port pair are used for the same IP Phone.
2. Go through Table 19 below.
3. If you cannot solve the problem using Table 19, go through the steps in “General Troubleshooting Steps” on page 181.
4. If you still can’t find the problem, call Mitel Technical Support (see “Before You Contact Technical Support” on page 179).

Tip: Running the power unit with an Power Inactive LED ON will not damage the Power Unit (the port power is disconnected, and a low power pulse checks the line status every 5 seconds).

Table 19: In-Line Power Troubleshooting

Symptoms	Probable cause	Corrective Action
Power unit is plugged in, but does not power up.	No power at outlet. *OR* faulty power outlet. *OR* faulty power cord.	1. Plug a known functioning device in the power outlet. 2. Verify that the power outlet protection circuit has not tripped. 3. Verify that the voltage of the power outlet is within specifications. 4. Verify that the Power Unit power cord works correctly (including good and solid ground connection).
		(Page 1 of 4)

Table 19: In-Line Power Troubleshooting (continued)

Symptoms	Probable cause	Corrective Action
Power unit is functioning, but fans do not work.	Blocked fan opening *OR* faulty internal power supply.	Verify that all the fan openings are clear of any blocking material.
Power unit is functioning, but AC LED is OFF.	Internal circuitry fault *OR* internal power supply failure.	1. If the fans are working, there is probably an internal circuit fault. 2. If the fans are not working, there is probably an internal power supply failure.
Power unit powered up, but Alarm LED still ON.	Power on self-test (POST) not completed *OR* internal fault.	1. Verify if POST sequence is as listed or not. 2. If the Alarm LED stays ON after the POST sequence, there is an internal fault.
IP device does not work, and both Port Status LEDs are OFF (Power unit is not detecting IP device).	Wiring problem OR faulty IP device OR faulty Power Unit.	1. Verify you are using a standard UTP Category 5, 6 or 6e cable (with 8 wires–4 pairs). 2. Verify that you are not using a crossover cable. 3. Verify that the connections for the port pair both correspond to the same IP device, and that the port connections are not reversed. 4. Verify that the cables connected to the Data In and Data Out ports correspond to the same IP device. 5. Connect the IP device to a different port pair on the Power Unit. If the device works normally, the original port is probably faulty. 6. Connect the IP device directly to the Power Unit using a short cable. If the device works normally, the original cable (or one of its connectors) is faulty. 7. If possible, connect the IP device to a different Power Unit. If the device works normally, the original Power Unit is probably faulty.

(Page 2 of 4)

Table 19: In-Line Power Troubleshooting (continued)

Symptoms	Probable cause	Corrective Action
IP device works, but there is no data link.	Wiring problem *OR* Faulty IP device *OR* Faulty Power Unit. *OR* Missing/faulty local power adapter.	1. Verify that the port's Power Active LED is continuously ON. 2. Verify that the connections for the port pair both correspond to the same IP device, and that the port connections are not reversed. 3. The IP device may require a local power adapter to operate. If an adapter is already in use, replace it with a known working adapter. If this works, replace the faulty adapter. 4. Verify you are using a standard UTP Category 5, 6 or 6e cable (with 8 wires–4 pairs). 5. Verify that the cable length between the Power Unit and the IP device does not exceed 100 metres. 6. Verify that you are not using any crossover cables. 7. Verify that the Power Unit is connected to a switch/hub with a good RJ-45 patch cord connection. 8. Connect the IP device directly to the Power Unit using a short cable. If the device works normally, the original cable (or one of its connectors) is faulty. 9. Try to connect a known working IP device to the same port (test device). If the test device works and the link is established, there is probably a faulty data link in the original IP device. 10. Connect the IP device to a different port pair. If the device works, one of the original ports is probably faulty, or there is a bad RJ-45 connection.
		(Page 3 of 4)

Table 19: In-Line Power Troubleshooting (continued)

Symptoms	Probable cause	Corrective Action
IP device not operating, with Power Inactive LED ON.	Discharged capacitor in IP device *OR* wiring problem *OR* missing/Faulty local power adapter *OR* faulty port.	1. Wait 5 to 10 seconds. If the Power Active LED turns ON, there was a discharged capacitor in the IP device. 2. Verify that you are not using any crossover cables. 3. The IP device may require a local power adapter to operate. If an adapter is already in use, replace it with a known working adapter. If this works, replace the faulty adapter. 4. Connect the IP device directly to the Power Unit using a short cable. If the device works normally, the original cable (or one of its connectors) is faulty. 5. Connect the IP device to a different port pair. If the device works, one of the original ports is probably faulty, or there is a bad RJ-45 connection. 6. Unplug the IP device, and verify that the Power Inactive LED turns OFF. If it does not, the port is probably faulty, or the RJ-45 socket is shorted.
IP device powered correctly, but Power Active LED is OFF.		Re-connect the IP device to a different port pair. If the new port pair Active Power LED turns ON, there is a fault in the original output port (probably a faulty LED).
IP device does not work, but Green Port Status LED ON.	Wrong connection *OR* faulty IP device.	1. Verify that the IP device is actually connected to that port. 2. Replace the device by a known working IP device (test device). If the test device powers up, the original IP device is probably faulty.

(Page 4 of 4)

Power Over Ethernet

The CXi controller's Layer 2 switch can provide 120 Watts of power to 802.3af-compliant devices according to the following general rules:

- Up to 16 IP Phones are supported
- Up to four PKMs (PKM12 or PKM48) are supported on Dual Mode IP phones. Only one PKM can be attached to a set. Multiple PKMs on a set require an AC adapter.
- Conference units require an AC adapter.
- Port 1 has the highest priority, port 16 the lowest. If the power budget is exceeded, power will be turned off to the ports, starting with port 16 and ending with port 1, until less than 120 Watts is being consumed.

Tip: Refer to Table 134 on page 377 for a list of all Mitel IP Phones and their power consumption.

Digital Service Units (DSU)

Tip: The CX and CXi controllers do not support Digital Service Units.

BRI Card Alarms and Call Logs

To query alarms or call logs:

1. Log into the BRI maintenance terminal.
2. Enter the **Configuration** menu item number.
3. Enter the **Debug** menu item number.
4. Enter the **Alarms and Call Log** menu item number.
5. Do one of the following:
   - To query the alarms, enter the **Query Alarms** menu item number.
   - To query the call logs, enter the **Query Call Logs** menu item number.

To clear and reset the call log:

1. Log into the BRI maintenance terminal.
2. Enter the **Configuration** menu item number.
3. Enter the **Debug** menu item number.

4. Enter the **Alarms and Call Log** menu item number.
5. Enter the **Restart Call Log** menu item number. The following message appears: ARE YOU SURE? (Y or N)
6. Enter **Y**.

To query the status of the BRI channels:

1. Log into the BRI maintenance terminal.
2. Enter the **Configuration** menu item number.
3. Enter the **Debug** menu item number.
4. Enter the **Alarms and Call Log** menu item number.
5. To query the BRI status, enter **5**.

To query BRI or PRI port statistics or the management link status:

1. Log into the BRI maintenance terminal.
2. Enter the **Configuration** menu item number.
3. Enter the **Debug** menu item number.
4. Enter the **Alarms and Call Log** menu item number.
5. Do one of the following:
   - To query the BRI port statistics, enter **7**, and then enter <port number>.
   - To query the PRI port statistics, enter **8**.
   - To query the management link status, enter **9**.

Troubleshoot Digital Trunks

Digital Trunking

The following table lists key maintenance commands that you can use to collect Digital Trunk INFOrmation.

Table 20: Digital Trunk Troubleshooting

Symptoms	DTINFO Command Qualifiers	Description
Any problem	show link config all show framer config all show link info show vdsu table	Displays link, framer, and vdsu configuration information.
Link alarms - Part 1 (trunks unavailable, network synch issues)	show framer stats all show framer regs all	Displays framer statistics and its register settings. Collect output from the "dtstats read", "net state" and "show faults digital links".
Link alarms - Part 2 (Trunks not in idle when there are no calls up)	show vdsu alarms <plid> show vdsu channel <plid>	Displays the state of vdsu alarms and channels. Use this command with "dtstats read" and "state" commands.
Outgoing or incoming calls rejected	trace vdsu namnum	Displays the calling/called number and name of the call. It also displays the reason an ISDN call was disconnected. Use this command to verify that ARS is setup correctly.
Call problems (calls dropped/ rejected, set displays not correct, and so forth)	trace tsp l2l3 <plid> OR trace tsp cc <plid> OR trace vdsu cp <plid> trace vdsu vb <plid>	Displays L2 or L3 or call control trace. If the problem is not protocol related, turn on the "cp/vb" tracing.
Call problems are generating message output that you need to capture	enable logtofile disable logtofile	Saves logging traces to a file named "DigTrkTrace.rtf" in the "/db" directory.

Troubleshoot the Network

IP Trunking

Tip: To rule out DHCP problems, and isolate network-related issues, we recommend that you program the IP Phone with a static IP Address (see "Setting Static IP Address on IP Display Set" on page 54).

Table 21: IP Trunk Troubleshooting

Symptoms	Probable cause	Corrective Action
IP trunk does not recover after router crash	ICMP redirect is enabled.	1. On the RTC shell, use **routeShow** to identify the addition RouteHost entries, then use **routeDelete** to remove the entry. 2. For a permanent solution: • Make sure that the route has a "permanent" static route to the remote IP trunk network. • Turn IP redirect off. • Turn on the routing protocol between local router and ISP router.

LAN

Table 22: LAN Troubleshooting

Symptoms	Probable cause	Corrective Action
Device fails to transmit data.	Packet collision.	Refer to "Troubleshooting Using L2 Statistics" in the System Administration Tool OnLine Help.
Data packet is altered between transmit and receive.	CRC/FCS and alignment errors	
Receiving device counts an error.	Frame length errors.	

If you still can't find the problem, call Mitel Technical Support (see "Before You Contact Technical Support" on page 179). Make sure you have the following information on hand before calling:

- ❒ network diagram
- ❒ routeShow result
- ❒ PING test result between controller and IP Phone
- ❒ rmess verify result
- ❒ State xnet all result

Tip: There are several new L2 maintenance commands that are useful for collecting details: l2_poe_satus; l2_stat_maclist; l2_stat_port; l2_stat_spanning_tree; l2_stat_sw.

E2T

Table 23: LX E2T Troubleshooting

Symptoms	Probable cause	Corrective Action
E2T fails to initialize	Changing from a hard coded E2T IP address to requesting one from the DHCP server. (If **any** IP addresses remain on the E2T (at "inet on ethernet", "host inet", or "gateway inet"), the E2T will use them and will obtain the rest of its parameters from the DHCP server.)	This change is made by changing the **flags (f)** parameter in the bootline of the E2T from **0x0** (hardcode) to **0x40** (DHCP). When changing the flag from 0x0 to 0x40 on the E2T, make sure that you blank out ALL IP addresses in the bootline of E2T.

Table 24: MXe E2T Troubleshooting

Symptoms	Probable cause	Corrective Action
E2T fails to initialize	Changing from a hard coded E2T IP address to requesting one from the DHCP server. (If **any** IP addresses remain on the E2T (at "inet on ethernet", "host inet", or "gateway inet"), the E2T will use them and will obtain the rest of its parameters from the DHCP server.)	1. Secure telnet to <RTC IP Address> port 2007 (this is the E2T serial port on the MXe) 2. Secure telnet to <RTC IP Address> port 2002 (VxWorks shell on the RTC) 3. At the VxWorks shell on the RTC type: "ToggleCpu 1" to reset the E2T card 4. Watch the port 2007 (E2T) telnet session. 5. Hit 3 spaces to interrupt the boot process. 6. Verify the bootline parameters as described in Table 23, "LX E2T Troubleshooting," on page 206.

CXi-specific Issues

Table 25: CXi Troubleshooting

Symptoms	Probable cause	Corrective Action
Unable to connect to the controller	Database being used is from a system that had dual-VLANs enabled, so the management PC, untagged on VLAN 1, cannot reach the controller on the Voice VLAN.	Run **vlan_off** command from the RTC console (through the RS-232 serial port) to reset the controller and disable the VLANs. Run **vlan_on** to enable the VLANs. The commands will cause the controller to reboot, so wait a couple minutes before trying to connect with your PC, attached to CX port 17.
IP Phones on third-party Layer 2 switch cannot connect with the CXi	System has VLAN enabled but the “tagging” is being removed prior to connecting with Port 17.	The CXi must receive VLAN tags (if VLAN enabled) to allow an IP phone to connect with the CXi. The third-party L2 switch needs to pass the Q and P tags to Port 17.
Unable to connect to the DSL modem	Bad connection, incorrect password, incorrect username, or wrong protocol.	Review Maintenance Logs for: Wan_port: state=down, proto=pppoe, cause=wan=start. Review ISP information sheet and make sure that the username, pw and protocol are correct. Disable and Enable the WAN Access in Internet Gateway/Wan Settings.
CXi ports 1 - 16 not functioning.	Layer2 port IP Address is not programmed.	Ensure IP Network Configuration is properly programmed.

(Page 1 of 3)

Table 25: CXi Troubleshooting (continued)

Symptoms	Probable cause	Corrective Action
Connection failures: ISP, IP trunks, IP phones.	Network configuration programming problem.	Verify programming in the following forms: **1.** System IP Configuration The address cannot conflict with the L2 Switch IP Address, and it must be on a different subnet than the WAN Ethernet IP Address. **2.** Layer 2 Switch form To program global settings and configure the Ethernet ports for the Layer 2 switch. **3.** IP Routing form Lists routes to destination networks on the LAN. **4.** WAN Settings form To enable the WAN interface and provide internet connectivity settings for Static IP, DHCP, or PPPoE. **5.** Remote Access (PPTP) **6.** Firewall Control **7.** Port Forward Table
No routing IP traffic correctly	Default Gateway should be third-party router (if one is installed), otherwise L2 IP Address should equal Gateway.	IP Routing form indicates a network list. All subnets referenced on this network list will follow the default gateway, otherwise the route will be directed to the WAN port (ensure that it is enabled).

(Page 2 of 3)

Table 25: CXi Troubleshooting (continued)

Symptoms	Probable cause	Corrective Action
No power on CXi ports 1 - 16	Device is pulling too much power; power is disabled in programming; 120 Watt budget has been exceeded.	Refer to Engineering Guidelines, Mitel IP Phone Power. When power budget is exceeded ports will shut down from port 16 to port 1. Run the **L2 Poestatus** maintenance command. Check Layer 2 Switch programming. Check device for fault.
Connection failures: IP trunks	IP trunks cannot work through the WAN port.	Install a third-party router (default gateway) and disable the WAN port OR, install a third-party router (default gateway), change Network list to include routes that will follow default gateway and enable WAN port. **Note**: IP trunk will follow default gateway (3rd party router).
		(Page 3 of 3)

PC Network Connectivity

Table 26: E2T Troubleshooting

Symptoms	Probable cause	Corrective Action
Loss of PC network connectivity via IP phone	IP phone lost power. IP phone reset via the debug menu. IP phone lost connectivity ~ 10 minutes; then will execute hard reset and DHCP discovery.	Connection will be automatically restored in 1 - 2 seconds.

IP Phone Registration

1. Record the error message on the IP Phone display, then go through Table 27 below.

Tip: To rule out DHCP problems, and isolate network-related issues, we recommend that you program the IP Phone with a static IP Address (see "Setting Static IP Address on IP Display Set" on page 54).

Note: IP sets require a firmware upgrade to support the new DHCP options introduced in Release 7.0; otherwise, the sets will fail to boot. Such failures can occur, for example, in a resilient cluster of mixed software releases or when sets with old firmware are added to a controller after it was upgraded to Release 7.0. For the sets to boot, DHCP options 128-133 must be present in the DHCP server. After the sets have booted, options 128-133 may be removed to avoid future conflicts with standardized or other vendors' use of these options.

2. If you still can't fix the problem, call Mitel Technical Support.

Tip: Use the debug option on display IP phones to view Version, Network, Telephony/DSP, Connection Browser Config, and memory Stats details (see page 170).

Make sure you have the following information on hand before calling:

- ❒ Is the problem with the local or remote subnet?
- ❒ DHCP server(s) settings
- ❒ Layer 2 switch configuration and settings
- ❒ Router configuration and settings
- ❒ Network Diagram
- ❒ IP addressing scheme
- ❒ VLAN configuration and settings

Table 27: IP Phone Registration Troubleshooting

Error Message on Display	Probable Cause	Corrective Action
Invalid VLAN ID	DHCP Option 43 or 125 on Release 7.0 or later systems or 132 and/or 133 for earlier releases not set correctly.	1. Identify the location of DHCP server and which DHCP server is assigned the IP address for the corresponding subnet (see page 317 for examples). 2. For an external Microsoft DHCP server (NT server, etc.), make sure that the option type is set to LONG. **Note:** For Windows 2000, refer to page 308. 3. For a Cisco® Router DHCP server, make sure that the option type is set to hex, and padded with 0s (for example, 0x00000002 for VLAN 2). 4. For the controller internal DHCP server, set the option type to numeric.
Duplicated IP address	Existing data device owns the IP address.	1. Check the IP address on the phone display. 2. Disconnect the IP Phone. 3. From a PC on the same subnet, ping the suspected IP Phone. If there is a response, identify the data device, and resolve the conflict.
	Corrupted DHCP server	1. On the suspected DHCP server, disable then recreate the scope. 2. If this is a Microsoft DHCP server, reboot the server.
DHCP discovery *OR* DHCP OFFER X REJ	DHCP option 43 or 125 on Release 7.0 or later systems or option 130 (MITEL IP PHONE) for earlier Releases is not programmed.	Identify the location of DHCP server and set to Option 130 as String type with value of “MITEL IP PHONE”.
	DHCP server does not have enough IP addresses.	Create a larger scope with more IP addresses on the DHCP server.

(Page 1 of 6)

Table 27: IP Phone Registration Troubleshooting (continued)

Error Message on Display	Probable Cause	Corrective Action
(Cont'd)	DHCP server cannot assign IP addresses for the corresponding subnet, even though there are enough IP addresses.	1. For a Microsoft DHCP server, reboot the server. 2. For the controller internal DHCP server, disable DHCP and rebuild the scope.
	L2 switch port is shut down or not configured properly.	1. Check the L2 switch, and ensure that the port is not shut down. 2. Ensure that this port can access the DHCP server subnet (that is, access the port for the same VLAN, etc.).
DHCP Discovery *OR* DHCP OFFER X REJ (VLAN) (after releasing the first IP from the native DHCP server)	DHCP Option 43 or 125 on Release 7.0 or later systems or Option 30 (MITEL IP PHONE) for earlier Releases is not program-med on the second scope of the DHCP server (or on the second DHCP server) *OR* VLAN ID is not assigned properly	1. Identify if there is one DHCP server for both VLANs, or if there is one DHCP server per VLAN (see "Network Configuration Examples" on page 317). 2. For one DHCP server for both VLANs, ensure that option 43 or 125 is properly configured (Release 7.0 and later) or that option 130 is programmed as String type with value of "MITEL IP PHONE " (prior to Release 7.0), in the scope of Voice LAN. 3. For one DHCP server per VLAN, ensure that option 43 or 125 (Release 7.0 and later) or 130 (prior to Release 7.0) is defined. 4. Verify that the proper VLAN ID is assigned in option 43 or 125 (Release 7.0 and later), or 132 (prior to Release 7.0).
	One DHCP server for two VLANs network configuration: IP helper address on the router interface is not set up correctly.	1. On the router interface (on which DHCP is not residing), enter the IP helper address and specify the IP address of the DHCP server on the other side of the subnet (that is, always set up IP helper address on the DHCP server client side). 2. Ensure the second scope is created for the corresponding VLAN (see "Network Configuration Examples" on page 317 for more information).

(Page 2 of 6)

Table 27: IP Phone Registration Troubleshooting (continued)

Error Message on Display	Probable Cause	Corrective Action
(Cont'd)	The L2 switch port for the phone interface is shut down or not configured properly	1. Check the L2 switch and ensure that the port is not shut down. 2. For a Cisco L2 switch, ensure that this is a trunk port with Dot1q encapsulation, and that this trunk port allows both native and Voice LAN to pass through. 3. For an HP L2 switch, ensure that Native Lan is untagged, and that Voice LAN is tagged (see "Network Configuration Examples" on page 317). 4. Verify whether there are two physical interfaces to the router (one per VLAN), or a router on a stick configuration (one physical with virtual sub-interfaces). 5. Ensure that the port(s) on both sides (L2 switch and router) are not shut down ("Network Configuration Examples" on page 317). 6. If there is a physical interface on the router for each VLAN, make sure that the L2 switch is set to correctly access port for the corresponding VLAN/ subnet (see "Network Configuration Examples" on page 317). 7. If there is one physical interface on the router for multiple VLANs, ensure that this is a trunk port on the L2 switch, and ensure that this trunk port allows both native and voice LAN to pass through. 8. On the router subinterface, ensure that the proper VLAN is associated to the remote subinterface (see "Network Configuration Examples" on page 317).

(Page 3 of 6)

Table 27: IP Phone Registration Troubleshooting (continued)

Error Message on Display	Probable Cause	Corrective Action
TFTP load failure	DHCP option 43 or 125 on Release 7.0 or later systems or option 128 for earlier Releases is not set up to point to the right TFTP server (Controller).	Check the DHCP server, and confirm that option 43, 125, or 128 is pointing to the right TFTP server (usually, the controller RTC IP address).
	No network connectivity between the controller and the phone.	1. Confirm that the controller is connected to the network. 2. For a Cisco L2 switch: verify that the L2 switch is access port (Voice LAN). 3. For an HP L2 switch: verify that the L2 switch is untagged (Voice LAN). 4. If the router is involved, make sure that the router's MTU is set to 600 or more.
	Firmware on controller is missing or corrupted.	1. Verify that the firmware (**ipp510bootenc.bin**, etc.) is in the **sysro/tftp** directory (particularly if the user has manually copied the firmware). 2. Confirm if TFTP on the controller is corrupted (this can be verified by connecting the IP Phone directly on the controller, or by observing the behavior of other IP Phones). **Tips:** If you have Option 132/133 programmed on the controller's internal DHCP server, disable them before trying Step 2.

(Page 4 of 6)

Table 27: IP Phone Registration Troubleshooting (continued)

Error Message on Display	Probable Cause	Corrective Action
Waiting for link	DHCP option 43 or 125 on Release 7.0 or later systems or option 129 for earlier Releases is not programmed correctly.	Check Option 43, 125, or 129 on DHCP to confirm that the IP address is programmed correctly (RTC IP Address of controller).
	The Layer 2 switch port may be running spanning tree.	Turn port fast on or disable Spanning tree (whichever is possible).
	The application server is broadcasting or multicasting on IP Phone port or on PC behind the IP Phone.	Turn off multicasting.
	The PC behind the IP Phone is changing speed 100/10.	Depending on the NIC, you may need to hardcode to 100 MBps instead of auto negotiation.
Waiting for link OR Lost link to Server	IP phone fails to receive Keepalive message in 30 seconds.	Verify if the network or the controller is down.
	There is electrical interference.	Verify the power source, and change the location of the power source.

(Page 5 of 6)

Table 27: IP Phone Registration Troubleshooting (continued)

Error Message on Display	Probable Cause	Corrective Action
TFTP Fail (Remote IP phone (statically programmed IP address) cannot access MN3300 across WAN).	The Layer 2 switch port for the phone interface is shut down or not configured properly.	1. Check the Layer 2 switch and ensure that the port is not shut down (see "Network Configuration Examples" on page 317 for more information). 2. For a Cisco Layer 2 switch: verify that this is a trunk port with Dot1q encapsulation, and ensure this trunk port allows both native and voice LAN to pass through. 3. For an HP Layer 2 switch: verify that Native Lan is untagged and Voice Lan is tagged.
	The Layer 2 switch port for router interface is shut down or not configured properly.	1. Verify which configuration you have (see "Network Configuration Examples" on page 317 for more information). 2. Ensure the port(s) on both sides (Layer 2 switch and router) are not shut down. 3. If there is physical interface on the router for each VLAN, make sure that the Layer 2 switch is set to access the port for the corresponding VLAN/subnet correctly; *OR* If this is a router on a switch, verify that this is a trunk port on L2 switch, and ensure this trunk port allows both native and voice LAN to pass through. 4. On the router's subinterface, verify that the proper VLAN is associated to the subinterface (see "Network Configuration Examples" on page 317).
	Typo in IP address, VLAN ID, gateway.	1. Delete and reprogram the static IP address. If there is no VLAN or priority, leave them as blank. 2. Verify that the gateway IP address is correct.

(Page 6 of 6)

Troubleshoot Phones and Peripherals

Phone Connection

If you can't fix the problem using Table 28, call Mitel Technical Support (see "Before You Contact Technical Support" on page 179).

Tip: Use the debug option on display IP phones to view Version, Network, Telephony/DSP, Connection Browser Config, memory Stats details (see page 170).

Table 28: Phone Connection Problems Troubleshooting

Symptoms	Probable Causes	Corrective Action
Can't make calls externally (display phone may show **call barred**).	COR restricted.	1. Identify the numbers dialed by the user, then check the route used in ARS. 2. Remove the COR number from COR group table in COR assignment used in the route, *OR* Change the COR group number in the route assignment form.
	COS restricted for PRI or QSIG trunk.	Enable **Public network access via DPNSS** in the set's COS.
Cannot make call over analog loop trunk (intermittent problem).	PBX is sending the dialing digits too fast for Telco's receiver on the LOOP trunk.	Insert a tone plan in the digit modification assignment for the route used by analog loop trunk (tone plan is used to insert one or two seconds delay without any tone detection).
If NONE of the sets are responding.	Problem with controller.	Perform a system check on the controller.
Sets cannot receive DID calls.	Non-DID is enabled in Station Service Assignment form.	Disable non-DID in the set's COS.

(Page 1 of 5)

Table 28: Phone Connection Problems Troubleshooting (continued)

Symptoms	Probable Causes	Corrective Action
No dial tone on set.	Set is not programmed.	In System Administration Tool, program the extension accordingly.
	Wrong wiring	Check the wiring between the phone jack and the ASU, peripheral cabinet, MDF, etc.
	Faulty handset wire.	1. Replace the handset cord. 2. Replace the handset. 3. Replace the set.
	Circuit is manbusy.	1. Enter the Maintenance command STATE <plid of the circuit>. 2. Enter the Maintenance command RTS <plid>.
	Circuit is locked out.	Verify the wiring between the phone and the patch panel.
Sets take 10-12 seconds to receive incoming calls.	ANI/DNIS number delivery trunk option is enabled in T1 trunk's COS.	Disable the ANI/DNIS number delivery in the trunk's COS. **Tip:** You can assign an unused COS to verify if this is the problem.
	Dialing digit conflict.	Check the following forms for any potential dialing conflict: - Station Service Assignment - Miscellaneous Assignment - Feature Access Code - Agent ID Assignment - System Option Assignment

(Page 2 of 5)

Table 28: Phone Connection Problems Troubleshooting (continued)

Symptoms	Probable Causes	Corrective Action
IP to IP calls OK, but not IP to TDM calls (rings once, then call drops).	E2T not loaded.	1. Verify that the E2T IP address is programmed correctly. 2. Verify that the E2T IP address is not used elsewhere on the network. 3. If the E2T IP address was hardcoded with a debug table, verify its settings (see Table 77 on page 301).
All resilient IP Phones are not functioning (no dial tone) after the primary ICP goes out of service.	Refer to the 3300 ICP Resiliency document on Mitel OnLine for corrective action.	
Resilient phones do not fail over to their secondary ICP when their primary fails.	Refer to the 3300 ICP Resiliency document on Mitel OnLine for corrective action.	
Some resilient phones are not functioning (no dial tone) after the primary ICP goes out of service.	Refer to the 3300 ICP Resiliency document on Mitel OnLine for corrective action.	
One resilient phone is not functioning (no dial tone) after its primary ICP goes out of service.	Refer to the 3300 ICP Resiliency document on Mitel OnLine for corrective action.	
While on a call at a resilient phone, the primary ICP goes out of service and the call is immediately dropped (no call survival). After you hang up the IP phone and go off-hook again, the IP phone is functioning on its secondary ICP.	Refer to the 3300 ICP Resiliency document on Mitel OnLine for corrective action.	

(Page 3 of 5)

Table 28: Phone Connection Problems Troubleshooting (continued)

Symptoms	Probable Causes	Corrective Action
While on a call at a resilient phone, the primary ICP goes out of service, and the call is immediately dropped (no call survival). After you hang up the IP phone and go off-hook again, the IP phone remains out of service.	Refer to the 3300 ICP Resiliency document on Mitel OnLine for corrective action.	
After an IP phone fails over to its secondary ICP, you can make calls from it, but other TDM phones, trunks, or IP devices in the cluster cannot call it.	Refer to the 3300 ICP Resiliency document on Mitel OnLine for corrective action.	
After the primary ICP is returned to service, the IP phones do not fail back to the primary. If an IP phone is on its secondary ICP, you hear beeps every 20 seconds, and the phone displays "Fail <ICP IP address>".	Refer to the 3300 ICP Resiliency document on Mitel OnLine for corrective action.	
Message waiting indicator on a resilient phone continues flashing for a Callback message that has already been returned.	Refer to the 3300 ICP Resiliency document on Mitel OnLine for corrective action.	
Hot desk users cannot log in after their IP phones fail over to the secondary ICP.	Refer to the 3300 ICP Resiliency document on Mitel OnLine for corrective action.	
Hot Desk user does not receive voice mail.	Refer to the 3300 ICP Resiliency document on Mitel OnLine for corrective action.	
		(Page 4 of 5)

Table 28: Phone Connection Problems Troubleshooting (continued)

Symptoms	Probable Causes	Corrective Action
A 5215 Dual Mode, 5220 Dual Mode, or 5235 IP Phone fails to boot up. Set display shows "Port Access Control – Press # to Continue".	802.1X port authentication is enabled in network. IP phone is not configured with a username and password.	Configure username and password on IP phone. See *"Configuring an Authentication Username and Password" on page 176*. OR Disable 802.1X support in the Layer 2 switch. See *"Enabling or Disabling 802.1X Authentication" on page 178.*
A 5215 Dual Mode, 5220 Dual Mode, or 5235 IP Phone fails to boot up. Set display shows "Port Access Failure – Rebooting".	802.1X port authentication is enabled in network. IP phone is not configured with correct username and password.	Check the username and password of the IP phone in database of the RADIUS server. Configure the correct username and password in the IP phone. See *"Configuring an Authentication Username and Password" on page 176* OR Erase the username and password that is stored in the phone. See "Erasing an Authentication Username and Password" on page 178. Reboot the phone in order to re-enter the username and password.
	802.1X port authentication is enabled in network. PC is connected to network through IP Phone. PC is not configured with correct username and password.	Check the username and password of the PC in database of the RADIUS server. Configure the correct username and password on the PC. OR Disable 802.1X support in the PC if enabled. OR Ensure RADIUS EAP is "EAP-MD5".

(Page 5 of 5)

Phone Audio Quality

If you can't fix the problem using Table 29, call Mitel Technical Support (see "Before You Contact Technical Support" on page 179).

Make sure you have the following information on hand before calling:

- ❒ Setup scenario
- ❒ Is there a common denominator (router, only one side of subnet, etc.)
- ❒ Other call scenarios (IP to IP, IP to TDM, etc.)
- ❒ Layer 2 switch configuration and settings
- ❒ Router configuration and settings
- ❒ Network diagram
- ❒ IP addressing scheme
- ❒ VLAN configuration and settings
- ❒ Layer 2 switch port statistics for FCS, collision and duplex mismatch.

Tip: Use the debug option on display IP phones to view Version, Network, Telephony/DSP, Connection Browser Config, memory Stats details (see page 170).

Table 29: Audio Quality Problems Troubleshooting

Symptoms	Probable cause	Corrective Action
One-way audio between Remote IP to TDM (VM)	No gateway IP address programmed on E2T.	1. If E2T gets IP address from DHCP server, make sure that Option 03 (Router) is assigned to the scope with the proper IP address for the subnet. 2. If E2T is hardcoded with a static IP address, make sure that the gateway IP address is programmed properly in VxWorks.
Distorted audio only on NSU	Voice encoding is not inverted.	For T1, enable **invert** for Voice encoding in link descriptor. For CEPT or API, enable **ADI invert** for voice encoding. (This does not apply to Embedded PRI.)
		(Page 1 of 3)

Table 29: Audio Quality Problems Troubleshooting (continued)

Symptoms	Probable cause	Corrective Action
Broken Audio, intermittent	Handsfree on the far end.	Ensure that neither device is using handsfree. Some handsfree phones only operate at half duplex.
	Packet loss, jitter via network.	1. Identify the speech path between the two end points, including router, switch WAN in the audio stream. 2. The network administrator needs to apply QOS/TOS to minimize jitter over slow speed interface (T1, Frame Relay, etc.), and give voice traffic priority over data.
	Limited bandwidth and too many calls across router, or combination data and voice.	1. Limit the number of calls to remote subnets. 2. The network administrator needs to apply QOS/TOS to give voice traffic priority over data.
	Physical port error (CRC, faulty cable, duplex mismatch, HUB).	1. Identify the speech path between the two end points, including router, switch WAN in the audio stream. 2. Verify that there is no duplex mismatch in each port settings, or faulty cable, or faulty port. 3. Make sure that the IP Phone is not plugged into a HUB.
	Compression zone enabled.	Compression will save bandwidth, but may cause noticeable clipping. If not sure, disable compression to see if it makes a difference.
	Router's CPU is exhausted or congested.	Router may be running excessive filtering. The network administrator may need to monitor the performance of the router.

(Page 2 of 3)

Table 29: Audio Quality Problems Troubleshooting (continued)

Symptoms	Probable cause	Corrective Action
Echo	Handsfree mode is used.	Check if far end is using handsfree. Switch to handset mode to see if this corrects it, or lower the volume in handsfree mode.
	Echo Canceller is beyond specifications.	1. Identify the path between the two end points, and verify if Trunk is always involved. 2. Check with Telco to see if the trunk is within specs. On a typical T1, the input signal should be -15 dB. If it is too high(-5 dB for example), echo may result. If this is the case, keep an echo log to isolate the problem.
	Network jitter issue.	If the problem only occurs between IP devices, check network jitter issue above.
Echo between IP Phones	Layer 2 switch setting problem.	1. Check the L2 switch for duplex mismatch and spanning tree. 2. Turn off spanning tree between the L2 switch and the IP Phone if possible (use the PortFast setting).
	Far end phone is on handsfree	Check if far end is using handsfree. Switch to handset mode to see if this corrects it, or lower the volume in handsfree mode.
	In conference call, echo is noticed from external trunk	1. Identify the path between the two end points, and verify if Trunk is always involved. 2. Check with Telco to see if the trunk is within specs. On a typical T1, the input signal should be -15 dB. If it is too high(-5 dB for example), echo may result. Keep a log to isolate the problem.
	There is an audio path between the users as well as between the phones.	Provide better acoustic shielding between users, e.g. close the door, provide sound-deadening partitions.

(Page 3 of 3)

IP Phone Boot Sequence

After you connect an IP Phone to the network, it goes through the following boot sequence (this applies to Release 5.0 and later):

Tip: MAC Addresses, and Main and Boot versions in the following table are examples for illustration purposes. The numbers displayed at the install site may be different. The x's are IP Address, VLAN, and Priority place holders.

Table 30: IP Phone Boot Sequence

Boot Sequence	Phone Display
1. Waiting for an Ethernet link to be established.	**Waiting for LAN link to come up**
2. If an Ethernet link is not established, continue with the bootup process.	**Bad LAN link** **Check Ethernet cable**
3. The first stage for bootup. **Note:** Refer to Table 31 on page 227 for 802.1x Port Access Control messages.	**08-00-0F-AA-BB-CC** **Booting: 04.02.01.06**
4. IP Phone contacts DHCP server to obtain IP address and VLAN information and a list of the controller addresses in the network. **Note:** Go to Table 32 if DHCP or TFTP fails.	**Waiting for DHCP** **Booting: 04.02.01.06** - **DHCP: Discovery** **Booting: 04.02.01.06**
5. The internal DHCP server provides one of these options: An external DHCP server provides one of these options: (where n is the number of the sub-option if encapsulation is used for the option.)	**Using option 125** **Using option 43** **Using option 128+** - **Using option 125:n** **Using option 43:n**
6. The DHCP server on the default VLAN responds with an Offer. If Option 43 or 125 (or option 130 prior to Release 7.0) is not properly set on the server, the set awaits further Offers (n is offer number).	**DHCP: Offer n Rej** **Booting: 04.02.01.06** - - - - - - - - - - - - - - - **DHCP: Offer n Acc** **Booting: 04.02.01.06**
7. The set replies with a Request and the server replies with an Acknowledgement.	**DHCP: Ack** **Booting: 04.02.01.06**
8. If the data in the Ack does not contain a VLAN ID and a packet Priority value, the set retains DHCP data, jumps to Step 11.	

(Page 1 of 3)

Table 30: IP Phone Boot Sequence (continued)

Boot Sequence	Phone Display
9. If the data included in the Ack does include a VLAN ID and packet Priority value, the set discards DHCP data and sends an untagged Release.	**DHCP: Releasing** **Booting: 04.02.01.06** **- - - - - - - - - - - - - - - - - - - -** **Vlan x Priority x** **Booting: 04.02.01.06**
10. The set goes through the Discovery/Offer/ Request/Ack sequence again.The packets sent are tagged to include VLAN and Priority values supplied by the first DHCP server.	
11. The TFTP server downloads the boot image and displays the set IP address. If there is no boot image, the set jumps to Step 13. Refer to Table 33 (page 229) for a description of possible error messages.	**xx.xx.xx.xx** **Downloading**
12. The boot file is copied to flash if it is a different version than the one in flash.	**Upgrading Flash** **DO NOT POWER DOWN**
13. If the boot load is the same as in flash, it is not copied.	**xx.xx.xx.xx** **Upgrade not required**
14. The set downloads a main image. A failure causes a phone reset, and the process starts again at step 1.	**xx.xx.xx.xx** **Download failed** **- - - - - - - - - - - - - - - - - - - -** **xx.xx.xx.xx** **Downloading** **- - - - - - - - - - - - - - - - - - - -** **xx.xx.xx.xx** **Starting main**
15. The set resets and the main load executes. The display changes to waiting for link. The set requests registration with the ICP (the first time request requires a PIN registration). The set waits for the ICP to take control.	**MAIN 08.04.01.01** **BOOT 04.02.01.06** **- - - - - - - - - - - - - - - - - - - -** **Set xx.xx.xx.xx** **ICP xx.xx.xx.xx** **- - - - - - - - - - - - - - - - - - - -** **Waiting for ACK...** **ICP xx.xx.xx.xx** **- - - - - - - - - - - - - - - - - - - -** **Waiting for COMMS...** **ICP xx.xx.xx.xx**

(Page 2 of 3)

Table 30: IP Phone Boot Sequence (continued)

Boot Sequence	Phone Display
16.After the main boot load is downloaded, (and only when a phone in a resilient network has homed to the wrong ICP) the phone seeks out the IP address of its primary 3300 ICP from the DHCP ICP Redirect list of 3300 ICPs in the network. It is possible for the phone to be redirected and you may see this display again.	**Set xx.xx.xx.xx** **ICP xx.xx.xx.xx** **- - - - - - - - - - - - - - - - - - - -** **Set xx.xx.xx.xx** **ICP xx.xx.xx.xx**
17.Once communication is established, the idle display appears on the set.	**<idle in service UI>** **<idle softkeys>**
	(Page 3 of 3)

Table 31: IP Phone Port Access Control Sequence

Sequence	Phone Display
1. Checking the L2 switch for 802.1x Port Access Control.	**Waiting for 802.1x authentication**
2. With access control, the L2 switch will ask for user and password (unless the data is stored in NVRAM).	**PORT ACCESS CONTROL** **PRESS # TO CONTINUE** **- -** **USER (# to end)** **—** **- -** **PASSWORD (# to end)** **—**
3. If Port Access Control fails.	**Port Access Failure** **REBOOTING. . .** **- -** **Waiting for 802.1x authentication**
4. If the data exchange succeeds or if the L2 switch does not support 802.1x Port Access Control.	**Waiting for LLDP**

Table 32: IP Phone Error Handling Displays

Message Description	Phone Display
Note: Check the IP Parameters (TFTP address, netmask, gateway address), to make sure that they are valid, before calling Mitel.	
If TFTP fails, usually due to incorrect TFTP Server or Gateway IP address, review IP parameters and correct errors.	**RTCS creat err** <number> **BOOTING xx.xx.xx.xx** **- -** **If add err** <number> **BOOTING xx.xx.xx.x** **- -** **RTCS Bind err** <number> **BOOTING xx.xx.xx.x**
The TFTP server sent an "I am busy" error so the phone will delay and retry.	**xx.xx.xx.xx** **Waiting for TFTP**
If the phone received a bad packet from the TFTP server, audit the TFTP server configuration and the network path.	**xx.xx.xx.xx** **TFTP Err:** <number>
This error indicates that you must review the IP parameters on the DHCP server or manually entered for the phone.	**xx.xx.xx.xx** **TFTPerr: Packet send**
Internal TFTP errors - contact Mitel Technical Support.	**xx.xx.xx.xx** **TFTPerr: Sock create** **- -** **xx.xx.xx.xx** **TFTPerr: Sock bind** **- -** **xx.xx.xx.xx** **TFTPerr: Packet alloc**

Table 33: Download and Software Error Displays

Message Description	Phone Display
Note: Check the IP Parameters (TFTP address, netmask, gateway address), to make sure that they are valid, before calling Mitel.	
These errors indicate that the Flash was not upgraded. The phone will pause for 3 seconds and continue.	**L2 download err** **- -** **Boot download err** **- -** **L2&Boot download err**
The ICP instructs the phone to get a new main executable. Two-line display set: Single-line display set:	**TFTP MAIN FROM** **xx.xx.xx.xx** **- -** **TFTP MAINLOAD**
If the phone received a bad packet from the TFTP server, audit the TFTP server configuration and the network path.	**xx.xx.xx.xx** **TFTP Err:** <number>
This error indicates that you must review the IP parameters on the DHCP server or manually entered for the phone.	**xx.xx.xx.xx** **TFTPerr: Packet send**
Internal TFTP errors - contact Mitel Technical Support.	**xx.xx.xx.xx** **TFTPerr: Sock create** **- -** **xx.xx.xx.xx** **TFTPerr: Sock bind** **- -** **xx.xx.xx.xx** **TFTPerr: Packet alloc**
TFTP IP address is missing from the configuration string.	**125:TFTP tag missing OR** **43:TFTP tag missing**
ICP IP address is missing from the configuration string.	**125:ICP tag missing OR** **43:ICP tag missing**
Encapsulation is incorrect.	**Bad 125 subopt endOR** **Bad 43 subopt end**

Checking the IP Phone Progress Display

A progress bar, consisting of flashing rectangles, is displayed in the upper right corner of the IP Phone display whenever a phone is trying to re-home (except on boot-up) to any ICP controller. The set will display a progress bar if a resilient IP phone re-homes as a result of a Hot Desk login.

Three rectangles indicate the progress of the activity:

- Left block flashing - waiting for TCP link connection with ICP
- Left block solid and middle block flashing - waiting for registration message acknowledgement from ICP
- Left and middle blocks solid, right block flashing - waiting for MiNET communications with the ICP that will take over the display at this point.

When the three rectangles are solid, the activity is complete. If the IP Phone does not complete the activity after several minutes, check the progress status by pressing the * key on the dial pad.

Re-home Sequence	Resilient Phone Display
Resilient waiting for link UI (first block flashing) 	<**idle ui line1**> <**idle ui line2**>
Resilient waiting for ACK UI (second block flashing) 	<**idle ui line1**> <**idle ui line2**>
Resilient waiting for COMMS UI (third block flashing) 	<**idle ui line1**> <**idle ui line2**>
Phone connected to secondary ICP (solid block) 	<**idle ui line1**> <**idle ui line2**>

IP Console

Table 34: IP Console Problems Troubleshooting

Symptoms	Probable cause	Corrective Action
IP console fails to register (red LED is lit on TKB)	TKB (keyboard) - does not have a reserved IP address *OR* does not have the right IP address *OR* is not communicating with the right controller.	1. Check DHCP lease to confirm if an expected IP address is assigned to TKB. 2. If not assigned properly, ensure that you enter the MAC address of TKB properly in the Multiline Set Assignment form in System Administration Tool. 3. Recycle the power of the TKB to ensure that the TKB is reloaded properly.
	Console PC does not have the proper IP address.	If the IP address of PC is on different subnet than the TKB, make sure that the router between these two subnets is functional.
	PC NIC has 802.1Q enabled on Data side while L2 switch is not configured to accept tagged frame on Native VLAN.	Disable 802.1Q on PC NIC **Note:** Only use 802.1Q on PC if PC and TKB are on the same VLAN (e.g 2) which L2 switch accepts tagged frame on the specified VLAN.
IP Console fails to launch	IP Console has been registered and IP console is reinstalled.	Delete the MAC address from IP console form and then re-register using the IP Console Configuration Wizard (Start/MN5550 IP console/Tools). **Note:** Do not reinstall the IP Console software unless you need to (new installation, corrupted software, etc.). You should always use the Configuration Wizard to register to a different controller.
	User does not have local administration privileges.	Add local administration privileges for the user.

Chapter 6
Maintenance

General Maintenance Procedures

Checking the System

1. Click **Maintenance Commands** in the System Administration Tool.
2. Enter the following commands:
   - **SH ST AL**: Checks for system alarms. There should be no alarms.
   - **DBMS STAT**: Checks the status of the initialized flag. The flag is on if the system is in sync. If the flag is off, enter DBMS Save.
   - **PROG R DIS**: Displays the scheduled system reset. By default, the system reboots at 2:15 a.m. daily ONLY if there is memory fragmentation. To force a system reboot at the scheduled time, see the Programmed Reboot command.
   - **ME S**: Checks the status of the communication links. All links should be open.
   - **PCM TO**: Checks for circuit switch link faults; there should be none.
   - **DBMS CH B** or **F**: Brief checks the sanity of the database. Full checks the sanity and the current status of the database.
3. Click **Maintenance Logs - Error** to check for error logs or click **Maintenance Logs - All** to see all maintenance logs.
4. Check that you have recent backups of the database and hard drive.

Tip: You should make a backup at least once a week. Keep a copy of the last 3 backups.

Checking Controller Hardware Profile

1. Click **System Hardware Modules** in the System Administration Tool.
2. Click **System Hardware Compute Cards** for data on the RTC / E2T.
   - Verify that the IP address of the E2T is the correct one.
   - Slot 1 is always the RTC. For a 100-User controller, this form displays the details on the RTC only.
   - Verify the value of the **Core Speed** field:
     For a 133 MHz system, the value is 132000000.
     For a 300 MHz system, the value is 297000000.
     For a 450 MHz system, the value is 450000000.

Maintaining Security

Maintaining VoIP Security

In an IP-enabled network, secure connections between IP endpoints is required and can be achieved in the following ways:

- Media Signaling Security ensures all messages transmitted over IP are encrypted.
- Voice Streaming Security ensures all voice packets transmitted over IP are encrypted. For more information about Secure RTP (SRTP), see Voice Streaming Security in the Online Help.

Secure Sockets Layer (SSL) and Security Certificate

To install the certificate:

1. On the **Security Alert** window, click **View Certificate**. The General window displays an error message meaning that you must trust the certificate and the Certifying Authority (CA) that issued the certificate.
2. Click **Certification Path**. Within the certificate chain, it is the Mitel Root CA that we need to trust.
3. Select **Mitel Networks Root CA** and click **View Certificate**.
4. Click I**nstall Certificate**.
5. Click **Next** to navigate through the Certificate Import Wizard windows.
6. Click **Finish** on the Completing the Certificate Import Wizard window.
7. Click **Yes** on the Root Certificate Store window.
8. Click **OK** until you can view the web page.

View Logs

This section contains the following:

Viewing Maintenance or Software Logs

To view maintenance or software logs:

1. Log into the System Administration Tool (see page 8).
2. Click the desired log category (Maintenance or Software).
   - To view all the logs in the category, click **All Maintenance Logs** (or **All Software Logs**).
   - To view error logs, click **Error**.
   - To view warning logs, click **Warning**.
   - To view information, click **Info**.
3. To highlight the desired log, move your cursor over it and click once. The details of the log are displayed in the lower half of the screen.

Table 35: System Reset Causes

Reset Cause	Interpretation	Root Cause
0x3	Hard reset	Unknown reset
0x13	Checkstop reset (see PPC82XX manual)	Double bus fault as documented in the Power PC Manual
0x43	Watchdog reset	The watchdog task was unable to write to the hardware watchdog. A higher priority task is running or interrupts are disabled. This is a software problem.
0x83	Power-on reset	The system lost AC power.

(Page 1 of 2)

Table 35: System Reset Causes (continued)

Reset Cause	Interpretation	Root Cause
0x103	Programmed reset	The system software intentionally restarted the system.
0x203	Push-button reset	The front panel reset button was pressed.
		(Page 2 of 2)

Collecting System Logs, Release 5.2 and Later

Product Support may request logs in the event of a system failure (see Table 36 below). In the event of a system lockup, go to "Collecting System Lockup Logs - Release 5.1 System" on page 240.

Table 36: System Logs

Log Type	Log Purpose
pstswlog.db	Current system software and maintenance logs
backup pstswlog.db	May contain additional logs if the pstswlogdb is overwritten
xrtc	Software exception or trap on RTC
xe2t	Software exception or trap on E2T
premortem***.txt	Network statistics on RTC
e2tpremortem.txt	Network statistics on E2T
system.wvr	System lockup events. Generated by entering debug commands or pre-installed sysinfo.txt during the lockup (refer to "Collecting System Lockup Logs - Release 5.1 System" on page 240).
output from RTC console	Additional error logs only output to the RTC console (see "Collecting System Lockup Logs - Release 5.1 System" on page 240).
diag.dat	Voice mail event file. Enter errlog_flush() before dumping the logs.
diag.sav	Voice mail backup event file.
master.dat	Voice mail master index for all mailboxes.

Collecting System Logs - Release 5.2 and Later

To download the system diagnostics file to your computer:

1. Select **Maintenance and Diagnostics** from the Selection drop-down list.
2. Click **System Diagnostics Reporting**.
3. Select the **Download the files to my computer** radio button.
4. Click **Send System Diagnostics Report**.
5. A warning window opens reminding you that this process may take a few minutes. Click **OK** to continue.
6. When the **File Download** dialog box appears, click **Save** (not Open).
7. Navigate to the desired folder on your computer or network drive.
8. Rename the file if desired (the file extension remains .tar.gz).
9. Click **Save**. The file is downloaded to your computer.

Collecting System Lockup Logs - Release 5.2 and Later

Use the Remote on/off button to generate a debug diagnostic file. This procedure applies to 100, 250-700 user, MX, and LX platforms running Release 5.1.5.8 or higher only.

To collect system lockup logs:

1. Press and hold the Remote on/off button until all of the alarm indicators on the panel light (approximately 3 seconds).
2. Complete the procedure above, “Collecting System Logs - Release 5.2 and Later”.

Collecting System Logs, Release 5.1

Collecting System Logs - Release 5.1 System

To collect the logs on a Release 5.1 system:

1. Log into the System Administration Tool (see page 8).
2. Select **System Diagnostics** and then click **Export**.
3. Click **Export** and then click **Continue**.
4. After the **File Download** dialog box appears, click **Save**.

5. Navigate to a folder or network drive on your PC. Ensure that the file extension is set to (**.tar**).
6. Click **Save** and then click **Close**.

To collect the logs through PC to controller network connectivity:

1. At the DOS prompt, type **cd c:\3300log** (example folder name)
   Type **ftp <ip address of the controller>**
   Enter the ESM username and password when prompted.
   You should see the ftp prompt when you successfully log in.
   Type **binary**
   Type **hash**
   Type **prompt**
2. Type **cd /db/database/files**
   Type **get pstswlog.db**
3. Type **cd /db/database/sw_log_backup**
   Type **mget *.db**
4. Type **cd /db**
   Type **get xrtc**
   Type **get xe2t**
   Type **get e2tpremortem.txt**
   Type **mget premortem*.txt**
5. Type **cd /db/spylog**
   Type **get system.wvr**
6. Type **cd /vmail /c/voxdrv**
   Type **get diag.dat**
   Type **get diag.sav**
   Type **cd /vmail/c/vm**
   Type **get master.dat**
7. Type **bye**.
8. Zip all of the files in the folder that you created (**c:\3300log** in this example) and send to Product Support in an e-mail with your problem ticket number.

Collecting System Lockup Logs - Release 5.1 System

In the event of a system lockup for software prior to Release 5.2, complete this procedure, then go to "To collect the logs through PC to controller network connectivity:" on page 240. This procedure is needed to obtain **system.wvr** logs and output from **RTC console**.

To prepare to for collecting system lockup logs:

1. Save the “HardResetHook” commands in a text file called **sysinfo.txt**. The file is also available at ftp://ftp.mitel.com/outgoing/.
   wvSpy 20, “system.wvr”, 3
   i
   HardResetHookAddTaskName “DRATask
   . . .
   . . .
   HardResetHookGroupTaskTrace
2. FTP sysinfo.txt file into the db directory of the 3300 ICP:
   At the DOS prompt, type **cd c:\sysinfo.txt**
   Type **ftp <ip address of the controller>**
   Login with the ESM username and password.
   Type **binary**
   Type **cd /db**
   Type **put sysinfo.txt** (OR enter each command at the RTC console)
   Type **bye**
3. Execute the sysinfo.txt on the RTC Console if the 3300 ICP locks up:
   Access RTC Console via communication software (i.e. HyperTerm).
   Type **cd “/db”**
   Type **<sysinfo**
4. Collect all required logs. See “To collect the logs through PC to controller network connectivity:” on page 240.

Viewing Logs Remotely, TCP/IP Socket Numbers

You can direct logs and Automatic Call Distribution (ACD) Real Time Events to remote applications by setting up TCP/IP Output Streaming from the remote application.

Tip: The remote application must act as a TCP/IP client. The default setting is three sockets (communication channels); maximum setting is ten sockets for each application.

To set up TCP/IP output streaming:

1. Open a Telnet session.
2. Under PORT, enter the appropriate socket number (see Table 37).
3. Enter the IP address of the controller RTC.

Tip: If the TCP/IP connection drops, reconnect the client application.

Table 37: TCP/IP Output Streaming Settings

Log Output	Socket Number
Software Logs	1750
Maintenance Logs	1751
SMDR Logs	1752
Hotel/Motel Logs	1753
LPR1 Printer Port	1754
ACD Real Time Event	15373
IP PMS (Release 6.0)	15374
PMS Voice Mail Integration	6830

Viewing Login and Logout Audit Logs

To view Login/Logout logs:

1. Log into the System Administration Tool (see page 8).
2. Click **Login/Logout Audit Logs**.
3. Use the Session ID number and the Login Type field to identify the login and logout events for a particular user.
4. Use the Audit Log ID to uniquely identify each log.
   The Audit logs contain the following information:
   - **Audit Log ID:** unique log identifier.
   - **Date and Time:** when the action occurred.
   - **Action:** login or logout.
   - **User login ID:** user name of the account that performed the login or logout.
   - **Source IP Address:** IP Address of the client station from which the login or logout was performed.
   - **Login Type:** ESM Login Page, System Administration Tool, Group Administration Tool, Telnet to RTC, Telnet to E2T, FTP, MiXML.
   - **User Authenticated:** True means the login was successful; False means a login failure.

- **Session Availability:** True means a session is available for an authenticated user. False means that the maximum allowed sessions has been reached.
- **Session ID:** The same session ID is recorded for a newly opened session and again at logout. Use both the login type and the session ID to identify events from the same session/user.
- **Comments:** Provides login and logout details, for example, reason for login failure and reason for a logout.

Tip: Login and logout logs are also displayed in the All Logs view as Maintenance Log Type and Login/Logout Security Audit Source. Successful logins and logouts are recorded as Information maintenance logs. Failed login attempts due to incorrect passwords are recorded as Warning maintenance logs.

Device Connectivity

Device move detection, in support of E911 Emergency Calling Services, is critical to maintaining the accuracy of Customer Emergency Services ID (CESID) information. With Release 5.2, the IP device location can be automatically updated or the location can be monitored for manual update. Detection of Layer 2 connectivity is through Spanning Tree Protocol (STP) or Cisco Discovery Protocol (CDP). The Device Connectivity form excludes Mitel Soft Phones, Symbol, DECT, and SpectraLink wireless phones, DNIC telephones, CITELlink telephones, and Hot Desk Users.

Automatic CESID Update

Requirements and restrictions for Automatic CESID:

- All Layer 2 switches must report to CDP or STP or both (use one or both protocols consistently on all L2 switches in the network)
- Designate Emergency Calls using Route Lists
- Not supported on hubs
- CDP or STP must be enabled on L2 switches
- Automatic CESID will not function during a backup or restore

Monitoring Device Move Detection

1. Log into the System Administration Tool (see page 8).
2. Click **Device Connectivity - Moved**, or **Device Connectivity - All**. You can print or export the form (see page 88).

Table 38: Device Connectivity Form Fields

Field name	Description
DN	Directory number of the IP device.
Date	Date and time of most recently reported L2 connectivity report from the set
Time	
Previous STP L2 Port MAC	MAC address of the STP Layer 2 switch where the IP device was connected before being moved.

(Page 1 of 3)

Table 38: Device Connectivity Form Fields (continued)

Field name	Description
Previous STP Port Identifier	Port number on the STP Layer 2 switch where the IP device was connected before being moved.
Previous CDP L2 Port MAC	MAC address of the CDP Layer 2 switch where the IP device was connected before being moved.
Previous CDP Port Identifier	Port number on the CDP Layer 2 switch where the IP device was connected before being moved.
Previous CDP L2 IP Address	IP address of the CDP Layer 2 switch where the IP device was connected before being moved.
Last Known STP L2 Port MAC	MAC address of the STP Layer 2 switch where the IP device was connected on first registration or registration after a move. - "Unknown" device is one that does not support STP with its current firmware load. A 'Reload' of set firmware may be required. - "Not Supported" device indicates that L2 switches do not support STP. Contact the L2 switch provider; an upgrade may be required.
Last Known STP Port Identifier	Port number on the STP Layer 2 switch where the IP device was connected on first registration or registration after a move. - For some hardware manufacturers and/or network configurations, a designated port number may be reported by STP instead of actual port number. The designated port number is assigned to the port during STP convergence.

(Page 2 of 3)

Table 38: Device Connectivity Form Fields (continued)

Field name	Description
Last Known CDP L2 Port MAC	MAC address of the CDP Layer 2 switch where the IP device was connected on first registration or registration after a move. - "Unknown" device is one that does not support CDP with its current firmware load. A 'Reload' of set firmware may be required. - "Not Supported" device indicates that L2 switches do not support CDP. Contact the L2 switch provider; an upgrade may be required.
Last Known CDP Port Identifier	Port number on the CDP Layer 2 switch where the IP device was connected on first registration or registration after a move.
Last Known CDP L2 IP Address	IP address of the CDP Layer 2 switch where the IP device was connected on first registration or registration after a move.
State	"In Service" or "Out of Service". This data used by the system to determine whether multiple in-service devices are connected through the same Layer 2 MAC and Port. Useful for identifying system configuration issues.
Move Acknowledged	"Not applicable" indicates a device that has not moved. This is the only editable field. After you have updated the Customer Emergency Services ID (CESID) Assignment form, change this field to **Yes**. Click **Data Refresh** to remove the device from the list of Moved devices.
	(Page 3 of 3)

Tip: Refer to the System Administration Tool online help for Device - Move examples and explanation of field information.

Device Move Detection Procedures

- Monitor the Device Connectivity - Moved form to identify devices that have moved. The monitoring schedule depends on how often you suspect devices may be moved, and the corporate emphasis on accurate Customer Emergency Services ID (CESID) information.
- In a resilient environment, it is usually sufficient to address a device move when it is detected on the Primary controller. If a device is moved while the primary controller is down, the move will be detected when the device comes back under the control of the primary.
- When you change a CESID Assignment for a phone DN in a Hot Desking environment based on a device move detection, the Mobile DN (Hot Desk) user should log out and log back in.
- When the Device Connectivity - Moved form indicates a device move has occurred in a resilient environment, you should update the CESID Assignment through OPS Manager's Moves, Adds, and Changes so that the CESID change is propagated to all controllers.
- The device move detection feature requires that the sets have the Release 5.0 or later firmware. You can update the firmware in three ways: issue the **LOAD IP DEVICE 1 to 700** command; power down the sets; or by a loss of connectivity with the 3300 ICP for 10 minutes or more.
- In a case where the primary 3300 ICP is Release 5.0 or later and the secondary is Release 4.x, a device move will not be detected if it occurs while the set has failed over to the secondary. The move will be detected when the device comes back under the control of the primary 3300 ICP with Release 5.0 or later software.

Viewing Device Connectivity Logs

To view device connectivity logs:

1. Click **All Maintenance Logs**.
2. Select **Source** in the **Go to** drop-down list.
3. Type **device move detection** in the **value** field.

IP Phone Analyzer

The Mitel 3300 ICP IP Phone Analyzer is an application that collects performance information from the IP devices on the network.

Requirements

Install the IP Phone Analyzer on a PC running Windows NT, Windows 2000, Windows XP, or Windows 98.

Tip: The PC must be connected to the network via a Layer 2 switch port on the controller.

Installing the IP Phone Analyzer

To install the IP Phone analyzer:

1. In the System Administration Tool, program the IP address of the PC to Option 131 for pre-Release 7.0 systems or to the ipa_srv tag in Option 43 for Release 7.0 and later systems.
2. Insert the 3300 ICP software CD-ROM in the PC's CD drive.
3. Open the CD's **Tools** folder, then the **Phone Analyzer** folder.
4. Double-click **Setup.exe**. Follow the IP Phone Analyzer install prompts.

Launching the IP Phone Analyzer

- Open **Mitel IP Phone Analyzer** (**Start**/**Programs**).

Tip: For detailed information, refer to IP Phone Analyzer Online Help.

Enabling Tool Analysis

To enable tool analysis from the IP Phone Analyzer Tool:

1. Select **Commands**, then **Register Set**.
2. Enter the IP address of the IP telephone.

To enable tool analysis from the IP telephone:

- Reboot the phone to add the IP address of the PC to the telephone. The IP address appear on the IP Phone Analyzer Status View window.

From the System Administration Tool:

- To monitor all IP telephones, issue the **LOAD IPDEVICE ALL** maintenance command. There will be a service outage while the telephones reset.

Disabling Tool Analysis

To disable tool analysis from the PC hosting the Analyzer Tool:

- Access the **Status View** window, left-click on the IP address, then right-click and select **Delete**.

To disable tool analysis from the System Administration Tool:

1. In the **DHCP Options** form for Release 7.0 and later systems, disable IP messaging to the PC tool by deleting the IP Phone Analyzer Address from the appropriate Option 125. For earlier releases, delete option 131.
2. To disable the monitoring of all IP telephones, issue the **LOAD IPDEVICE ALL** maintenance command.
   There will be a service outage while the telephones reset.

To disable tool analysis from an IP telephone:

- Restart the set to clear the PC IP address from the telephone.

Disabling/Enabling Voice Encryption

To Disable/Enable Voice Encryption:

1. From the System Administration tool, access the System Options Assignment form.
2. The Voice Encryption Enabled field is set to "Yes" by default.
3. Click **Change**.
4. To disable voice encryption, select **No**.

LSMeasure Tool

Use the LSMeasure Tool to determine the line settings for Loop Start (LS) trunks that are connected to the Analog Main Board and Analog Option Board in the controller, or to the Universal ASU.

Refer to Measuring LS Trunk Line Settings in the System Administration Tool Online Help for detailed instructions and message interpretation.

To launch the LSMeasure Tool:

1. Log into the IP address of the Real Time Controller (RTC).
   - To log in through a telnet session, at the "telnet>" prompt, enter open <IP Address of RTC> 2002
   - For RS-232 maintenance session, set the serial port parameters:
     Port: COM1
     Baud Rate: 9600
     Data Bits: 8 data bits
     Stop Bit: 1
     Parity: None
2. At the –> prompt, type **LSMeasure** and press **Enter**.
3. Enter **7** to exit the LSMeasure tool when the tests are complete.

Appendix A
Hardware Reference

System Configurations

There are several basic options for the 3300 ICP:

- 100-user system
- CXi system with embedded Analog and an Ethernet Layer 2 switch
- CX system without embedded Analog and without Ethernet ports
- MX system with embedded Analog
- MXe system without embedded Analog
- MXe system with embedded Analog
- LX, 250 and 700-user system
- LX controller with 512 MB memory on the RTC for 1400 users

Controller Hardware Details

For detailed information on the 3300 ICP components, see the Hardware Technical Reference Manual on Mitel OnLine.

Table 39: 3300 Controller Versions

Controller	133 MHz	266 MHz	300 MHz	450 MHz
100-User	n/a	n/a	50002211	n/a
3300 CXi (with Ethernet)	n/a	50004640 50005097	n/a	n/a
3300 CX (without Ethernet)	n/a	50004641 50005096	n/a	n/a
3300 MX with Analog	n/a	n/a	50004190	n/a
3300 MX without Analog	n/a	n/a	50004343	n/a
3300 MXe	n/a	n/a	n/a	50005100 50005080
250-User	50001262	n/a	50002970	n/a
3300 LX / 700-User	50001263	n/a	50002971	50004191
3300 LX controller 512M	n/a	n/a	n/a	50004942
Note: See page 235 to determine your controller speed. Part numbers are usually on a Mitel sticker at the back of the controller.				

Controller Components

Tip: For each module, the leftmost connectors correspond to Port 1 for that module, and the rightmost to Port 2.

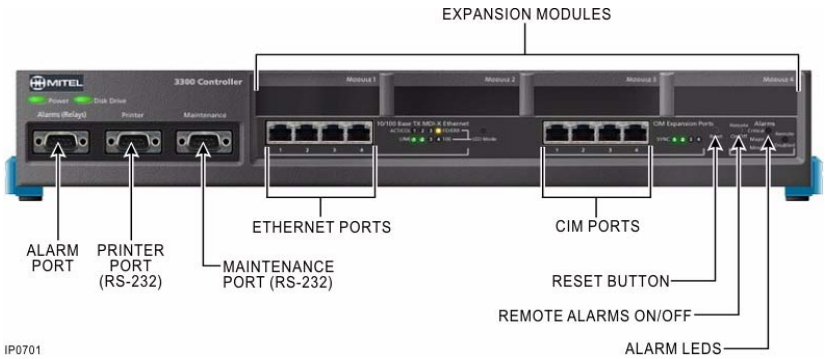


Figure 31: LX, 250/700 Users Controller — Front Panel

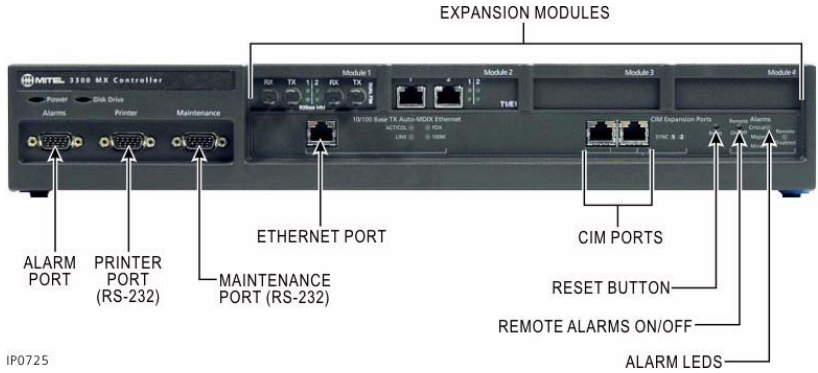


Figure 32: MX Controller — Front Panel

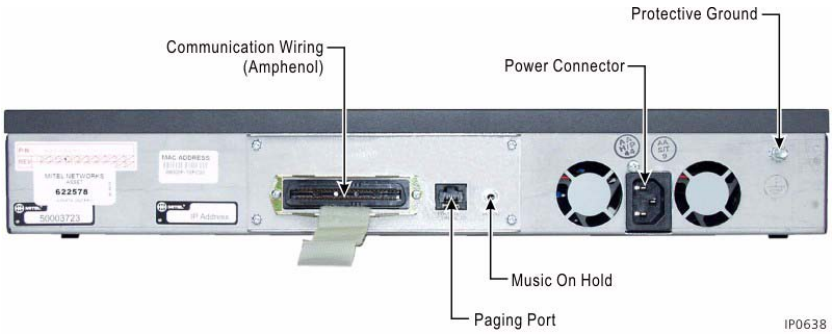


Figure 33: MX Controller — Back Panel

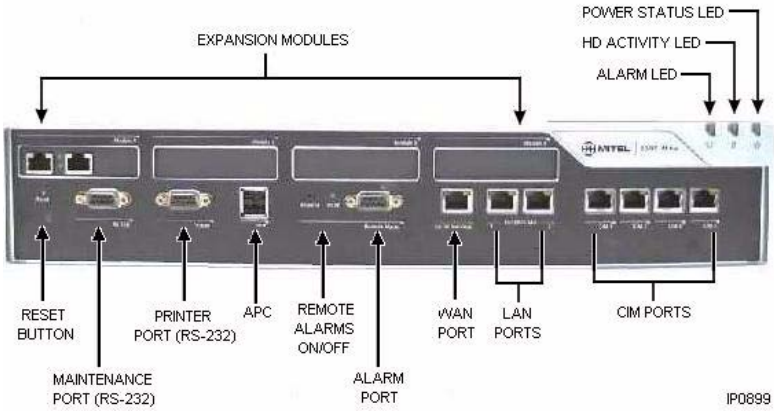


Figure 34: MXe Controller — Front Panel

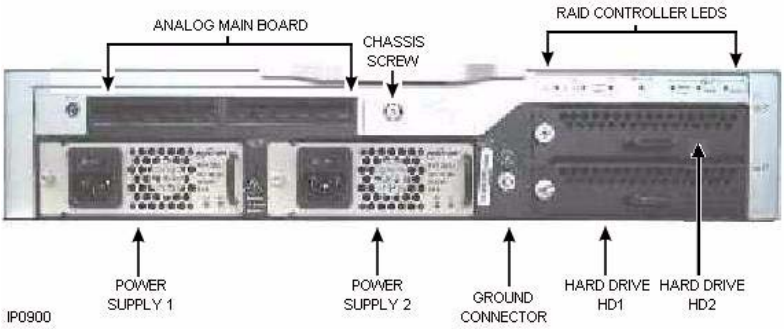


Figure 35: MXe Controller — Back Panel, Redundant with Analog

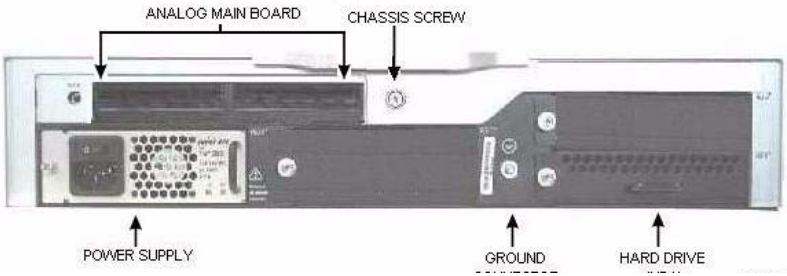


Figure 36: MXe Controller — Back Panel, Non-Redundant

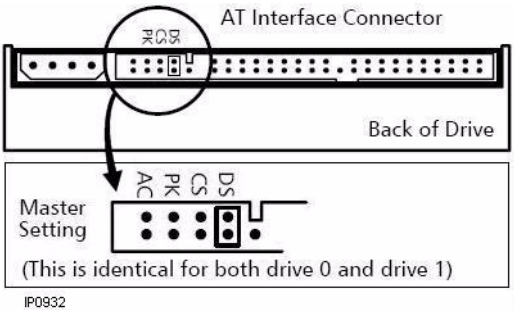


Figure 37: MXe Controller — Hard Drive Jumper Settings

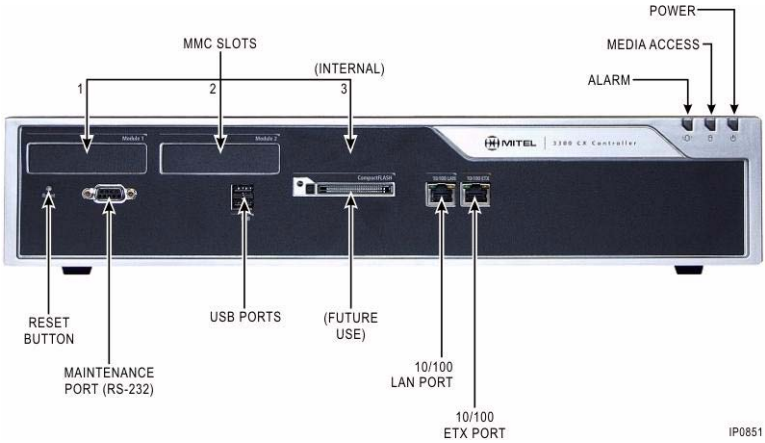


Figure 38: CX Controller — Front Panel

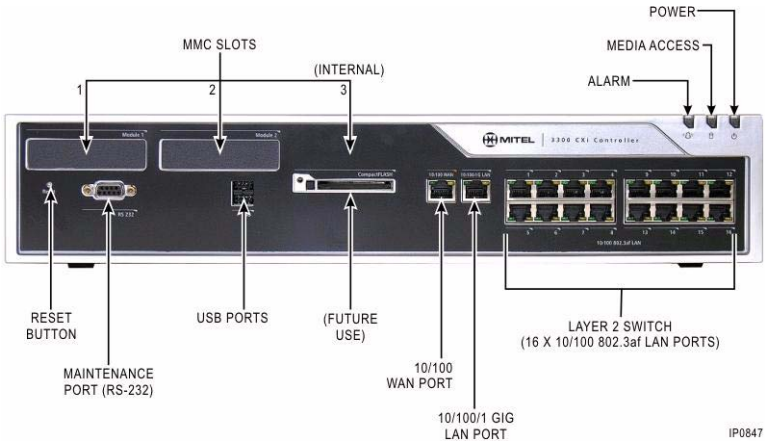


Figure 39: CXi Controller — Front Panel (200ICP place-holder)

Figure 40: CX Controller — Back Panel

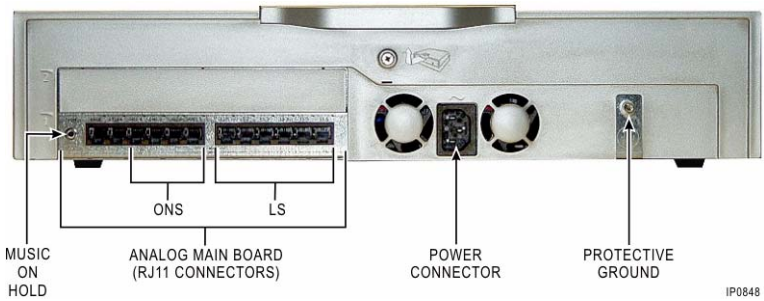


Figure 41: CXi Controller — Back Panel

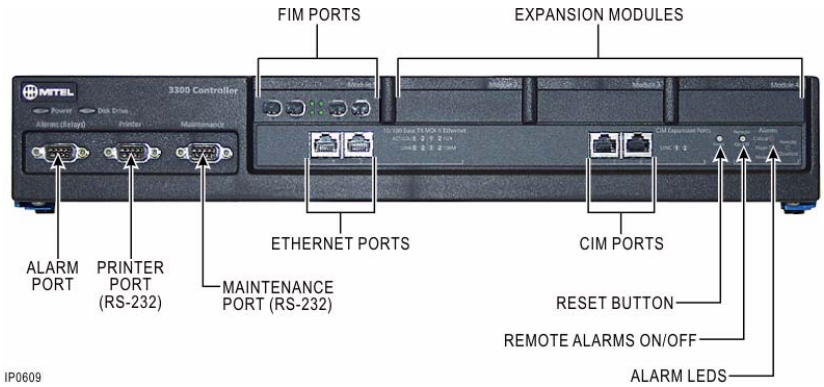


Figure 42: 100-User Controller — Front Panel

Tip: The 100-user controller has 2 Ethernet ports, but only the leftmost port can be used.

Controller Cabinet Numbering

- Cabinet 1 (hardcoded): internal.
- Cabinets 2 to 5 (hardcoded): CIM ports, from left to right (not CX/CXi).
- Cabinets 6 to 13 (6 to 9 for the MX and 100-user): module ports (left to right).

T1/E1 Combo Card

The T1/E1 combo module provides T1 trunking and DSP functionality for the CX with Release 6.0 software and for all controllers (266/300 MHz minimum) with Release 7.0 software. The DSP provides resources for CLASS tone generation, Record a Call conferences, DMTF receivers, voice compression. The card also provides voice echo cancellation.

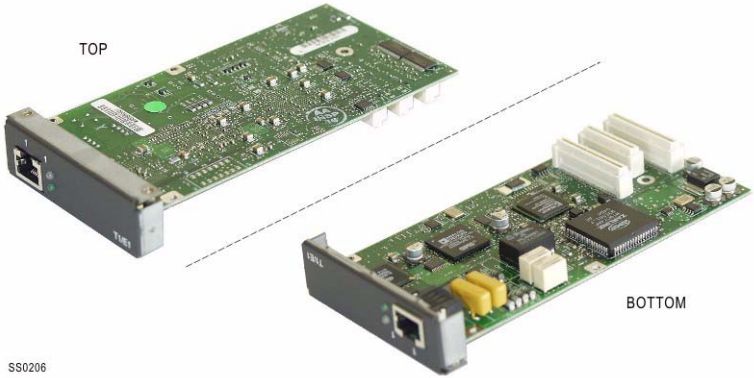


Figure 43: T1/E1 Combo Card (prior to Release 7.0)

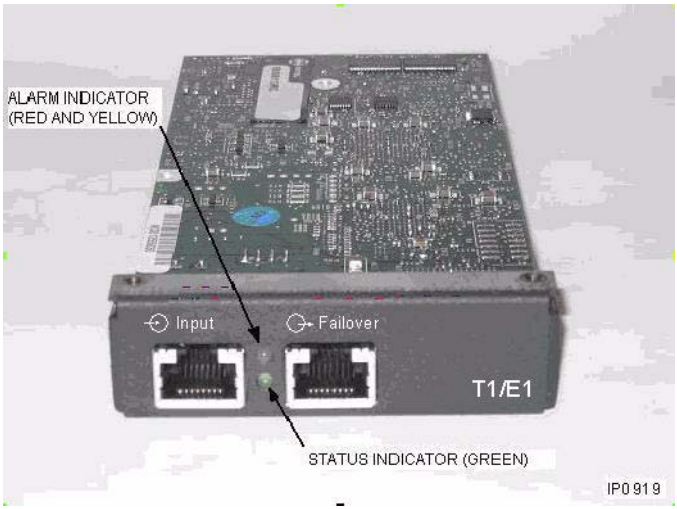


Figure 44: T1/E1 Combo Card - Resilient, from Release 7.0

Table 40: T1/E1 Combo Card Tip/Ring Assignments

Pin	Signal	NT/LT Settings	
		NT (Default)	LT
1	--	Rx Ring	Tx Ring
2	--	Rx Tip	Tx Tip
3	N/C	--	--
4	--	Tx Ring	Rx Ring
5	--	Tx Tip	Rx Tip
6	N/C	--	--
7	N/C	--	--
8	N/C	--	--
Note: Network and Line Termination settings are software-controlled. DO NOT move the jumpers. The settings apply to both connectors on the resilient card.			

Dual T1/E1 Framer

Figure 45 below shows the dual T1/E1 module, which provides embedded PRI and embedded T1/D4 functionality to a minimum 300 MHz controller.

Figure 45: Dual T1/E1 Framer

Quad BRI Framer

Figure 46 below shows the Quad BRI module which provides embedded BRI functionality to a minimum 300 MHz controller.

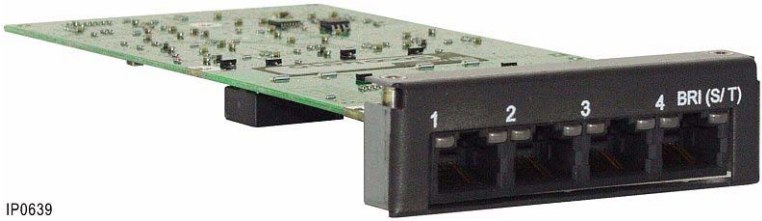


Figure 46: Quad BRI Framer

RJ-45 Pin Orientation

The RJ-45 connector is used for Ethernet, CIM, Music on Hold, Paging, RS-232 Maintenance ports, and E1 and T1 interfaces.

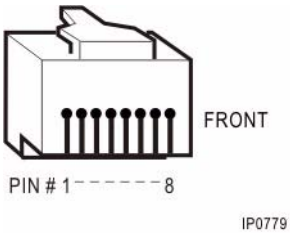


Figure 47: RJ-45 pin orientation

Analog Board (MX Controller)

The Analog Boards provide connectivity for analog trunks and telephones (POTS and On-Premise Station, ONS).

Table 41: Embedded Analog - Circuits/Ports

Circuits/Ports	Analog Main Board	Analog Option Board
LS CLASS Circuits	6	6
ONS CLASS Circuits	2	2
Power Fail Transfer Circuits	1	0
Music On Hold Port	1	0
Loudspeaker Port	1	0

Table 42: Embedded Analog Cabinet Configuration

Slot	Card Type
1	Hybrid LS ONS (6 LS + 2 ONS)
2	Hybrid LS ONS (6 LS + 2 ONS) optional
3	1 Port E & M Trunk
4	1 Port Loudspeaker Pager
5	No card present
6	ASU Controller
7	Copper I/F

Table 43: Embedded Analog Music on Hold Connector Pinout

Conductor	Signal	Virtual Circuit PLID
Shield	MOH_COM	4 1 3 1
Ring	MOH_1	
Tip	MOH_2	
Note: The Music On Hold port uses a 3.5mm stereo jack for input signal connection. It will also accept a 3.5mm mono plug. The two input signals are equivalent to the left and right channel signals from a stereo source and are combined internally into a single channel.		

Table 44: Embedded Analog Pager Connector Pinout

Pin	Signal	Virtual PLID
1	Common contact	
2	Normally closed contact	
3	Normally open contact	
4	Page1 (Tip)	4 1 4 1
5	Page2 (Ring)	4 1 4 1
6	No connection	
7	Not used	
8	Not used	

Note: The Paging port is an 8-pin RJ-45 connector on the rear panel of the MX controller. The paging port has a tip/ring pair for audio and contact closures for zone control. The normally closed contact opens when paging and the normally open contact closes when paging. See “RJ-45 Pin Orientation” on page 261.

Table 45: Embedded Analog Amphenol Connector Pinout

Pin	Color Code	Analog Main Board	Analog Option Board	PLID
26/1	W/BL, BL/W	ONS Ring/Tip 1 PFT #1		4-1-1-1
27/2	W/O, O/W	ONS Ring/Tip 2 PFT #2		4-1-1-2
28/3	W/G, G/W		ONS Ring/Tip 3	4-1-2-1
29/4	W/BR, BR/W		ONS Ring/Tip 4	4-1-2-2
30/5 - 35/10 NOT USED				
36/11	BK/BL, BL/BK	LS Ring/Tip 1 PFT #1		4-1-1-3
37/12	BK/O, O/BK	LS Ring/Tip 2 PFT #2		4-1-1-4
38/13	BK/G, G/BK	LS Ring/Tip 3		4-1-1-5
39/14	BK/BR, BR/BK	LS Ring/Tip 4		4-1-1-6
40/15	BK/S, S/BK	LS Ring/Tip 5		4-1-1-7
41/16	Y/BL, BL/Y	LS Ring/Tip 6		4-1-1-8
42/17	Y/O, O/Y		LS Ring/Tip 7	4-1-2-3
43/18	Y/G, G/Y		LS Ring/Tip 8	4-1-2-4
44/19	Y/BR, BR/Y		LS Ring/Tip 9	4-1-2-5
45/20	Y/S, S/Y		LS Ring/Tip 10	4-1-2-6

(Page 1 of 2)

Table 45: Embedded Analog Amphenol Connector Pinout (continued)

Pin	Color Code	Analog Main Board	Analog Option Board	PLID
46/21	V/BL, BL/V		LS Ring/Tip 11	4-1-2-7
47/22	V/O, O/V		LS Ring/Tip 12	4-1-2-8
48/23 - 50/25 NOT USED				
Note: Power Fail Transfer is provided internally between the LS trunks and the ONS lines. Preselected DTMF or rotary telephones can be connected directly to CO trunks in the event of system failure. In the event of a failure, the controller can switch phones on ONS circuits at PLID 4/1/1/1 and 4/1/1/2 to Central Office trunks at PLID 4/1/1/3 and 4/1/1/4.				
(Page 2 of 2)				

Analog Board (CX and MXe Controllers)

Analog Boards provide connectivity for analog trunks and telephones.

Table 46: Embedded Analog - Circuits/Ports

Circuits/Ports	Analog Main Board CX and MXe	Analog Option Board CX only
LS CLASS Circuits	6	6
ONS CLASS Circuits	4	4
Power Fail Transfer Circuits	2	2
Music On Hold Port	1	0
Loudspeaker Port (Page)	1	0

Table 47: Analog Main Board/Analog Option Board Port Assignment

Analog Option Board Ports (CX only)												
1	1/2	4	3	2	1		1	2	3	4	5	6
PLIDs		4124	4123	4122	4121		4125	4126	4127	4128	4129	41210
Analog Main Board Ports (CX and MXe)												
Page	**Relay**	**ONS Ports**					**LS Ports**					
1	1/2	4	3	2	1		1	2	3	4	5	6
4141		4114	4113	4112	4111		4115	4116	4117	4118	4119	41110
Note: AMB PLIDs - PFT#1 ONS 4-1-1-1 -> LS 4-1-1-5; PFT#2 ONS 4-1-1-2 -> LS 4-1-1-6												

Table 48: Analog Main Board/Analog Option Board Pinouts

Port	Pin Number	Function
LS 1 - 6	3	Ring
	4	Tip
ONS 1 - 4	3	Ring
	4	Tip
ONS 3 - 4	2	Contact sensor
	5	Contact sensor
Relay 1/2	3	RLY1_Common
	4	RLY1_no
	6	RLY1_nc
	2	RLY2_Common
	5	RLY2_no
Paging	3	Paging signal
	4	Paging signal
	2	Paging relay common
	5	No paging contact
	1	No paging contact

Table 49: Embedded Analog Music on Hold Connector Pinout

Conductor	Signal	Virtual Circuit PLID
Shield	MOH_COM	4 1 3 1
Ring	MOH_1	
Tip	MOH_2	
Note: The Music On Hold port requires a 3.5mm stereo jack for input signal connection. The two input signals are equivalent to the left and right channel signals from a stereo source and are combined internally into a single channel.		

Controller Alarm Port Pinouts

Table 50: Controller Alarm Port Pinout

Pin	Signal	Pin	Signal
1	Critical Alarm	6	Not Used
2	Critical Alarm Return	7	Minor Alarm
3	Not Used	8	Minor Alarm Return
4	Major Alarm	9	Not Used
5	Major Alarm Return		

Controller Remote Alarm Behavior

Table 51: Controller Remote Alarm Behavior

Action	Behavior
Power-up or push-button reset	Remote alarms are enabled by default and the LED is turned off. Press the remote alarm button to disable remote alarms. Disabled when the LED is ON.
Software-activated reboot	Remote alarms remain in the state that they were in prior to the reboot.
Software Install or Upgrade	If remote alarms are disabled, an install/upgrade may enable the alarms.
Power failure	When the system comes back up, the remote alarm will be enabled, the default.

Network Services Units

The Network Services Unit provides connectivity to digital trunks.

There are three variants of the NSUs:

- Universal NSU
- R2 NSU
- BRI NSU

Universal/R2 NSU

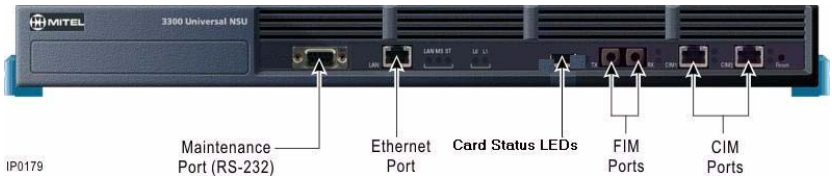


Figure 48: Universal NSU—Front Panel

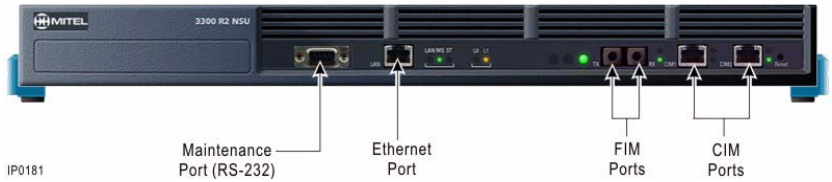


Figure 49: R2 NSU—Front Panel

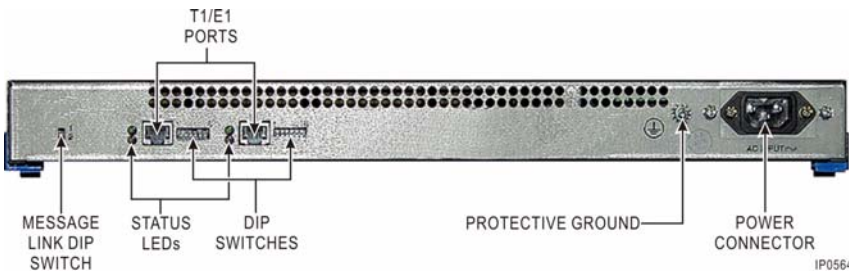


Figure 50: Universal/R2 NSU—Back Panel

Universal and R2 NSU DIP Switch Settings

Table 52: Message Link DIP Switch Setting

DIP Switch	Use	Notes
Rear panel, left side	Primary NSU	Set to 1 (up). Connected to the controller
	Secondary NSU	Set to 2 (down). Connected to another NSU

Table 53: T1/E1 Ports DIP Switches Defined

DIP Switch	Use	Notes
1	Tx Ground	Ground when down; floating when up.
2	Rx Ground	Ground when down; floating when up.
3	Impedance selector #1	120 ohm (enabled when down).
4	Impedance selector #2	100 ohm (enabled when down).
5	Impedance selector #3	75 ohm (enabled when down).
6	LT/NT selector	Up for NT; down for LT.

Table 54: T1/E1 Ports DIP Switch Settings

Impedance (ohms)	Trunk Mode	1 Tx Gnd	2 Rx Gnd	3 120 ohm	4 100 ohm	5 75 ohm	6 LT/NT
100	T1 (T1/D4)	Up	Up	Up	Down	Up	Up/Down
120	E1 (PRI)	Up	Up	Down	Up	Up	Up/Down
75	E1 (R2)	Note	Note	Up	Up	Down	Up/Down

Note: The **Ground** setting is site-dependent. Normally, Tx is grounded and Rx is not grounded, but that depends on which remote connection is grounded. These switches are used only with the coaxial adapter (BNC adapter required); leave up (floating) for twisted pair connection to the E1 port.

Note: See for Table 58 on page 270 for T1 and E1 Connector Pin Allocation for setting dip switch 6, LT/NT.

Universal and R2 NSU Pin Allocations

Table 55: CIM Port Connector (Controller, NSU and ASU)

RJ-45 Connector Pin	Signal Name
1	RX+
2	RX-
3	TX+
4	Not used
5	Not used
6	TX-
7	Not used
8	Not used

Note: The Universal ASU connects to the controller over a Category 5 Universal Twisted Pair (UTP) crossover cable through a CIM interface. The Category 5 cable is of the same type used for Ethernet connections and within the cable twisted pairs are arranged as: 1,2: 3,6; 4,5; 7,8. Each tied pair is connected to a 75 ohm resistor. The Universal ASU can be located up to 30 meters (98.4 feet) away from the controller. The interface employs a single standard 8-pin modular jack consisting of 2 balanced signal pairs and is located on the front of the unit.

Table 56: Ethernet Connector

RJ-45 Connector Pin	Signal Name
1	TX+
2	TX-
3	RX+
4	Not used
5	Not used
6	RX-
7	Not used
8	Not used

Table 57: RS-232 Maintenance Connector

RJ-45 Connector Pin	Signal Name
1	DCD (data carrier detector)
2	RXD (receive data)
3	TXD (transmit data)
4	DTR (data terminal ready)
5	GND (ground)
6	Not used
7	RTS (ready to send)
8	CTS (clear to send)
9	Not used

Table 58: T1 and E1 Connector Pin Allocation

RJ-45 Connector Pin	Signal Name	
	NT Mode: Switch-6 UP	LT Mode: Switch-6 DOWN
1	RX Ring	TX Ring
2	RX Tip	TX Tip
3	Unused	Unused
4	TX Ring	RX Ring
5	TX Tip	RX Tip
6	Unused	Unused
7	Unused	Unused
8	Unused	Unused

Table 59: NSU Trunk Type Programming Information

NSU	Protocol	Link Descriptor (Integrated Access)	MSDN Trunk Circuit Descriptor Type
Universal T1/E1	T1/E1 PRI/QSIG	ISDN Node	Universal T1 Universal E1
Universal T1	T1 E&M	T1D4	Universal T1
Universal T1/E1	T1/E1 MSDN	DPNSS	Universal T1 Universal E1
R2	R2	ISDN Node	R2

BRI NSU

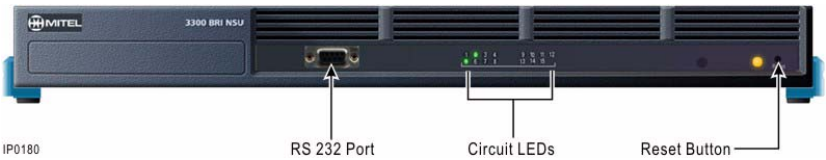


Figure 51: BRI NSU—Front Panel

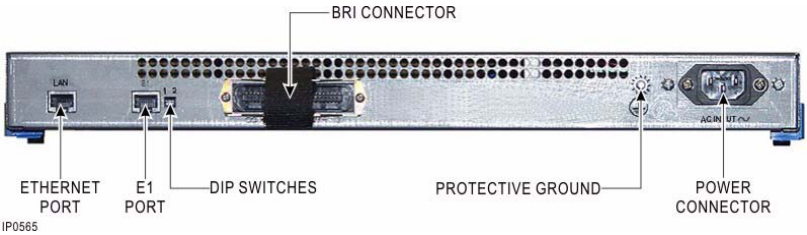


Figure 52: BRI NSU—Back Panel

Table 60: BRI Connector Pinout (Amphenol 25-pin)

Pin	Signal	Pin	Signal	Pin	Signal
1	T1	11	T11	31	R6
2	T2	12	T12	32	R7
3	T3	13	T13	33	R8
4	T4	14	T14	34	R9
5	T5	15	T15	35	R10
6	T6	26	R1	36	R11
7	T7	27	R2	37	R12
8	T8	28	R3	38	R13
9	T9	29	R4	39	R14
10	T10	30	R5	40	R15

BRI NSU DIP Switch Settings

Table 61 below shows the settings for the CEPT port DIP switch for the BRI NSU.

Table 61: CEPT Mode - E1 Port DIP Switch Settings

Switch	Use	Setting	Notes
1	Tx Ground	Up: Floating Down: Ground	Not required for RJ-45 connector.
2	Rx Ground	Up: Floating Down: Ground	Not required for RJ-45 connector
Note: This setting is site-dependent. Normally Tx is grounded and Rx is not grounded, but that depends on which remote connection is grounded. These switches are used only with the coaxial adapter; leave up (floating) with twisted pair connection. Not required for RJ-45 connector.			

Analog Services Unit

The Analog Services Unit (ASU) provides connectivity for analog trunks and telephones (POTS and On-Premise Station, ONS). There are three variants of 3300 ASUs:

- ASU
- Universal ASU
- ASU II (only on systems running Release 7.0 and later).

For information specific to embedded analog, refer to page 262.

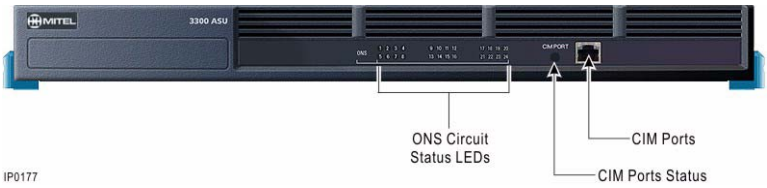


Figure 53: ASU—Front Panel

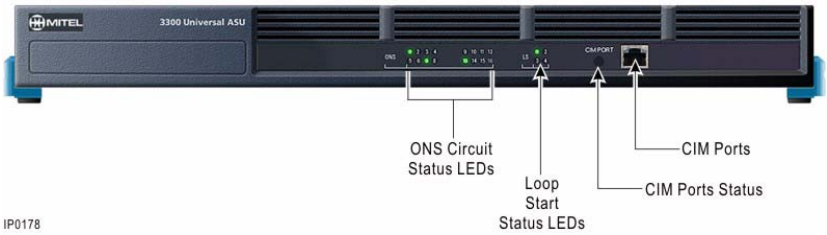


Figure 54: Universal ASU—Front Panel

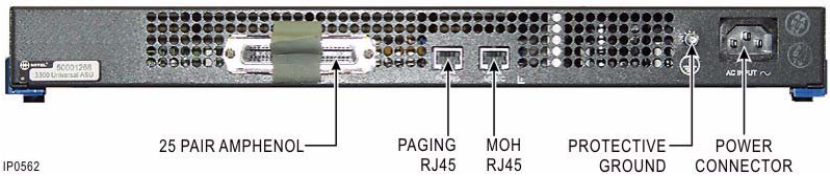


Figure 55: Universal ASU—Back Panel

Figure 56: ASU II—Front Panel with a Line Card

Figure 57: ASU II—Back Panel

There are two line card available for the ASU II:

- 16 port ONS card
- 4 + 12 port Combo card (4 LS trunks and 12 ONS lines).

Table 62: ASU II Card Lock Latch Color Code

Card Type	Latch Color
16 Port ONS Card	White
4 + 12 Port Combo	Green

Table 63: ASU II 25-Pair Male D-Type Connector Pinout

Pin	Color Code	16 port ONS	PLID	4 + 12 port Combo	PLID
26/1	W/BL, BL/W	ONS Tip/Ring 1	n 1 x 1	ONS Tip/Ring 1	n 1 x 1
27/2	W/O, O/W	ONS Tip/Ring 2	n 1 x 2	ONS Tip/Ring 2	n 1 x 2
28/3	W/G, G/W	ONS Tip/Ring 3	n 1 x 3	ONS Tip/Ring 3	n 1 x 3
29/4	W/BR, BR/W	ONS Tip/Ring 4	n 1 x 4	ONS Tip/Ring 4	n 1 x 4
30/5	W/S, S/W	ONS Tip/Ring 5	n 1 x 5	ONS Tip/Ring 5	n 1 x 5
31/6	R/BL, BL/R	ONS Tip/Ring 6	n 1 x 6	ONS Tip/Ring 6	n 1 x 6
32/7	R/O, O/R	ONS Tip/Ring 7	n 1 x 7	ONS Tip/Ring 7	n 1 x 7
33/8	R/G, G/R	ONS Tip/Ring 8	n 1 x 8	ONS Tip/Ring 8	n 1 x 8
34/9	R/BR, BR/R	ONS Tip/Ring 9	n 1 x 9	ONS Tip/Ring 9	n 1 x 9
35/10	R/S, S/R	ONS Tip/Ring 10	n 1 x 10	ONS Tip/Ring 10	n 1 x 10
36/11	BK/BL, BL/BK	ONS Tip/Ring 11	n 1 x 11	ONS Tip/Ring 11	n 1 x 11
37/12	BK/O, O/BK	ONS Tip/Ring 12	n 1 x 12	ONS Tip/Ring 12	n 1 x 12
38/13	BK/G, G/BK	ONS Tip/Ring 13	n 1 x 13	N/C	
39/14	BK/BR, BR/BK	ONS Tip/Ring 14	n 1 x 14	N/C	
40/15	BK/S, S/BK	ONS Tip/Ring 15	n 1 x 15	N/C	
41/16	Y/BL, BL/Y	ONS Tip/Ring 16	n 1 x 16	N/C	
42/17	Y/O, O/Y	N/C		N/C	
43/18	Y/G, G/Y	N/C		N/C	
44/19	Y/BR, BR/Y	N/C		N/C	
45/20	Y/S, S/Y	N/C		N/C	
46/21	V/BL, BL/V	N/C		LS Ring/Tip 1	n 1 x 13
47/22	V/O, O/V	N/C		LS Ring/Tip 2	n 1 x 14
48/23	V/G, G/V	N/C		LS Ring/Tip 3	n 1 x 15
49/24	V/BR, BR/V	N/C		LS Ring/Tip 4	n 1 x 16
50/25	V/S, S/V	N/C		N/C	

Note: In the PLID column, n represents the unit number and x represents the number of the slot in which the card is installed (either one or two).

Table 64: ASU 25-Pair D-Type Connector Pinout

Pin	Color Code	ASU	PLID	Universal ASU	PLID
26/1	W/BL, BL/W	ONS Ring/Tip 1	n 1 1 1	ONS Ring/Tip 1	n 1 1 1
27/2	W/O, O/W	ONS Ring/Tip 2	n 1 1 2	ONS Ring/Tip 2	n 1 1 2
28/3	W/G, G/W	ONS Ring/Tip 3	n 1 1 3	ONS Ring/Tip 3	n 1 1 3
29/4	W/BR, BR/W	ONS Ring/Tip 4	n 1 1 4	ONS Ring/Tip 4	n 1 1 4
30/5	W/S, S/W	ONS Ring/Tip 5	n 1 1 5	ONS Ring/Tip 5	n 1 1 5
31/6	R/BL, BL/R	ONS Ring/Tip 6	n 1 1 6	ONS Ring/Tip 6	n 1 1 6
32/7	R/O, O/R	ONS Ring/Tip 7	n 1 1 7	ONS Ring/Tip 7	n 1 1 7
33/8	R/G, G/R	ONS Ring/Tip 8	n 1 1 8	ONS Ring/Tip 8	n 1 1 8
34/9	R/BR, BR/R	ONS Ring/Tip 9	n 1 2 1	ONS Ring/Tip 9	n 1 2 1
35/10	R/S, S/R	ONS Ring/Tip 10	n 1 2 2	ONS Ring/Tip 10	n 1 2 2
36/11	BK/BL, BL/BK	ONS Ring/Tip 11	n 1 2 3	ONS Ring/Tip 11	n 1 2 3
37/12	BK/O, O/BK	ONS Ring/Tip 12	n 1 2 4	ONS Ring/Tip 12	n 1 2 4
38/13	BK/G, G/BK	ONS Ring/Tip 13	n 1 2 5	ONS Ring/Tip 13	n 1 2 5
39/14	BK/BR, BR/BK	ONS Ring/Tip 14	n 1 2 6	ONS Ring/Tip 14	n 1 2 6
40/15	BK/S, S/BK	ONS Ring/Tip 15	n 1 2 7	ONS Ring/Tip 15	n 1 2 7
41/16	Y/BL, BL/Y	ONS Ring/Tip 16	n 1 2 8	ONS Ring/Tip 16	n 1 2 8
42/17	Y/O, O/Y	ONS Ring/Tip 17	n 1 3 1	LS Ring/Tip 1	n 1 3 1
43/18	Y/G, G/Y	ONS Ring/Tip 18	n 1 3 2	LS Ring/Tip 1-1	1 MPD
44/19	Y/BR, BR/Y	ONS Ring/Tip 19	n 1 3 3	LS Ring/Tip 2	n 1 3 2
45/20	Y/S, S/Y	ONS Ring/Tip 20	n 1 3 4	LS Ring/Tip 1-2	2 MPD
46/21	V/BL, BL/V	ONS Ring/Tip 21	n 1 3 5	LS Ring/Tip 3	n 1 3 3
47/22	V/O, O/V	ONS Ring/Tip 22	n 1 3 6	LS Ring/Tip 1-3	3 MPD
48/23	V/G, G/V	ONS Ring/Tip 23	n 1 3 7	LS Ring/Tip 4	n 1 3 4
49/24	V/BR, BR/V	ONS Ring/Tip 24	n 1 3 8	LS Ring/Tip 1-4	4 MPD
50/25	V/S, S/V	N/C		N/C	

Note: In the PLID column, n represents the unit number: LX is 2 - 5; MX is 2 and 3. The LS Ring/Tip 1-n connections are used in the UK for Meter Pulse Detection (MPD). These ports should be wired across the corresponding LS Ring/Tip connection of the trunk. We recommend that the MPD connections are made at the last hard wired point.

Table 65: ASU II Combo Card SFT/PFT Port Connections

LS Port	ONS Port
1	1
2	2
3	3
4	4
Note: Up to four SFT/PFT calls can occur at the same time between pairs of LS and ONS ports. ONS is supported against an LS trunk.	

Table 66: Universal ASU Music on Hold Connector Pinout

Pin	Signal	Virtual Circuit
1/2	Tip/Ring 1	*n* 1 4 1
3/6	Tip/Ring 2	*n* 1 4 2
4/5	Tip/Ring 3	*n* 1 4 3
7/8	Tip/Ring 4	*n* 1 4 4
Note: CIM 1: *n* = 2. CIM 2: *n* = 3. **Note**: The four MOH tip/ring pairs occupy an 8-pin female modular jack on the rear panel. MOH can be assigned to either of the first two ports on a Universal ASU E&M card.		

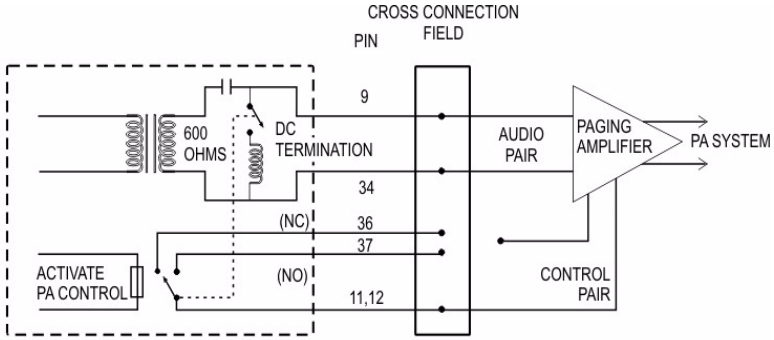
Table 67: Universal ASU Pager Connector Pinout

Pin	Signal	Zone	Virtual Circuit
1	Tip	00	n 1 5 1
2	Ring	00	n 1 5 1
3	Common contact	00	
4	Tip	01	n 1 5 2
5	Ring	01	n 1 5 2
6	Normally open contact	00	
7	Common contact	01	
8	Normally open contact	01	
Note: CIM 1: *n* = 2. CIM 2: *n* = 3. **Note**: The Paging port is a standard 8-pin modular RJ-45 connector on the rear panel. **Note**: Each paging port has a tip/ring pair for audio and a second tip/ring pair contact closures for zone control. The contact closes when paging on zones.			

5485 IP Paging Unit

Table 68: 5485 IP Paging Unit Pinout

Pin	Color Code	Signal
9	BR/R	Audio output, Positive
34	R/BR	Audio output, Negative
36	BK/BL	Relay Closure (normally closed)
37	BK/O	Relay Closure (normally open)
11	BL/BK	Page Control input
12	O/BK	



NOTE 1. All wiring must be done in accordance with the National Electrical Code (USA) or Canadian Electric Code and/or local electrical inspection authorities.

NOTE 2. Relay contacts may be connected only to a low voltage secondary circuit (60V@100mA max.). Under no circumstances should these contacts be used to switch primary AC power.

LL0036

Figure 58: 5485 IP Paging Unit Cross Connection

Peripheral Cabinet

Each peripheral cabinet contains peripheral interface cards providing ONS and/or DNI ports. Each cabinet has one peripheral switch controller (PSC) card for control of peripheral cards and one fiber interface module (FIM) that provides connection to the controller.

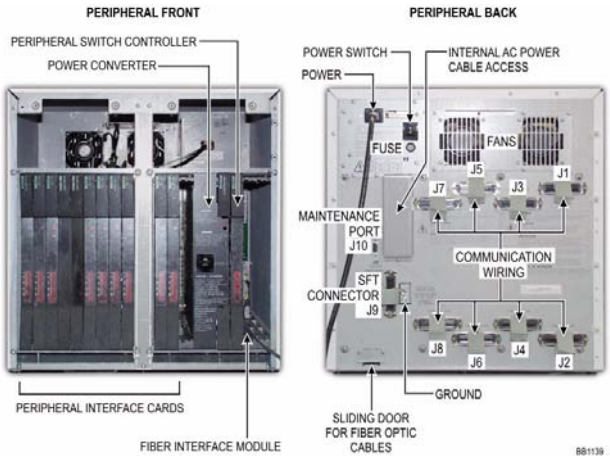
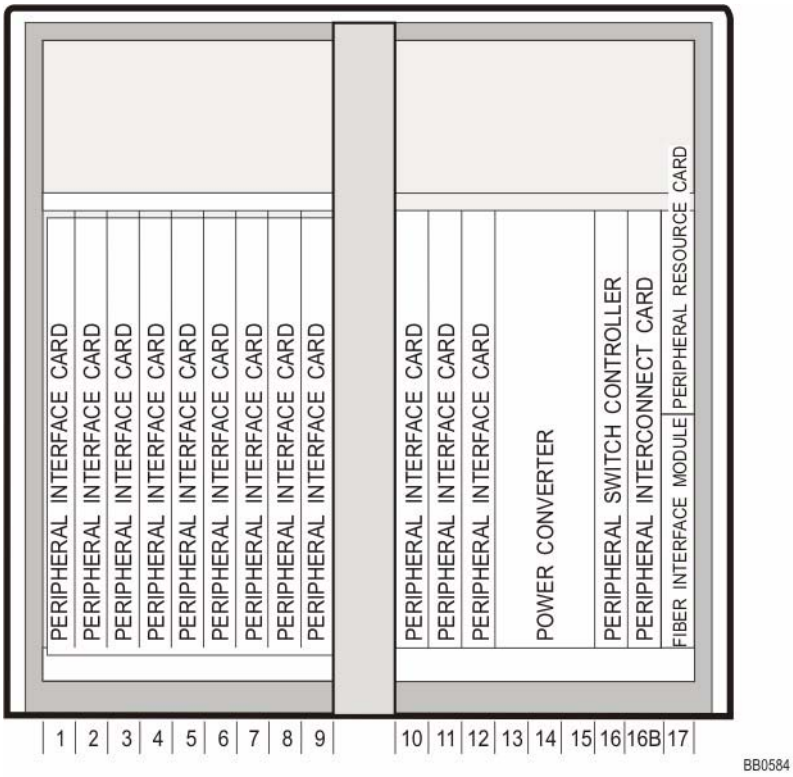


Figure 59: Peripheral Cabinet Components

The following peripheral interface cards can be installed in peripheral cabinets (some cards are only available in specific countries):

- DNI line card
- LS/GS trunk card
- ONS CLASS/CLIP line card
- ONS line card
- E&M tie trunk card
- OPS line card
- DID/loop tie trunk card.

Peripheral Cabinet Card Layout



Fiber Interface Module

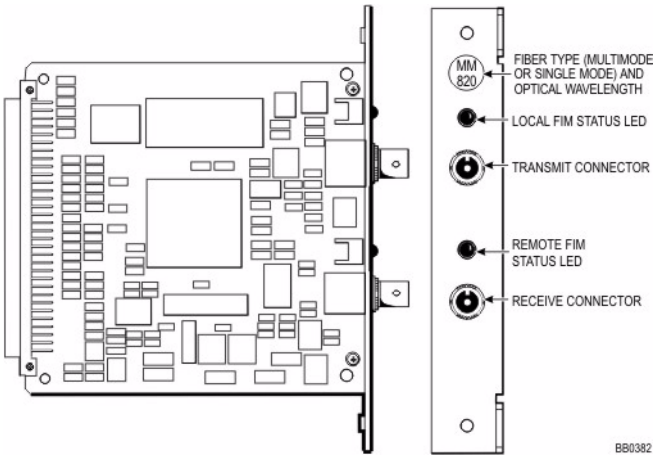


Figure 60: Peripheral Cabinet FIM

E&M Trunk Card

CONFIGURATION SERIAL NO.	SWITCH POSITION (NOTE) SN-1	SWITCH POSITION (NOTE) SN-2	CIRCUIT CONFIGURATION	TYPES OF INTERFACE CIRCUITS: SIGNAL CARRIER SET TYPES	TYPES OF INTERFACE CIRCUITS: COLLOCATED TRUNK TYPES
1	A	B	-48V, M, N/C, SB, SG, -48V, E, E	TYPE I	NONE
2	B	A	M, M, SB, SG, -48V, E, E	TYPE II TYPE IV	TYPE II TYPE IV
3	B	B	M, N/C, SB, SG, -48V, E, E	TYPE V	TYPE I TYPE III TYPE V

NOTE: SWITCH SECTIONS ARE SN-1 AND SN-2, WHERE N IS THE PARTICULAR TRUCK CIRCUIT NUMBER ON THE CARD.

BB0149

Figure 61: Switchable Interface Configurations

E&M Trunk Card

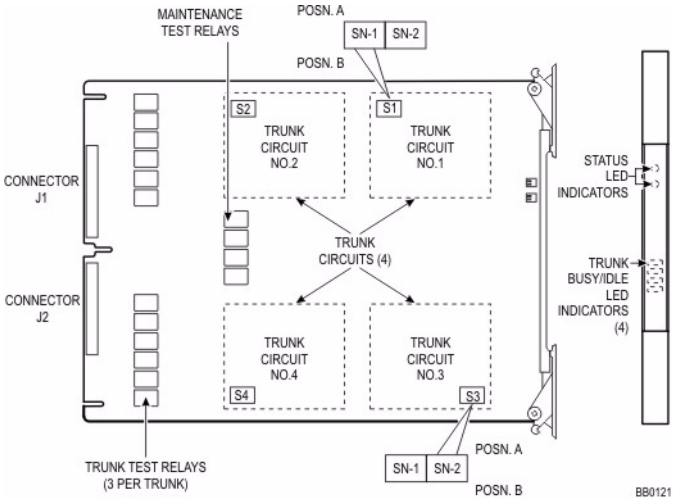


Figure 62: SN-1 and SN-2 Switches

LG/GS Trunk Card

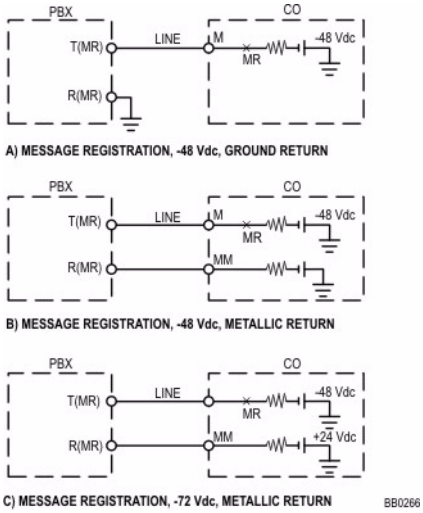


Figure 63: Message Registration Arrangements

OPS Line Card

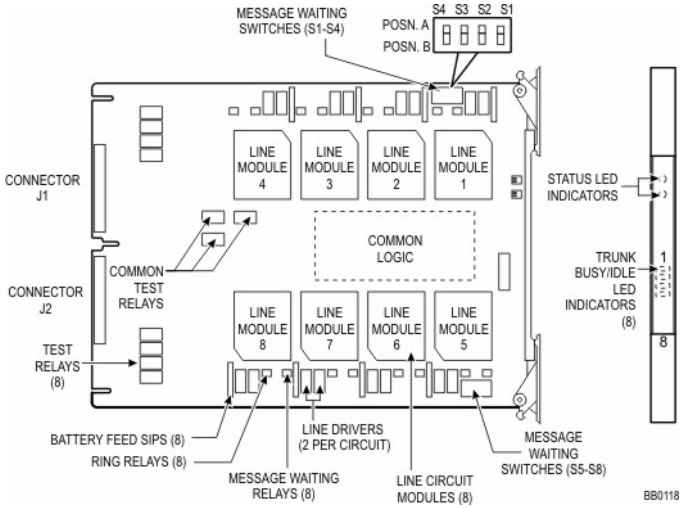


Figure 64: OPS Line Card

About Peripheral Interface Cabling

Peripheral equipment is connected to the interface circuits of the system via a cross-connect field. Peripheral interface cards are connected to the cross-connect field by 25-pair cables. Cables terminate at the node on 50-pin jacks, J1 through J8, with the number of cables being dependent on the quantity and type of interface cards installed in the node.

Jacks J1 through J8 are hardwired to backplane connectors in slots 1 through 12 to form four slot groups, each comprising three adjacent cards and each associated with a pair of jacks. Two adjacent slot groups are shown in backplane connector arrangements. The circuits of interface cards contained in a slot group are evenly distributed to the relevant pair of jacks, such that, half the circuits of each card in a group are connected to the odd-numbered jack and half to the even-numbered jack. Peripheral wiring (backplane) details the hardwire connections between one slot group and the associated jacks. The wiring sequence is identical for the remaining three slot groups.

Cable plugs P1 through P8 are secured to J1 through J8 with hook and loop type fasteners. The type of equipment used and the layout of the cross-connect field cables is at the discretion of the installation company. Installation information for such equipment must be obtained from the equipment manufacturer.

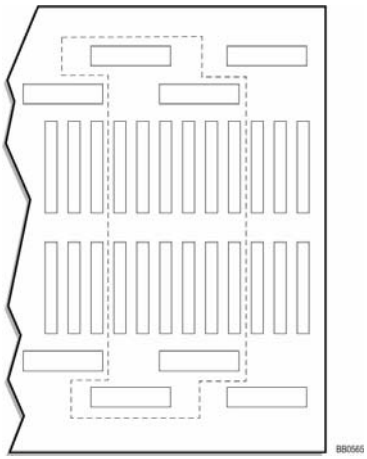


Figure 65: Peripheral Cabinet Backplane Connectors

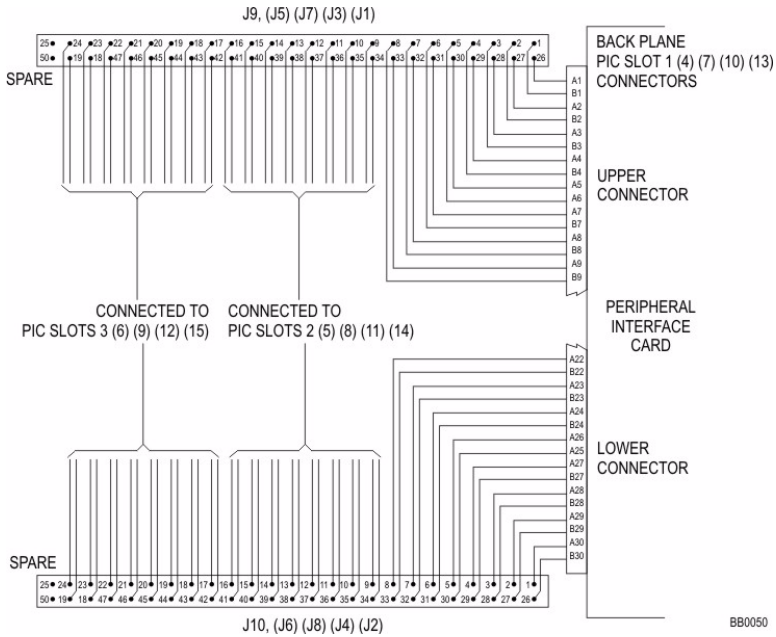


Figure 66: Peripheral Cabinet Backplane Wiring

Peripheral Cabinet Cabling

The following three tables show the pinout signals of the interface cards as they appear on J1 through J8. The following abbreviations are used in the tables:

- ONS L C: ONS line card and ONS CLASS/CLIP line card
- OPS L C: OPS line card
- LS/GS trunk: loop start/ground start trunk card
- E&M trunk: E&M trunk card
- DID/LT trunk: direct inward dialing/loop tie trunk card
- DID/2 trunk: direct inward dialing
- COV L C: SUPERSET 4 line card
- DNI L C: digital network interface line card.

Use the appropriate tables to cable the peripheral cabinet card connectors to the main distribution frame.

Tip: When cabling the SX-2000 MicroLIGHT node connectors, use the cabling tables that correspond to the peripheral interface card slot in the node.

Connectors for customer supplied 25-pair cables terminating on peripheral backplane (to MDF) and SFT unit (to MDF) use AMP Champ or equivalent cable connectors:

- 50-pin RS (receptacle - screw lock)
- female
- screw lock
- 90 tapered slide-on hood.

Table 69: Peripheral Cabinet Card Slot Pinouts (Cards 1, 4, 7 and 10)

Peripheral Backplane Jacks	Pin	Color Code	ONS L C	OPS L C	LS/GS Trunk	E&M Trunk	DID/LT Trunk	DID/2 Trunk	COV L C	DNI L C
J1 (slot 1) J3 (slot 4) J5 (slot 7) J7 (slot 10)	26	W/BL	1T	1T	1T	1T	1T	1T	1T	1T
	1	BL/W	1R	1R	1R	1R	1R	1R	1R	1R
	27	W/O	2T	1MWB	1T(MR)	1T1			2T	2T
	2	O/W	2R	1MWA	1R(MR)	1R1			2R	2R
	28	W/G	3T	2T	2T	1E	2T	2T	3T	3T
	3	G/W	3R	2R	2R	1SG	2R	2R	3R	3R
	29	W/BR	4T	2MWB	2T(MR)	1M			4T	4T
	4	BR/W	4R	2MWA	2R(MR)	1SB			4r	4R
	30	W/S	5T	3T	3T	2T		3T	5T	5T
	5	S/W	5R	3R	3R	2R		3R	5R	5R
	31	R/BL	6T	3MWB	3T(MR)	2T1			6T	6T
	6	BL/R	6R	3MWA	3R(MR)	2R1			6R	6R
	32	R/O	7T	4T	4T	2E		4T		7T
	7	O/R	7R	4R	4R	2SG		4R		7R
	33	R/G	8T	4MWB	4T(MR)	2M				8T
	8	G/R	8R	4MWA	4R(MR)	2SB				8R
J2 (slot 1) J4 (slot 4) J6 (slot 7) J8 (slot 10)	26	W/BL	9T	5T	5T	3T	3T	5T	7T	9T
	1	BL/W	9R	5R	5R	3R	3R	5R	7R	9R
	27	W/O	10T	5MWB	5T(MR)	3T1			8T	10T
	2	O/W	10R	5MWA	5R(MR)	3R1			*R	10R
	28	W/G	11T	6T	6T	3E	4T	6T	9T	11T
	3	G/W	11R	6R	6R	3SG	4R	6R	9R	11R
	29	W/BR	12T	6MWB	6T(MR)	3M			10T	12T
	4	BR/W	12R	6MWA	6R(MR)	3SB			10R	12R
	30	W/S	12T	7T	7T	4T		7T	11T	13T
	5	S/W	13R	7R	7R	43R		7R	11R	13R
	31	R/BL	14T	7MWB	7T(MR)	4T1			12T	14T
	6	BL/R	14R	7MWA	7R(MR)	4R1			12R	14R
	32	R/O	15T	8T	8T	4E		8T		15T
	7	O/R	15R	8R	8R	5SG		8R		15R
	33	R/G	16T	8MWB	8T(MR)	4M				16T
	8	G/R	16R	8MWA	8R(MR)	4SB				16R

Table 70: Peripheral Cabinet Card Slot Pinouts (Card 2, 5, 8 and 11)

Peripheral Backplane Jacks	Pin	Color Code	ONS L C	OPS L C	LS/GS Trunk	E&M Trunk	DID/LT Trunk	DID/2 Trunk	COV L C	DNI L C
J1 (slot 2) J3 (slot 5) J5 (slot 8) J7 (slot 11)	34	R/BR	1T	1T	1T	1T	1T	1T	1T	1T
	9	BR/R	1R	1R	1R	1R	1R	1R	1R	1R
	35	R/S	2T	1MWB	1T(MR)	1T1			2T	2T
	10	S/R	2R	1MWA	1R(MR)	1R1			2R	2R
	36	BK/BL	3T	2T	2T	1E	2T	2T	3T	3T
	11	BL/BK	3R	2R	2R	1SG	2R	2R	3R	3R
	37	BK/O	4T	2MWB	2T(MR)	1M			4T	4T
	12	O/BK	4R	2MWA	2R(MR)	1SB			4R	4R
	38	BK/G	5T	3T	3T	2T		3T	5T	5T
	13	G/BK	5R	3R	3R	2R		3R	5R	5R
	39	BK/BR	6T	3MWB	3T(MR)	2T1			6T	6T
	14	BR/BK	6R	3MWA	3R(MR)	2R1			6R	6R
	40	BK/S	7T	4T	4T	2E		4T		7T
	15	S/BK	7R	4R	4R	2SG		4R		7R
	41	Y/BL	8T	4MWB	4T(MR)	2M				8T
	16	BL/Y	8R	4MWA	4R(MR)	2SB				8R
J2 (slot 2) J4 (slot 5) J6 (slot 8) J8 (slot 11)	34	R/BR	9T	5T	5T	3T	3T	5T	7T	9T
	9	BR/R	9R	5R	5R	3R	3R	5R	7R	9R
	35	R/S	10T	5MWB	5T(MR)	3T1			8T	10T
	10	S/R	10R	5MWA	5R(MR)	3R1			8R	10R
	36	BK/BL	11T	6T	6T	3E	4T	6T	9T	11T
	11	BL/BK	11R	6R	6R	3SG	4R	6R	9R	11R
	37	BK/O	12T	6MWB	6T(MR)	3M			10T	12T
	12	O/BK	12R	6MWA	6R(MR)	3SB			10R	12R
	38	BK/G	13T	7T	7T	4T		7T	11T	13T
	13	G/BK	13R	7R	7R	43R		7R	11R	13R
	39	BK/BR	14T	7MWB	7T(MR)	4T1			12T	14T
	14	BR/BK	14R	7MWA	7R(MR)	4R1			12R	14R
	40	BK/S	15T	8T	8T	4E		8T		15T
	15	S/BK	15R	8R	8R	4SG		8R		15R
	41	Y/BL	16T	8MWB	8T(MR)	4M				16T
	16	BL/Y	16R	8MWA	8R(MR)	4sb				16R

Table 71: Peripheral Cabinet Card Slot Pinouts (Cards 3, 6, 9 and 12)

Peripheral Backplane Jacks	Pin	Color Code	ONS L C	OPS L C	LS/GS Trunk	E&M Trunk	DID/LT Trunk	DID/2 Trunk	COV L C	DNI L C
	42	Y/O	1T	1T	1T	1T	1T	1T	1T	1T
	17	0/Y	1R	1R	1R	1R	1R	1R	1R	1R
	43	Y/G	2T	1MWB	1T(MR)	1T1			2T	2T
	18	G/Y	2R	1MWA	1R(MR)	1R1			2R	2R
	44	Y/BR	3T	2T	2T	1E	2T	2T	3T	3T
	19	BR/Y	3R	2R	2R	1SG	2R	2R	3R	3R
J1 (slot 3)	45	Y/S	4T	2MWB	2T(MR)	1M			4T	4T
J3 (slot 6)	20	S/Y	4R	2MWA	2R(MR)	1SB			4R	4R
	46	V/BL	5T	3T	3T	2T		3T	5T	5T
J5 (slot 9)	21	BL/V	5R	3R	3R	2R		3R	5R	5R
	47	V/O	6T	3MWB	3T(MR)	2T1			6T	6T
J7 (slot 12)	22	O/V	6R	3MWA	3R(MR)	2R1			6R	6R
	48	V/G	7T	4T	4T	2E		4T		7T
	23	G/V	7R	4R	4R	2SG		4R		7R
	49	V/BR	8T	4MWB	4T(MR)	2M				8T
	24	BR/V	8R	4MWA	4R(MR)	2SB				8R
	50	—	—	—	—	Spare	—	—	—	—
	25	—	—	—	—	Spare	—	—	—	—
	42	Y/O	9T	5T	5T	3T	3T	5T	7T	9T
	17	0/Y	9R	5R	5R	3R	3R	5R	7R	9R
	43	Y/G	10T	5MWB	5T(MR)	3T1			8T	10T
	18	G/Y	10R	5MWA	5R(MR)	3R1			8R	10R
	44	Y/BR	11T	6T	6T	3E	4T	6T	9T	11T
J2 (slot 3)	19	BR/Y	11R	6R	6R	3SG	4R	6R	9R	11R
J4 (slot 6)	45	Y/S	12T	6MWB	6T(MR)	3M			10T	12T
	20	S/Y	12R	6MWA	6R(MR)	3SB			10R	12R
J6 (slot 9)	46	V/BL	13T	7T	7T	4T		7T	11T	13T
	21	BL/V	13R	7R	7R	43R		7R	11R	13R
J8 (slot 12)	47	V/O	14T	7MWB	7T(MR)	4T1			12T	14T
	22	O/V	14R	7MWA	7R(MR)	4R1			12R	14R
	48	V/G	15T	8T	8T	4E		8T		15T
	23	G/V	15R	8R	8R	4SG		8R		15R
	49	V/BR	16T	8MWB	8T(MR)	4M				16T
	24	BR/V	16R	8MWA	8R(MR)	4sb				16R
	50	—	—	—	—	Spare	—	—	—	—
	25	—	—	—	—	Spare	—	—	—	—

Digital Service Unit

The Digital Service Unit (DSU) provides digital trunk interfaces for public or private network access, and specialized digital functions (such as messaging and ISDN service).

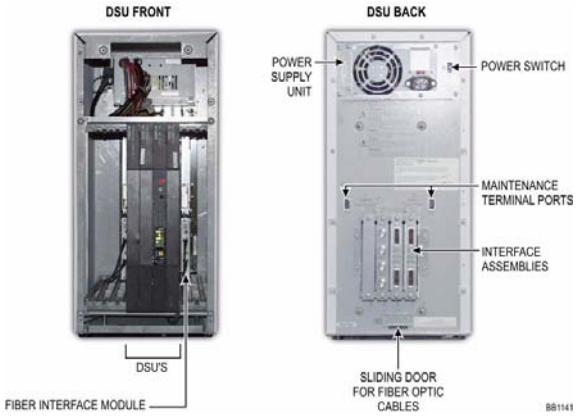
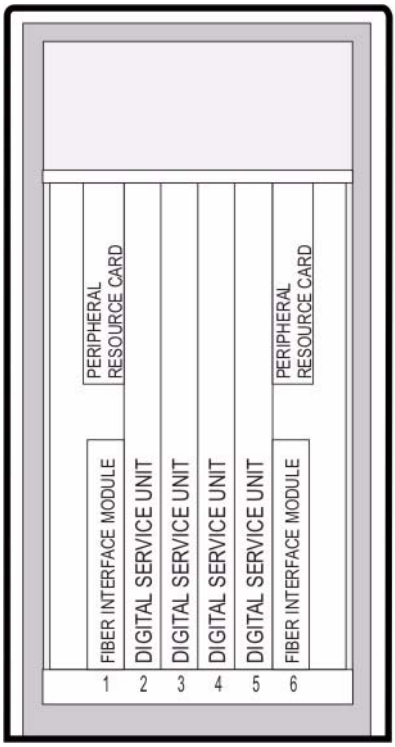


Figure 67: DSU Components

The following cards can be installed in a DSU (some cards are only available in specific countries):

- DS1 formatter
- CEPT formatter
- T1/E1 digital trunk formatter
- BRI card (6 circuits)
- BRI card (15 circuits)
- Euro PRI card
- NA PRI card
- R2 card.

DSU Card Layout



DS1 Formatter

Table 72: DS1 DB-15 Connector Pinout

Pin	Color Code	Description
1/9	W/O, O/W	Tx Tip/Ring
2/4	W/G, G/W	Frame Ground
3/11	W/BL, BL/W	Rx Tip/Ring
Others	—	Unused

Table 73: DS1 Pinouts for Line/Network Termination

Pin	Line Termination Mode	Network Termination Mode
1	Tx Ring	Rx Ring
2	Tx Tip	Rx Tip
3	Unused	Unused
4	Rx Ring	Tx Ring
5	Rx Tip	Tx Tip
6	Unused	Unused
7	Unused	Unused
8	Unused	Unused

PRI Card

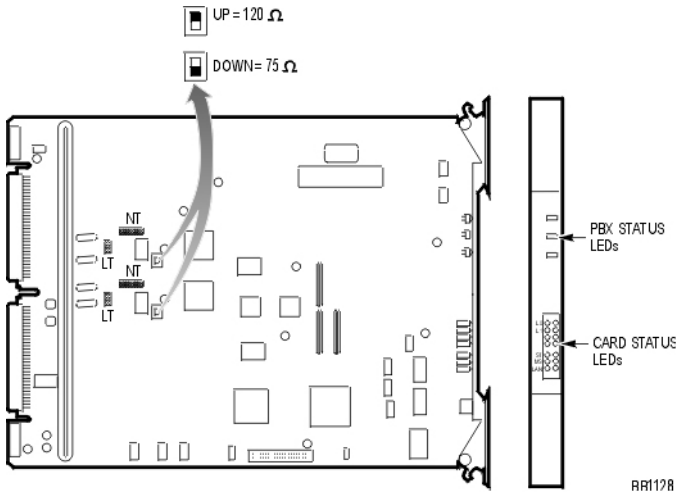


Figure 68: PRI Card Termination Settings

Peripheral Resource Card

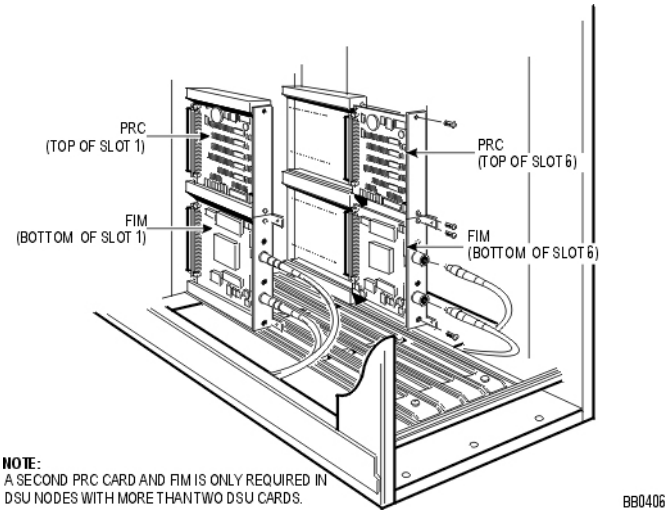


Figure 69: Peripheral Resource Card Installation

R2 Card

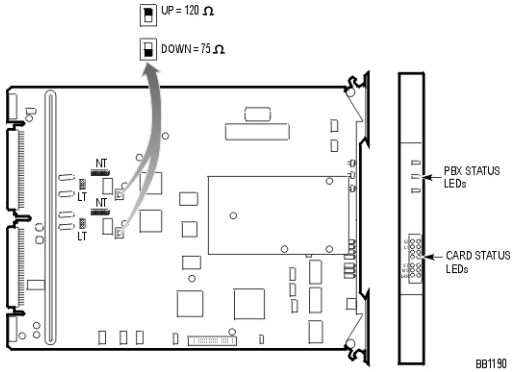


Figure 70: R2 Card Termination Settings

Table 74: R2 Card RJ-45 Connector Pinout

Pin	Function
1, 2	TX
4, 5	RX

IP Phones

Powering Features

Table 75: IP Phone Powering Features

Option	5201, 5205, 52125215, 5230, 5235, 5330, 5340, Navigator	5220, 5224, 5240, TeleMatrix 3000IP
Ethernet / AC Power Adapter (48 VDC LAN Power)	Yes	Yes
AC Power Adapter (24 VDC)	No	Yes
Power Dongle (Cisco-Compliant)	Yes	Yes
3300 In-line Power Dsine Hub	Yes	Yes
Spare Pair Power, 802.3af	Yes	Yes
Signal (Phantom) Pair Power, 802.3af	Yes	Yes
Optional Power Adapter for NA: 50002070 - 5x01, 5x05, 5215; 50000690 - 5x10, 5x20, 5x30, 5x40, 5305, 5310, 5485, 5550; 50002070, 50005080, 50002090 - 5235 (with a DNIC interface module); 9132-800-210-NA - 4015IP, 4025IP.		

Appendix B
Installation Planner

CXi/MXe Requirements for IP Networking

Tip: Refer to the Engineering Guidelines, Network Configuration for CXi- and MXe-specific guidelines and, configuration and programming requirements.

LAN Requirements

- A subnet with IP addresses reserved for the following:
  - the CXi/MXe system
  - the internal Layer 2 switch
  - the system gateway (router on the LAN or the CXi/MXe itself)
  - static IP addresses or DHCP-assigned addresses for IP phones (DHCP-assigned addressing is recommended).
- A Dynamic Host Configuration Protocol (DHCP) server within the Broadcast Domain. The CXi and MXe include a DHCP server.

Tip: IP phones/IP devices should only be served by one DHCP server.

- Optional:
  - a router or firewall on the same subnet as the CXi/MXe. (Note that firewall (including NAT) is on by default for incoming connectivity from the Internet via the WAN port.)
  - external Layer 2 switches (unmanaged for a voice only; managed and VLAN-capable for a voice and data implementation). The CXi supports as many switches as required but you cannot exceed the maximum 64 IP users.
  - SMTP server address to support e-mail forwarding
  - DNS server address; external DHCP server information;
  - one PC per IP phone (phones must be dual-port models); PCs must have 10/100BaseTx Ethernet cards.

Tip: Layer 2 switches should only be connected to Port 17 on the CXi and the left Gigabit port on the MXe. This rule lessens the chance of spanning tree issues (loops in the network).

Tip: IP trunks cannot work through the WAN port.

WAN Requirements

- Internet Gateway (WAN interface) IP address details; program one of the following address assignment methods:

  Static address assignment

  - IP address
  - Subnet Mask
  - Default Gateway

  DHCP address assignment

  - Client name (as required by ISP)
  - Client ID or MAC address (as required by ISP)

  PPPoE address assignment

  - User name
  - Password
- (Optional) Port Forwarding details—i.e., list of IP address and port number for services on internal network that are to be made available to external network.

Other Considerations

- System IP Configuration form
  - Reset the controller when you change any settings, except DNS
  - Enter the voice VLAN priority (0-7) for expedited forwarding of traffic, which should match the voice priority programmed on the external L2 switches as well as the value programmed for DHCP Option 43 or Option 125 (whichever is used). The data VLAN default is 1. The default voice VLAN priority is 6.
  - Enter the Differentiated Services Code Point Value (DSCP) for voice streaming and signaling. This value should match the value programmed for DHCP Option 43 or Option 125 (whichever is used). The default is 44 (for upgrades) or 46 (for new installations).
- Layer 2 Switch form
  - Tag VLAN 1 on Trunk Ports: Select "Enabled" to enable 802.1p/Q VLAN tagging for VLAN 1 on the 10/100/1G LAN port(s). The field applies to untagged and VLAN 1 tagged packets only; voice VLAN tagging is always preserved.

- IP Routing form
  - When the CXi/MXe receives a packet from a host on the LAN, it checks the table. If a route is found on the Network List, the CXi/MXe forwards the packet to the system Gateway or a router connected to the local subnet. If no route is found, the CXi/MXe forwards the packet to the internet through its WAN interface.

CXi/MXe VLAN Behavior

- Default VLAN 1
  In the default case where the CXi/MXe is on the default VLAN, the CXi/MXe accepts tagged VLAN 1 frames and untagged frames. Any non-VLAN 1 tagged frames are dropped. The CXi/MXe treats untagged frames as VLAN 1 frames. The CXi/MXe prioritizes traffic based on the priority tag and maintains two priority queues. The low priority queue is for untagged frames and tagged VLAN 1 frames with priority 0-3. The high priority queue is for tagged VLAN 1 frames with priority 4-7. Traffic in the high priority queue is processed first. On egress, all traffic on all ports is untagged with the exception of port 17 on the CXi and the two LAN ports on the MXe, where the user has the option to tag the traffic via the “VLAN Tags on Trunk Ports” parameter.
- Voice VLAN
  In order for the phones to operate on the Voice VLAN, the CXi/MXe L2 Switch must also be on the same Voice VLAN, or unknown VLAN frames will be dropped. With the introduction of Voice VLAN support, the CXi/MXe will accept untagged frames and tagged VLAN 1 or Voice VLAN frames. All other VLAN tagged frames will be dropped. Priority queues are maintained as described above, but in this case, for Voice VLAN tagged traffic. On egress, Voice VLAN traffic remains tagged on all ports. Untagged frames are treated as VLAN 1 and forwarded to an external router.

Installation

The traditional installation remains the same as for the MX and LX controllers because the CXi and MXe rely on external routers to perform VLAN routing just as the CX, MX, and LX do.

The main difference is that the CXi and MXe maintain Voice VLAN tags on egress. An externally managed L2 switch connected to the CXi/MXe uplink port(s) must tag Voice VLAN traffic unlike the setup for the other controllers that require untagged Voice VLAN traffic.

Controller Configuration Settings (RTC)

Do not change these settings unless you are directed to make changes by an RN. Unauthorized changes may prevent the system from booting up.

Table 76: Controller Configuration Settings

Prompt	Value	Note
boot device	ata=0, 0	Boot device is Disk.
processor number	0	Not used.
host name	bootHost	
file name	ALL platforms, after Release 6.0: /partition1/Rtc8260 (Prior to Release 6.0: LX/700-user: /partition1/Rtc8260 MX: /partition1/Lite200UP 100-user: /partition1/Lite8260)	Boot location and file name. File names are case-sensitive. [Settings prior to Release 5.0: 250/700-user: /sysro/Rtc8260 100-user: /sysro/Lite8260]
inet on ethernet (e)	**default IP address: 192.168.1.2:ffffff00**	**IP address and subnet mask (hex) for controller RTC. Provided by your IT administrator.**
inet on backplane (b)		
host inet (h)		IP address of PC used for software upgrades.
gateway inet (g)		**IP address of the default gateway for the 3300 ICP (must be outside the DHCP range).**
user (u)	**ftp**	
ftp password (ftp)	**ftp**	
flags (f)	0x0	Fixed IP address (0x40 used on E2T for DHCP).
target name (n)		
startup script (s)		
other (o)	motfcc	Other device, E2T using Network boot from.

Tip: Do not use leading zeroes in the IP addresses. For example, enter 192.168.1.2; not 192.168.001.002.

DHCP Configuration Settings

Table 77: E2T Static IP Address Programming

Option Name	Value	Notes/Example
Name	Name of E2T	
Subnet	Subnet of E2T	Select subnet.
IP Address	IP address of E2T	192.168.1.5
Protocol	“BOOTP or DHCP”	
Hardware Address:		
Type	MAC Address	
Other - Type	n/a	
Address	MAC address of controller E2T (see the Note)	00:12:3a:4b:c5:67
Other - Address Length	n/a	
Client ID	n/a	
Note: The E2T MAC address is found on the MAC Address label on the rear panel of the ICP. Of the three MAC Address labels on the rear panel, use the one that refers to “E2T MAC”, “Slot 1”.		

Table 78: IP Address Range (Scope) Programming

Option Name	Value	Notes/Example
Name of the range		
Subnet		System-generated
IP Range Start (see note)	Start of scope	192.168.1.15
IP Range End (see note)	End of scope	192.168.1.25
Protocol	Select “None”, “BOOTP”, “DHCP”, or “BOOTP or DHCP”	Default is “BOOTP or DHCP”
Client’s class ID must match name	Clear checkbox.	
Lease Time	2 Weeks	Minimum 5 minutes.
Note: Cannot be modified once form is saved.		

Table 79: Mitel DHCP Server Options

Option ID	Name	Type	Value (notes, example)
3	Router IP address	IP Address.	192.168.1.3
6	DNS server IP address	IP Address	Required for the 5230 IP Appliance.
125 (Applies to Rel. 7.0 and later systems. Option 43 can also be used.)	Vendor Specific Information	ASCII String	Default is "id:ipphone.mitel.com;sw_tftp=192.168.1.2;call_srv=192.168.1.2; vlan=1;l2p=6;dscp=46"
44	NetBIOS name	IP Address	Server IP address. Required for the 5230 IP Appliance.
66	TFTP Server Name	ASCII String	Required when using an external DHCP Server. Boot Server Host Name (same as RTC IP address, for E2T only).
67	bootfile	ASCII String	Boot file name (for E2T only).
128 (See note)	TFTP Server (usually the controller RTC)	IP Address	IP address of the TFTP server (192.168.1.2)
129 (See note)	RTC IP Address for this controller	IP Address	IP address (192.168.1.2) Enter up to four IP addresses of remote fail-over RTCs. Separate entries with a comma and a space.
130 (See note)	IP Phone DHCP server discrimination string.	ASCII String	**MITEL IP PHONE**
131 (See note)	IP Phone Analyzer PC	IP Address	

(Page 1 of 2)

Table 79: Mitel DHCP Server Options (continued)

Option ID	Name	Type	Value (notes, example)
132 (See note)	VLAN ID (optional)	HEX, numeric	2 (for external server, use Hex LONG; for internal server use decimal)
133 (See note)	Priority (optional)	HEX, numeric	6 (for external server, use Hex LONG; or internal server use decimal)
134 (See note)	DiffServ Code Point	Numeric	44 (prior to Rls 6.0) 46 (from Rls 6.0)
140	IP DECT Open Mobility Manager (OMM)	IP Address	IP Address of the primary Radio Fixed Part (RFP)
150	IP DECT secondary OMM	IP Address	IP Address of the secondary Radio Fixed Part (RFP)
151	SpectraLink Voice Priority (SVP) server	IP Address	
Note: Required on Release 7.0 systems to allow IP sets to upgrade to firmware that supports options 125 and 43.			
(Page 2 of 2)			

Use the settings in Table 80 for all scopes supporting IP voice devices.

Table 80: DHCP Server Configuration Settings

IP Address Scope			
Start Address			
End Address			
Subnet Mask			
Lease Duration	Days:	Hours:	Minutes:
Options (at Subnet Scope for all devices)	**ID**	**Data Type**	**Value**
(Router) Default Gateway	003	IP Address	

Table 80: DHCP Server Configuration Settings (continued)

Options (at Global Scope for WEB devices)			
DNS Server	006	IP Address	
DNS Domain Name	015	ASCII String	
Options (for 3300 E2T)			
TFTP Server (hostname or IP)	066	ASCII String	(typically the IP address of the controller RTC)
TFTP BootFile	067	ASCII String	/sysro/E2T8260
Options (for IP Phones)			
The following two options apply to Release 7.0 and later. The second, Option 125, is the factory-programmed default.			
Vendor Specific Information	43	ASCII String	Default value is, "id:ipphone.mitel.com;sw_tftp=192.168.1.2;call_srv=192.168.1.2; vlan=1;l2p=6;dscp=46"
Vendor-Identifying Vendor-Specific Information	125		
The following 5 options apply to software load prior to Release 7.0.			
IP Phone TFTP Server	128	IP Address	(typically the IP address of the controller RTC)
MN3300 (RTC) IP Address	129	IP Address	
Mitel IP Phone DHCP server	130	ASCII String	MITEL IP PHONE
VLAN ID	132	Internal: Numeric External: Long	2
VLAN Priority	133	Internal: Numeric External: Long	6

Table 80: DHCP Server Configuration Settings (continued)

Note: ·Option 128-135 correspond to the following Option 43/125 tags:

Option	Equivalent Option 43/125 Tag
128	sw_tftp
129	call_srv
130	id:ipphone.mitel.com
131	ipa_srv
132	vlan
133	l2p
134	dscp
135	app_proxy

The Option 125 string is auto-generated upon upgrade to Release 7.0 provided that Options 128-135 were previously programmed in the DHCP Options form AND Option 130 contains the "MITEL IP PHONE" discrimination string AND there is no option 60 ipphone.mitel.com scope configured in the given subnet.

Programming E2T via Debug Cable or Secure Telnet

Use the settings in Table 81 below to program the E2T using a debug cable. The debug (Tapi) cable is an RS-232 serial cable with a PS2 connector at one end and a DB9 connector at the other. For the MXe, connect to the controller through secure telnet to port 2007.

Tip: Use this section only if you already have a debug cable, and **only if you are directed to do so by Mitel Technical Support**.

Table 81: Debug Cable E2T VxWorks Settings

Prompt	Value	Note
boot device	motfcc	Boot device is Network.
processor number	0	Not used.
host name	bootHost	
file name	/sysro/E2T8260	Boot location and file name.
inet on ethernet (e)		IP address and subnet mask (hex) for controller E2T (for example, 134.199.63.11:ffffff00). Obtain it from your IT administrator.
inet on backplane (b)		
host inet (h)		IP address of controller RTC.
gateway inet (g)		IP address of the end user's default gateway for the 3300 ICP (must be outside the DHCP range).
user (u)	ftp	
ftp password (ftp)	@	
flags (f)	0x0	Fixed IP address (0x40 used on E2T for DHCP).
target name (n)		
startup script (s)		
other (o)		

Configuring External DHCP Settings for E2T

You must reserve an IP address for the E2T on the DHCP server; assign options 66 and 67 on the external DHCP (Windows NT) to E2T reserved IP address. During installation of the 3300 ICP you will manually enter a static IP address on the RTC card. The E2T card will send a DHCP broadcast to obtain an IP address from the DHCP server. The DHCP server (internal or external) must be enabled to supply a free IP and option 66 and 67.

In the following procedure examples

- IP subnet for the 3300 ICP network is 10.10.18.0
- RTC (static IP) is 10.10.18.4
- E2T (reserved by DHCP scope) is 10.10.18.58.

To reserve an IP address for the E2T on the external DHCP server:

1. Highlight the Subnet 10.10.18.0 in the DHCP server **DHCP Manager - (Local)** window.
2. Click **Scope** and select **ADD Reservation**.
3. Enter the IP address and MAC address of the E2T. The MAC address is found on the MAC Address label on the rear panel of the ICP. Use the MAC Address label that refers to “E2T MAC” “Slot 1”.
4. Click Add.

To add options 66 and 67 to the E2T card IP address:

1. Highlight the Subnet 10.10.18.0 in the DHCP server **DHCP Manager - (Local)** window.
2. Click **Scope** and select **Active Leases**.
3. In the **Active Leases** dialog box, highlight the reserved IP address and then click **Properties**.
4. Click **Options** in the **Properties** dialog box.
5. In the **DHCP Options: Reservation** window, select **option 066 Boot Server Host Name** and click **Add**.
6. Click **Value** to assign the RTC IP address in the **String** area.
7. In the **DHCP Options: Reservation** window, select **option 067 Bootfile Name** and click **Add**.
8. Click **Value** to specify the path **/sysro/e2t8260** in the **String** area.

Configuring a Windows 2000 DHCP Server (prior to Release 7.0)

You can modify a Windows 2000 DHCP server to support IP Phones. A DHCP server must be configured for each subnet. The following items must be configured:

- TFTP Server IP address
- IP address of the RTC card
- Mitel tag "MITEL IP PHONE".

To modify a Windows 2000 DHCP Server:

1. In the **Start** menu, point to **Programs**, then **Administrative Tools**, and click **DHCP**.
2. Highlight the Server name and point to **Action**, then click **Set Predefined Options**.
3. In the **Predefined Options and Values** window, click **Add**.
4. In the **Option Type** window, set the following:
   - **Name**: IP phone TFTP Server IP Address
   - **Type**: IP Address
   - **Code**: 128. Then click OK.
   - **Value**: enter the IP address of the TFTP server (the controller RTC) then click **OK**.
5. In the **Predefined Options and Values** window, click **Add** again.
6. In the **Option Type** window, set the following:
   - **Name**: RTC IP Address
   - **Type**: IP Address
   - **Code**: 129. Then click OK.
   - **Value**: enter the IP Address of the RTC card. Click **OK**.
7. In the **Predefined Options and Values** window click **Add** again.
8. In the **Option Type** window, set the following:
   - **Name**: Mitel Vendor String
   - **Type**: String
   - **Code**: 130. Then click **OK**.

- **Value**: MITEL IP PHONE. Click **OK**.

Tip: If you are using VLANs complete all of the following steps. If you are not using VLANs complete steps 13 to 18 and step 21.

9. In the **Predefined Options and Values** window click **Add** again.
10. (optional) In the **Option Type** window, set the following:
    - **Name**: VLAN ID
    - **Type**: Hex LONG (32 bit word)
    - **Code**: 132. Then click **OK**.
    - **Value**: enter a numeric value for the Voice VLAN. Click **OK**.

Tip: The server will automatically convert the numeric value to Hex.

11. In the **Predefined Options and Values** window, click **Add** again.
12. (optional) In the **Option Type** window, set the following:
    - **Name**: Priority
    - **Type**: Hex LONG
    - **Code**: 133. Then click **OK**.
    - **Value**: enter a value from 1 to 7; Mitel recommends **0x6**. Click **OK**.

Tip: The server will automatically convert the numeric value to Hex.

13. Highlight the **Scope** which contains the IP range for the IP Phones and select **Scope Options**.
14. In **Action**, click **Configure Options**.
15. In **General**, select option **003 Router** and enter the IP address of the default Gateway and then click **Add**.
16. Select Option **128**.
17. Select Option **129**.
18. Select Option **130**.
19. Select Option **132**.
20. Select Option **133**.
21. Click **OK**.]

Configuring a Windows 2000 or Windows 2003 DHCP Server (Rls 7.0 and later)

Neither Windows 2000 nor Windows 2003 support DHCP Options 124/125. Options 60/43 must be used instead.

Note: Options 128-133 used in previous ICP releases are required to provide backward compatibility with IP sets that have yet to be upgraded with firmware (2.0.0.18 or later) that supports options 124/125 or 60/43. After the upgrade, the old options may be removed to prevent future conflicts with standard use or other vendors' use of these options.

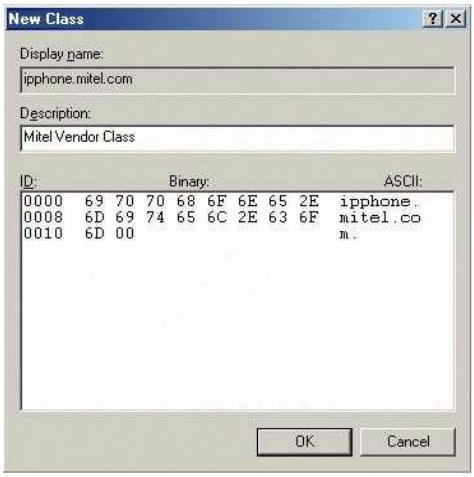
Note: If you intend to rely on LLDP VLAN Discovery in the network, you must first upgrade the 3300 ICP to Release 7.0 or later and upgrade the IP Phone firmware to version 2.0.0.18 or later.

Note: LLDP-MED non-compliant telephones cannot use LLDP for VLAN discovery. They must use DHCP VLAN discovery. Non-compliant sets are: 5001, 5005, 5010, 5020 IP Phones, 5140 IP Appliance, 5201, 5205, 5207, 5215 (single mode), 5220 (single mode), 5230 IP Phones, 5240 IP Appliance, 5485 IP Pager, and 5550 IP Console keypad.

To create Options 60/43 on a Windows 2000 (or Windows 2003) DHCP server:

1. Upgrade the 3300 ICP to Release 7.0.
2. Upgrade the IP Phone firmware. (See page 51).
3. Start DHCP Manager.
4. In the console tree, click the applicable DHCP server branch.
5. Right-click the server, then click **Define Vendor Classes** followed by **Add**.
6. In the **New Class** dialog box, type "Mitel Vendor Class" or other name for the new option.
7. Type "ipphone.mitel.com" in the right side of the text box under **ASCII**.

8. Enter a null terminator (0x00) at the end of the hex string under **Binary**. The completed dialog box should look like this:



IP0927

9. Click **OK**, and then click **Close**.
10. On the **Action** menu, select **Set Predefined Options**.
11. In the **Predefined Options and Values** dialog box, select the Mitel Vendor Class from the Option class list. Click **Add**.
12. In the **Option Type** dialog box, enter the following:

Field name	What to enter...
Name	Mitel Option
Data type	String
Code	001

13. Click **OK**.
14. In the **Predefined Options and Values** dialog box, select 001 Mitel Option as the Option name and enter the Mitel Information Data string with the appropriate values.
15. Enter the Mitel ID string with the appropriate values for <IP address> and <N>,

    id:ipphone.mitel.com;sw_tftp=<*IP address*>;call_srv=<IP address>; dscp=<*N*>;vlan=<*N*>;l2p=<*N*>

For defaults, see Table 80 on page 303.

Tip: You can use the DHCP Options form in the System Administration Tool to create the configuration string, then copy it into a text editor and modify it as required.

16. Click **OK**.
17. Add the Mitel option to the DHCP scopes that require it, modifying the ID string accordingly.

System Administration Tool Settings

Table 82: System Administration Tool Settings

Setting	Default	Personalized (enter value)
username	system	
password	password	

IP Phone Settings

Table 83: IP Phones Settings

IP Phone MAC Information		
IP Set Registration Code		(See System Option Assignment)
IP Set Replacement Code		

Telephone Programming Guide

Use the format below to collect information for programming the phones.

Table 84: Telephone Programming Settings

Set Programming Guide				
User Name	**Location**	**Set Type**	**Number**	**MAC Address (optional)**

Table 85: Telephone Compression Conditions

Call setup conditions	G729 compression supported	Compression DSP required
IP Phone to IP Phone (except 5x01, 5x05, and 5207)	Yes	No
IP Phone to IP Trunk to IP Phone (except 5x01, 5x05, and 5207)	Yes	No
IP Phone to TDM Phone	Yes	Yes
IP Phone to Embedded voice mail	Yes	Yes
IP Phone in conference	Yes	Yes
IP Phone on Hold, listening to music	Yes	Yes
IP Phone listening to music	No	n/a
TDM Phone to IP Trunk to TDM Phone	Yes	Yes
Direct Set-to-set paging (using first codec)	Yes	No

Appendix C
Typical Network Configurations

Network Configuration Examples

This section shows examples of the three most common, non-resilient, network configurations for a 3300 ICP LX, MX, CX, 250/700-User:

- Configuration 1: One DHCP Server per VLAN (below)
- Configuration 2: One DHCP Server for Two VLANs (page 320)
- Configuration 3: Router on a Stick (one router interface to multiple VLANs) (page 321).

Tip: See “CXi/MXe Configuration Procedures” on page 323 for CXi-specific configuration examples.

DHCP Server Settings (Example)

The following settings must be programmed in the DHCP server:

- DHCP IP Address Range
- Subnet Mask
- Option 03 (Router)
- Option 125 or 43 (Mitel configuration string)
- Option 128 (TFTP Server IP Address)
- Option 129 (RTC IP Address)
- Option 130 (MITEL IP PHONE)
- Option 132 (VLAN ID)
- Option 133 (Priority)

Note: Option 125 (preferred) or 43 should be used for Release 7.0. Options 128-133 may be required for backward compatibility during upgrades. For earlier releases, use options 128-133.

Tip: See “Configuring a Windows 2000 DHCP Server (prior to Release 7.0)” on page 308 and “Configuring a Windows 2000 or Windows 2003 DHCP Server (Rls 7.0 and later)” on page 310 for information on programming 3300 DHCP settings on a Windows 2000 DHCP server.

Configuration 1: One DHCP Server per VLAN

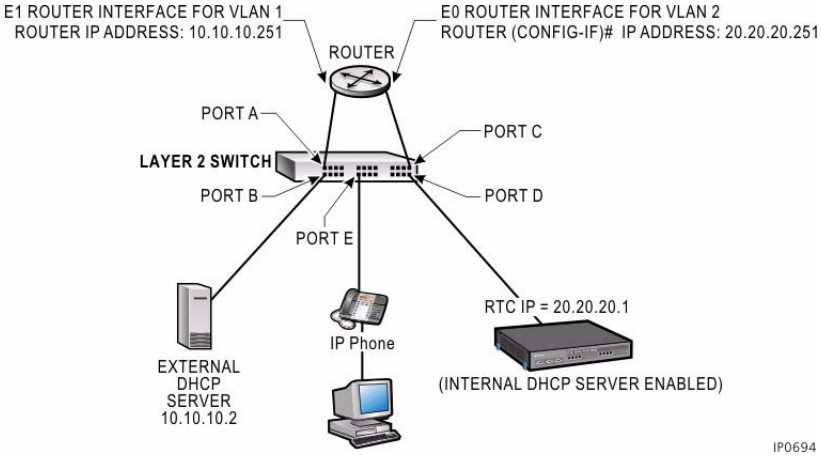


Figure 71: One DHCP Server per VLAN - Example

Table 86 below shows the DHCP settings programmed for this configuration.

Table 86: DHCP Settings Example (Configuration 1)

Setting	DHCP Server on VLAN 1 (IP: 10.10.10.2) Scope 1	Internal DHCP Server on Controller Scope 1
DHCP	10.10.10.10 to 10.10.10.100	20.20.20.10 to 20.20.20.100
Subnet	255.255.255.0	255.255.255.0
Opt. 03	10.10.10.251	20.20.20.251
Opt 125 or 43 (Rel. 7.0>)	id:ipphone.mitel.com;sw_tftp=192.168.1.2;call_srv=192.168.1.2;vlan=1;l2p=6;dscp=46;	
Opt. 128*	20.20.20.1	20.20.20.1
Opt. 129*	20.20.20.1	20.20.20.1
Opt. 130*	MITEL IP PHONE	MITEL IP PHONE
Opt. 132*	2	—
Opt. 133*	6	—
* Required on Release 7.0 systems to allow IP sets to upgrade to firmware that supports options 125 and 43.		

Layer 2 Switch Settings (Example)

Table 87 and Table 88 below show examples of settings on a Cisco and an HP Layer 2 switch for this example. See Figure 71 for the port numbers.

Tip: These settings also apply for the other network configuration examples.

Table 87: Cisco Layer 2 Switch Settings Example (Configurations 1, 2 and 3)

Port	Use	Command
A B	Access port for VLAN 1	None (by default, all ports belong to VLAN 1)
C D	Access port for VLAN 2	Router(config-if)#switchport mode access Router(config-if)#switchport access VLAN 2
E	Trunk port with Dot1q for IP Phone	Router(config)#interface fast 0/5 Router(config-if)#switchport mode trunk Router(config-if)#switchport trunk encapsulation dot1q

Table 88: HP Layer 2 Switch Settings Example (Configurations 1, 2 and 3)

Port	Use	Command (on HP VLAN menu)
A B	Access port for VLAN 1	VLAN 1 = untagged VLAN 2 = NO
C D	Access port for VLAN 2	VLAN 1 = NO VLAN 2 = untagged
E	Trunk port	VLAN 1 = untagged VLAN 2 = tagged

Configuration 2: One DHCP Server for Two VLANs

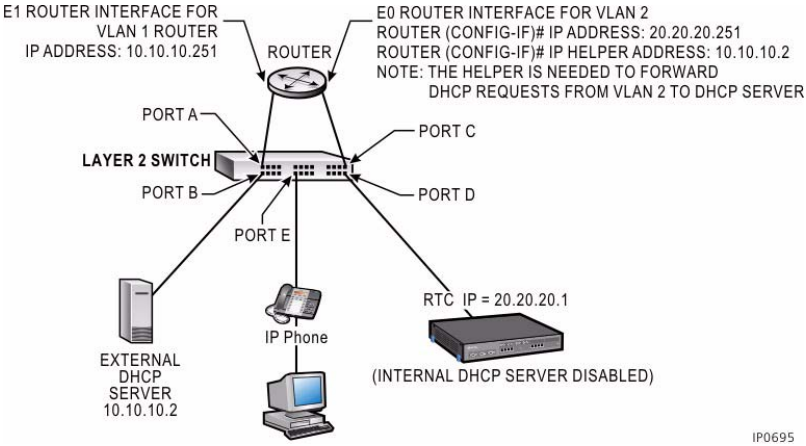


Figure 72: One DHCP Server for two VLANs - Example

Table 89 below shows the DHCP settings programmed for this configuration.

Table 89: DHCP Settings Example (Configurations 2 and 3)

Setting	DHCP Server on VLAN 1 (IP: 10.10.10.2)	
	Scope 1	Scope 2
DHCP	10.10.10.10 to 10.10.10.100	20.20.20.10 to 20.20.20.100
Subnet	255.255.255.0	255.255.255.0
Opt. 03	10.10.10.251	20.20.20.251
Opt 125 or 43 (Rel. 7.0>)	id:ipphone.mitel.com;sw_tftp=192.168.1.2;call_srv=192.168.1.2; vlan=1;l2p=6;dscp=46;	
Opt. 128*	20.20.20.1	20.20.20.1
Opt. 129*	20.20.20.1	20.20.20.1
Opt. 130*	MITEL IP PHONE	MITEL IP PHONE
Opt. 132*	2	2
Opt. 133*	6	6
* Required on Release 7.0 systems to allow IP sets to upgrade to firmware that supports options 125 and 43.		

Layer 2 Switch Settings (Example)

See “Layer 2 Switch Settings (Example)” on page 319.

Configuration 3: Router on a Stick

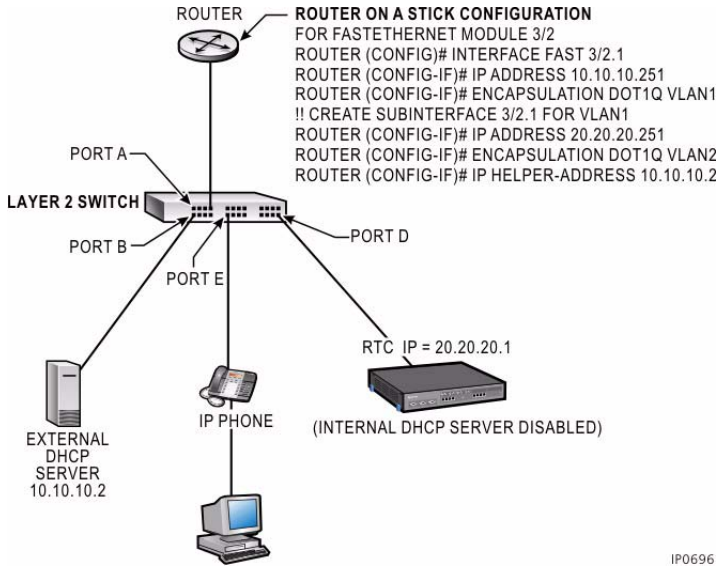


Figure 73: Configuration 3 Example

Table 89 on page 320 shows the DHCP settings for this configuration.

Layer 2 Switch Settings (Example)

See “Layer 2 Switch Settings (Example)” on page 319.

LLDP-MED and IP Phone Network Policy

LLDP-MED stands for Link Layer Discovery Protocol - Media Endpoint Discovery. LLDP-MED is based on VoIP-specific extensions to the IEEE 802.1A LLDP standard. Refer to the Network Configuration chapter in the Engineering Guidelines for details.

Cisco Discovery Protocol (CDP)

Prior to Release 5.1 the Mitel IP devices discovered VLAN information dynamically through DHCP. With Release 5.1, Mitel IP device messages are now compatible with Cisco Discovery Protocol (CDP) for the purpose of port duplex and speed settings, port MAC identification and Auxiliary VLAN assignment. If your network uses Cisco Layer 2 switches, you may configure your L2 ports as Access ports and use the auxiliary VLAN to set the voice VLAN, allowing both phones and PC to share the same network port. For more information on configuring your network, refer to the 3300 ICP Engineering Guidelines, available at http://edocs.mitel.com.

The IP devices understand CDP messages for the following:

- Advertising their in-line power consumption
- Discovering the voice VLAN setting from the Cisco L2 switch
- Advertising their duplex setting, platform, and software release for the "show cdp neighbor" command on the L2 console.

To obtain VLAN information via CDP:

- Set the network part as Access
- Enter the Voice VLAN, or the Auxiliary_VLAN setting
- Enter the data or default VLAN into the Native_VLAN setting
- In DHCP there is no requirement to enter VLAN or Priority into the default/data VLAN
- Set the Priority field to "6" in the voice VLAN scope of DHCP.

CXi/MXe Configuration Procedures

Firewall/Port Forwarding

The Port Forward Table form allows external traffic to reach resources on the internal network and can contain up to 40 entries.

Table 90: Port Forward Table (CXi/MXe only)

Parameter	Function/Values
Protocol	The WAN interface protocol; UDP or TCP.
Src Start Port	The source port at the start of the range.
Src End Port	The source port at the end of the range.
Dst IP Address	IP Address of the destination device.
Dst Start Port	Destination port at the start of the range.
Dst End Port	Destination port at the end of the range.

PPTP Remote Access

The PPTP form is used to program the internet gateway as a PPTP (Point to Point Tunneling Protocol) server for a remote client on the internet.

Table 91: PPTP (CXi/MXe only)

User Name	The username that the server uses to authenticate the remote client.
Password	Password that the server uses to authenticate the remote client.
Client IP Address	Address that the remote PPTP client uses on the LAN.
PPTP Access	Set to “Enable” to enable PPTP remote access.

WAN Settings (Internet Gateway)

The WAN Settings form is used to enable the WAN interface and provide internet connectivity settings.

- Enable WAN Access
- Select a WAN IP method: Static IP Address, DHCP Client, or PPPoE.

Tip: Refer to the Network Configuration chapter in the Engineering Guidelines.

Configuration 1: CXi Typical Voice-Only Network

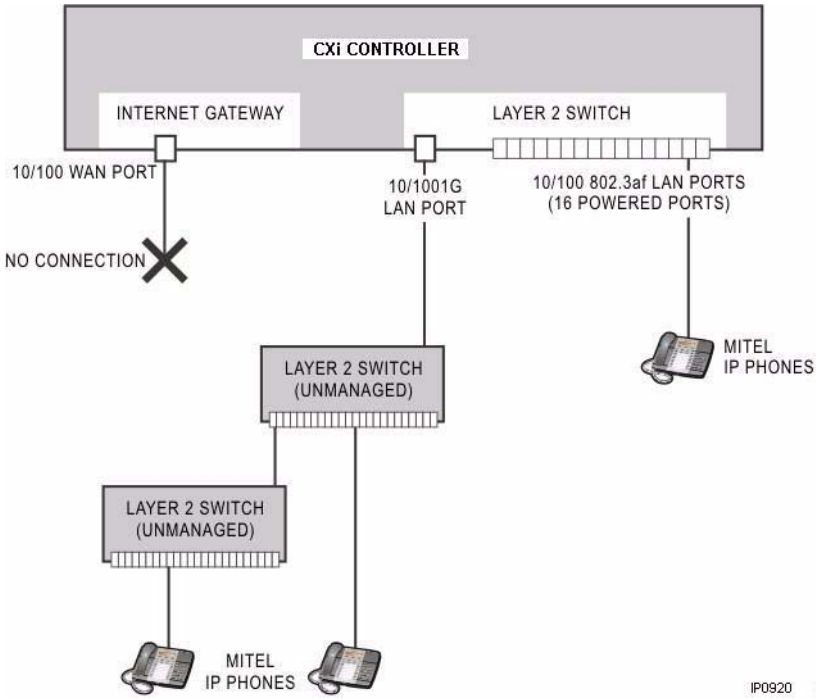


Figure 74: CXi Configuration 1 Example

IP Address	192.168.1.2
Subnet	255.255.255.0
Gateway	192.168.1.1
Layer 2	192.168.1.1

Configuration 2: MXe Typical Voice-Only Network

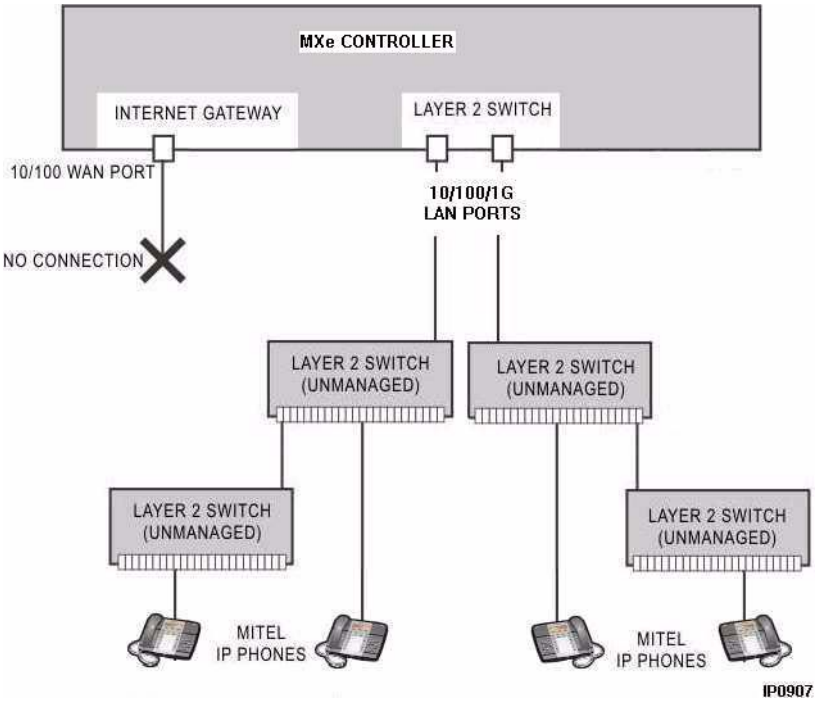


Figure 75: MXe Configuration 2 Example

IP Address	192.168.1.2
Subnet	255.255.255.0
Gateway	192.168.1.1
Layer 2	192.168.1.1

Configuration 3: CXi Typical Voice and Data Network

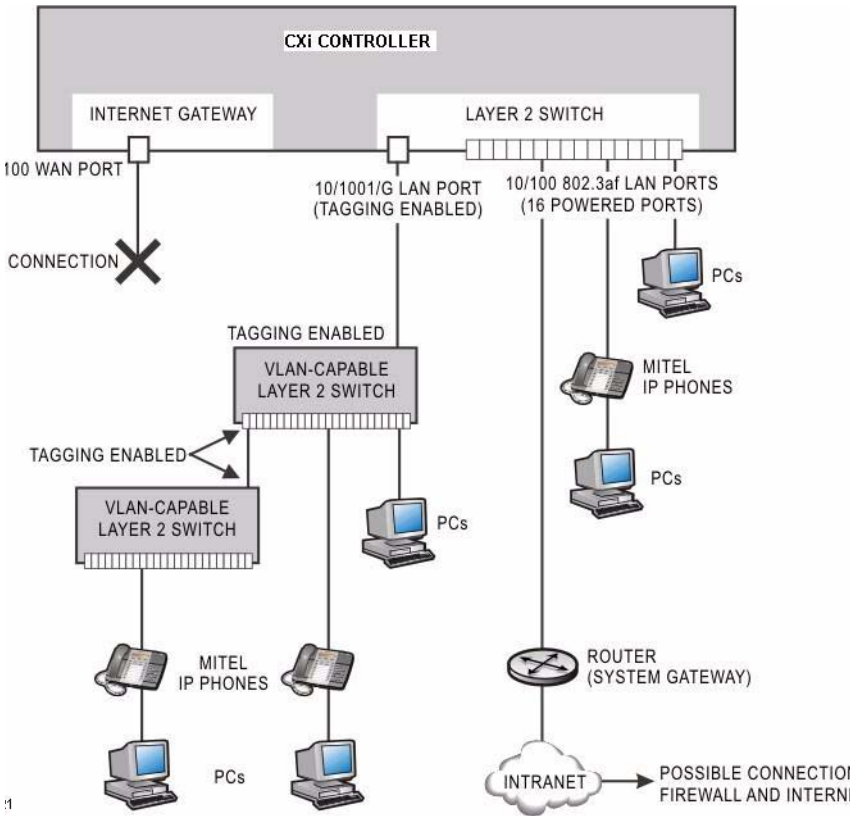


Figure 76: CXi Configuration 3 Example

IP Address	192.168.1.2
Subnet	255.255.255.0
Gateway (Router)	192.168.1.1
Layer 2	192.168.1.3

Tip: If an IP Address is on the IP Network List in the IP Routing form, the connection will be routed to 192.168.1.1 (router).
If the IP Address is not on the IP Network List, then the connection will be routed to the WAN Port automatically.

Configuration 4: MXe Typical Voice and Data Network

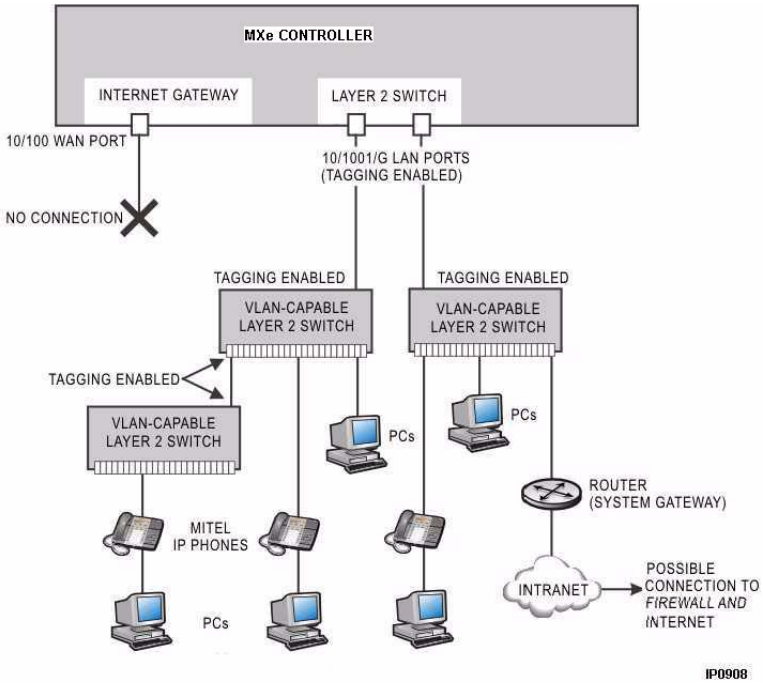


Figure 77: MXe Configuration 4 Example

IP Address	192.168.1.2
Subnet	255.255.255.0
Gateway (Router)	192.168.1.1
Layer 2	192.168.1.3

Tip: If an IP Address is on the IP Network List in the IP Routing form, then the connection will be routed to 192.168.1.1 (router).
If the IP Address is not on the IP Network List, then the connection will be routed to the WAN Port automatically.

Windows 2000 FTP Server

Figure 78, Figure 79 and Figure 80 below show examples of the settings needed on a Windows 2000 FTP server.

To program these FTP settings

1. Open the **Computer Management** control panel (**Start/Settings/Control Panels/Administrative Tools/Computer Management**).
2. In **Services and Applications**, click on **Internet Information**.
3. Program the settings as shown below (use the **IP Address** drop-down menu to select the PC's IP address).

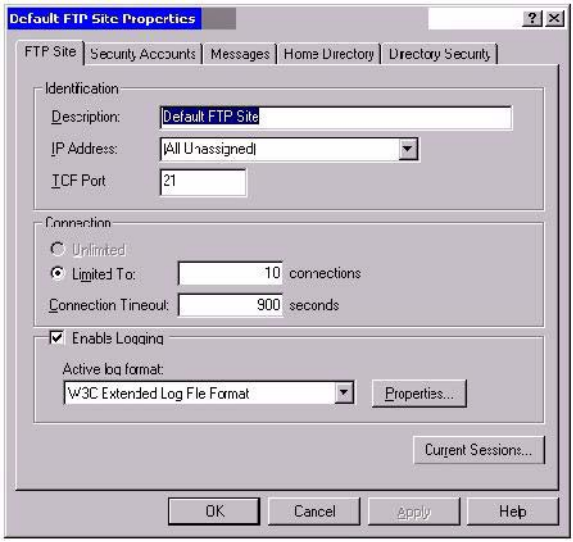


Figure 78: Windows 2000 FTP Site Tab

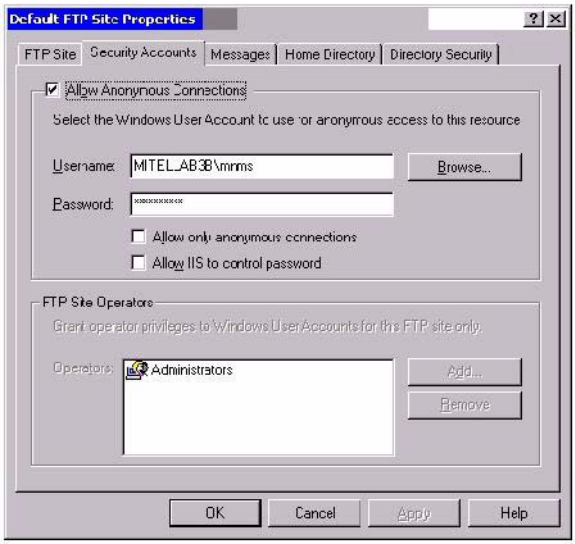


Figure 79: Windows 2000 Security Accounts Tab

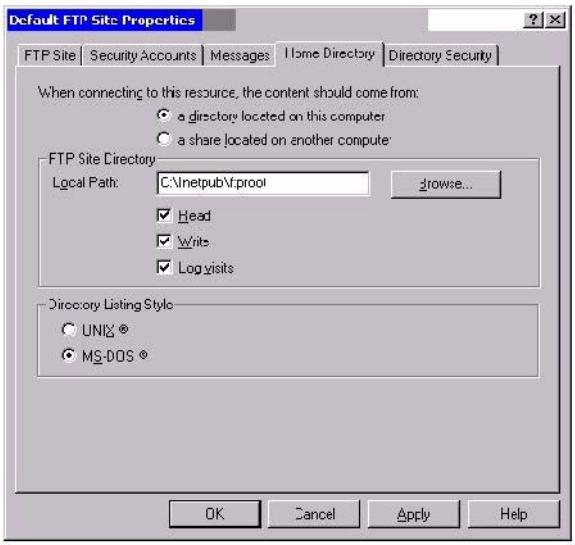


Figure 80: Windows 2000 Home Directory Tab

Appendix D
Status LEDs

This appendix describes the following LEDs in the 3300 ICP system.

- Controller LEDs (below)
- Network Services Unit LEDs (page 346)
- Analog Services Unit LEDs (page 351)
- IP Phone and IP Appliance LAN LEDs (page 354)
- Peripheral Cabinet LEDs (page 355)
- Digital Services Unit LEDs (page 356)
- In-Line Power Unit LEDs (page 361)

For detail on any alarms, see “View Alarms” on page 182.

Controller LEDs

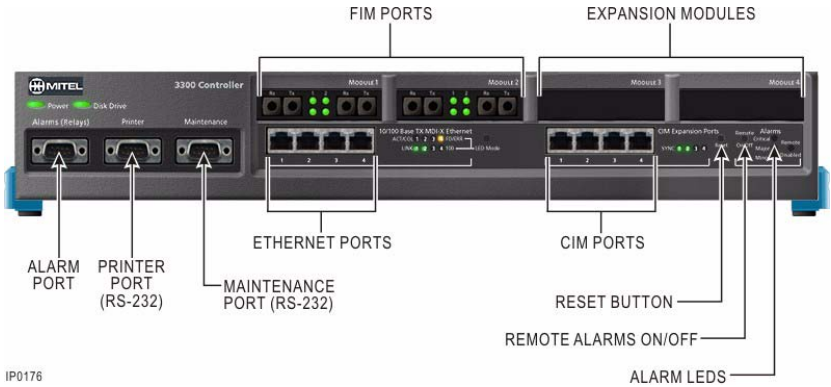


Figure 81: Controller LEDs (LX; MX; 100-User; 250/700-User)

Power LED (page 335)
Hard Drive LED (page 335)
FIM LEDs (page 338)
Ethernet LEDs (page 338)
CIM LEDs (page 340)
Alarm (Relay) LEDs (page 340)
Dual T1/E1 Framer (page 342)
Quad BRI Framer (page 345)

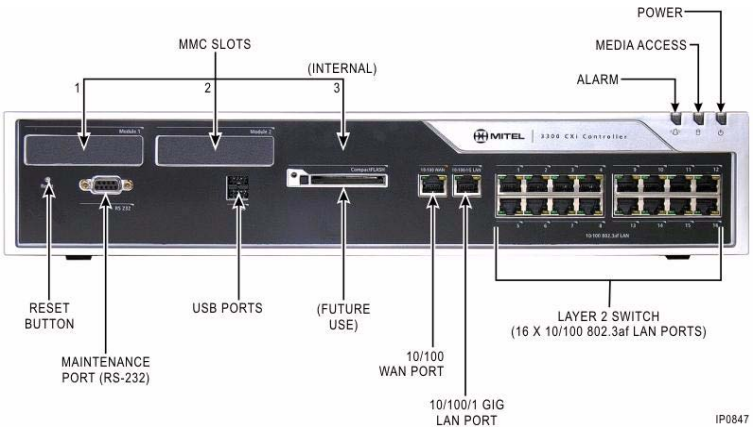


Figure 82: Controller LEDs (CX; CXi)

Power LED (page 335)
Hard Drive LED (page 335)
Alarm (Relay) LED (page 340)
Ethernet LEDs (page 338)
T1/E1 Combo Card (page 344)
Quad BRI Framer (page 345)

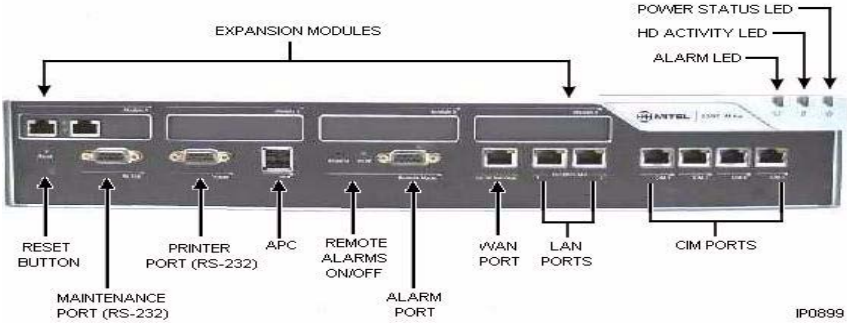


Figure 83: MXe Controller — Front Panel

Power LED (page 335)
Hard Drive LED (page 335)
FIM LEDs (page 338)
Ethernet WAN/LEDs (page 338)
CIM LEDs (page 340)
T1/E1 Combo Card (page 344)
Dual T1/E1 Framer (page 342)
Quad BRI Framer (page 345)

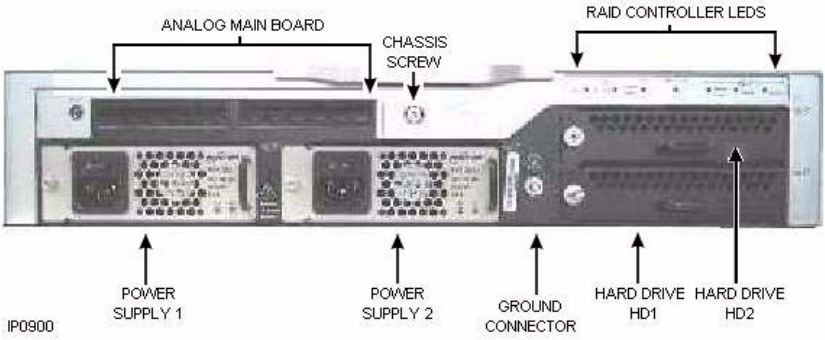


Figure 84: MXe Controller — Rear Panel with Analog

Power Supply LED (page 342) RAID Controller LEDs (page 336)

Power Status, Front Panel

Table 92: Controller Power LED

LED Status	Meaning
Green on	The system successfully booted and is operating normally.
Red - two flashes	The unit is starting up properly (see only during boot process).
Red on solid	The unit has detected an error and is held in reset mode.
Red flashing	The unit has detected an error and will attempt a reset.
OFF	The unit is not plugged in or is faulty.

Hard Drive Activity, Rear Panel

Table 93: Hard Drive Activity LED

LED Status	Meaning
Off	The hard drive disk is inactive.
On flashing	The internal hard disk is being accessed.

RAID Controller

Refer to Knowledge Base Article 06-2806-00012 "RAID Controller Operations Manual" for RAID operation details.

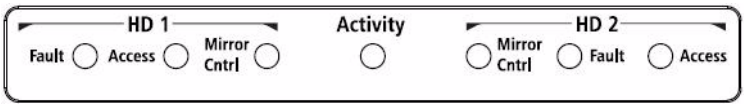


Figure 85: RAID Controller LEDs

Table 94: RAID Controller LEDs

Activity	Meaning
Green ON	No access
Orange ON	Read or write occurring on hard disk

Table 95: Mirror Control Button Functions

Activity	Meaning	
0 - 5 seconds	LED flashes slow (1/sec)	Power down disk
5 - 10 seconds	LED flashes medium (2/sec)	Mirror rebuild
10 - 15 seconds	LED flashes fast (4/sec)	Reserved
15 - 20 seconds	LED solid on	Reserved
> 20 seconds	LED off	No operation
Note: To abort a button press, hold the mirror control button down for more than 20 seconds.		

Table 96: RAID Fault and Access LEDs

Hard Drive State	Fault	Access	Description
Normal	OFF	GREEN	Read or write
Request off-line	OFF	GREEN flashing (1/sec)	Button pushed while online
Going off-line	OFF	GREEN	Button released, processing request
Off-line	OFF	OFF	
Request on-line	Note	GREEN flashing (1/sec)	
Coming on-line	OFF	OFF	Button released, processing
Drive removed	ORANGE	OFF	Replace drive and rebuild
Drive reinserted	ORANGE	OFF	Perform rebuild
Request rebuild	Note	GREEN flashing (2/sec)	
Rebuilding	GREEN flashing	GREEN	Button released, processing; may take 6 hours
Rebuild complete	OFF	GREEN	Resume normal operation
Soft fault	ORANGE flashing	GREEN	Read fault
Hard fault	ORANGE	OFF	Replace drive and rebuild
Note: Depends on previous LED state: OFF = Online; ORANGE = Fault.			

FIM

The top LED indicates the status of local FIM. The bottom LED indicates the status of the remote FIM.

The controller FIM monitors the synchronization of the clock appearing on the fiber link from the peripheral cabinet or DSU. The FIM in the peripheral cabinet or DSU monitors the synchronization of the clock appearing on the fiber link from the controller.

Table 97: Controller FIM LEDs (LX; MX; MXe; 100-User; 250/700-User)

LED Status	Meaning (Both LEDs)
ON	In-frame synchronization.
Flashing	Out of synchronization *OR* Tx and Rx fiber optic cables reversed.
OFF	Power off *OR* held in reset.

LAN Ethernet Ports

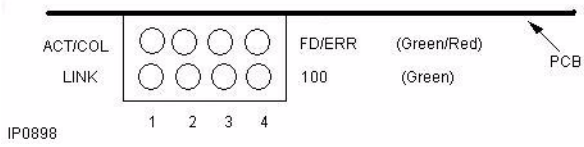


Figure 86: Controller LAN Ethernet Port LEDs (LX; 100/250/700-User)

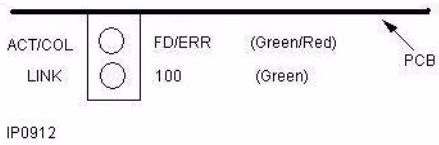


Figure 87: Controller LAN Ethernet Port LEDs (MX)

Table 98: Controller Ethernet Ports LEDs (LX; MX; 100-User; 250/700-User)

LED		Meaning	
Top	**Bottom**	**Normal Mode**	**Switch Pressed Mode**
ON (Green)	—	Link activity	Full duplex
ON (Red)	—	Collision	ERR
—	ON (Green)	Link integrity	100 Mbps
—	OFF	No link integrity	10 Mbps

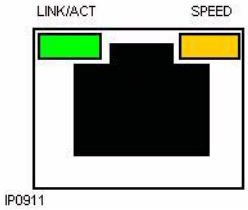


Figure 88: Controller LAN Ethernet Port LEDs (CX/CXi and MXe)

Table 99: WAN/LAN Port LEDs (CX, CXi, and MXe)

LED	Meaning
Green on	Link is active.
Green blinking	Link is active and transmitting or receiving.
Green off	Link is inactive.
Yellow on	Data transmission/reception is at 100 Mbps (the port speed for the 10/100/1GigE LAN Port can be up to 1 Gbps).
Yellow off	Data transmission/reception is at 10 Mbps.

CIM

Table 100: Controller CIM LEDs

LED Status	Meaning (All LEDs)
ON	Communication link established and configured
Flashing	Link established but not configured
OFF	No power

Controller Alarm

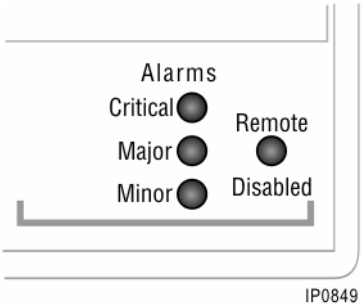


Figure 89: Controller Alarm (Relay) LEDs (LX; MX; 100-User; 250/700-User)

Table 101 below shows the meaning of the Alarm LEDs.

Table 101: Controller Alarm (Relay) LEDs (LX; MX; 100-User; 250/700-User)

Alarm	State	Meaning
Critical	Red on	Service is lost; immediate maintenance required (critical alarm invokes system fail transfer if enabled). *OR* Power on reset ongoing. *OR* INIT switch activated (resets all boards).
	off	No alarm.

(Page 1 of 2)

Table 101: Controller Alarm (Relay) LEDs (continued) (LX; MX; 100-User; 250/700-User) (continued)

Alarm	State	Meaning
Major	Red on	Service has degraded beyond predetermined threshold. *OR* Embedded voice mail is not functioning or disk space is at 98%.
	off	No alarm.
Minor	Red on	Minor malfunction in system (minor alarm raised when system not fully operational). *OR* Embedded voice mail disk space is at 90%.
	off	No alarm.
Remote Disabled	Red on	Alarm is on, but silenced (Silence state is toggled by the Remove Alarms ON/OFF switch). *OR* PRO or INIT switch active.
	off	Alarm is audible *OR* Controller is powering up.

(Page 2 of 2)

Table 102 below shows the meaning of the single alarm LED.

Table 102: Controller Alarm LED (CX, CXi, and MXe)

Alarm	LED State	Meaning
Critical	Red flashing	Service is lost; immediate maintenance required (system fail transfer invoked if enabled) *OR* Power on reset ongoing.
Major	Orange flashing	Service has degraded beyond predetermined threshold. *OR* Embedded voice mail is not functioning or disk space is at 98%.

(Page 1 of 2)

Table 102: Controller Alarm LED (continued)(CX, CXi, and MXe) (continued)

Alarm	LED State	Meaning
Minor	Yellow flashing	Minor malfunction in system (minor alarm raised when system not fully operational). *OR* Embedded voice mail disk space is at 90%.
Reset button depressed	Red/ Orange/ Yellow	Alarm is on, but silenced (Silence state is toggled by the Remote Alarms ON/OFF switch). *OR* PRO or INIT switch active.
	OFF	Normal operation.
Note: See on "Controller Remote Alarm Behavior" on page 266 for a description of the Remote Alarm LEDs on the MXe.		
		(Page 2 of 2)

Power Supply Unit LEDs

Table 103: Power Supply Unit LEDs

LED Status	Meaning (All LEDs)
OFF	No AC power being supplied. Check input cord.
ON	Normal operation.

Dual T1/E1 Framer Module

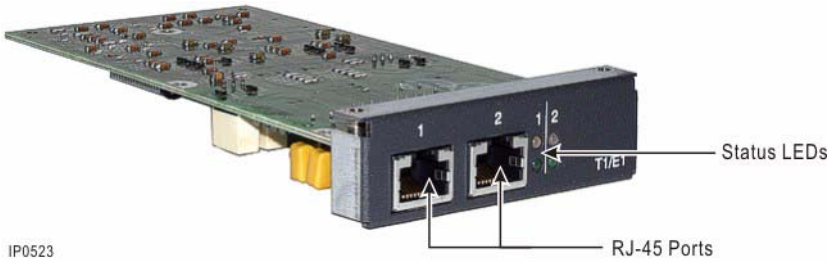


Figure 90: Dual T1/E1 Framer Module

Table 104: Controller Dual T1/E1 Framer LEDs

LED		Meaning
Alarm (bottom)	**Status (top)**	
ON (Red)	—	No Layer 1.
ON (Yellow)	—	Alarm indication from far end.
OFF	—	No error
—	ON (Green)	ISDN D-Channel established.
—	Flashing (Green)	Layer 1 established. (ISDN only)
—	OFF	No link.
On (Yellow) with right side OFF	ON (Green)	Blue alarm from far end.
OFF	OFF	Not programmed.

T1/E1 Combo Card

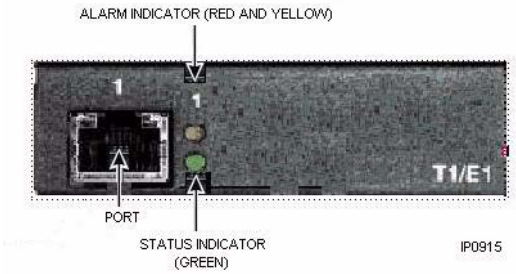


Figure 91: Controller T1/E1 Combo Card (Rls 6.0)

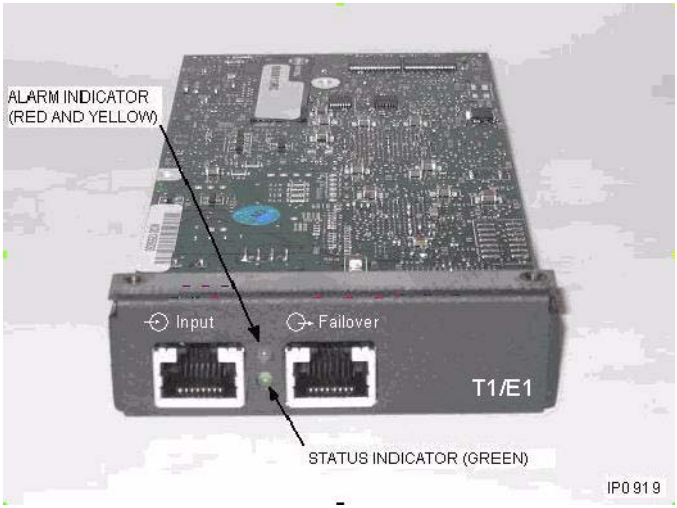


Figure 92: Resilient T1/E1 Combo Card (Rls 7.0)

Table 105: Controller T1/E1 Combo Card

Status LED (green)	Alarm LED (red/yellow)	Meaning
Off	Off	Link not programmed or link descriptor not assigned.
Off	Solid Red	Red alarm. Loss of signal; check link connection.
Off	Solid Yellow	Yellow alarm. No signal from remote end; check link with analyzer. (This state is normal during startup.)
Solid Green	Solid Yellow	Blue alarm. Check link with analyzer.
Solid Green	Off	Layer 1 synchronized. Good link state; no alarms.
Flashing Green	Solid Yellow	Alarm indication from remote end.
Flashing Green	Flashing Red	The card is in resilient mode.

Quad BRI Framer Module

For each BRI port on the Quad BRI MMC, there are two LEDs - red on the upper left and green on the upper right. These LEDs represent the status of the BRI ports as described in Table 106.

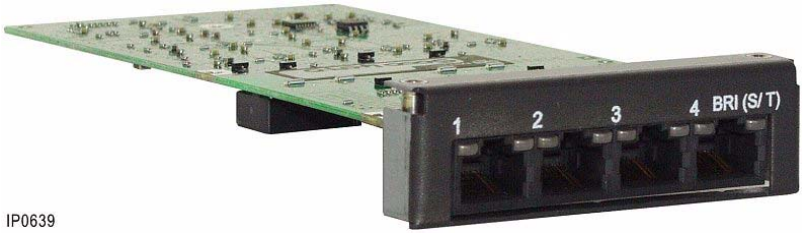


Figure 93: Controller BRI Framer LEDs

Table 106: Controller BRI Framer LEDs

LED		Meaning
Alarm	**Status**	
Red Green	OFF OFF	BRI port not programmed. Link Descriptor is not assigned in the Digital Link Assignment form.
Red Green	ON OFF	BRI port programmed but not active. BRI cable not plugged in, or wrong cable type (1:1 or crossover). BRI link may not be active (or layer 1 power save is active). No alarms are returned to the 3300 and circuits are idle. To prevent routing problems when there is a faulty BRI port, program the MSDN/DPNSS Stepback feature. Refer to the System Administration Tool online Help for details.
Red Green	OFF ON	BRI port programmed and active. Does not mean that the D-channel is active. BRI can negotiate this on a per-call basis.

Network Services Unit LEDs

Universal/R2 NSU

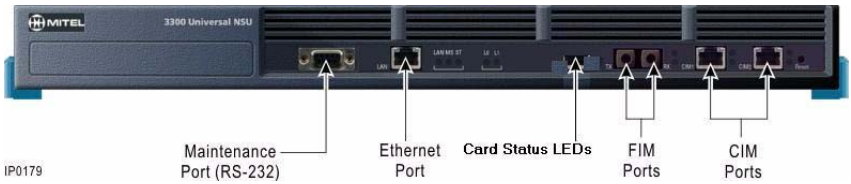


Figure 94: Universal and R2 NSU LEDs

NSU FIM LEDs

Table 107: NSU FIM LEDs

LED Status	Meaning for local (upper) and remote (lower) FIM
ON	In-frame synchronization.
Flashing	Out of synchronization *OR* Tx and Rx fibers reversed.
OFF	Power off *OR* held in reset.
Note: When a Remote FIM LED is OFF, check the Local FIM LED; if the Local FIM LED is ON, a fiber optic cable may be faulty.	

NSU CIM LEDs

Table 108: NSU CIM LEDs

LED Status	Meaning (all LEDs)
OFF	No Power.
Flashing	Powered on.
ON	Communication Link synchronized with other node.

Universal NSU LED States

Table 109: Universal NSU LED States

LED	State	Meaning
LAN	flashing	LAN activity
MS (message system)	solid green	Message link open to the system
	OFF	Message link not open to the system; may be downloading when L0 and L1 are “walking”
ST (status)	flashing	Operational; flashing at 0.5 sec intervals
	OFF	Not operational
	solid	Card is booting or not operating; should be blinking at 0.5 sec intervals
L0 and L1 (on front and rear)	right side - solid red	No Layer 1
	right side - OFF	No error
	left side - solid green	D-channel established (PRI) Layer 1 established (T1, E1, DPNSS)
	left side - flashing green	Layer 1 established (PRI)
	left side - OFF	No link
	right side - yellow with left side - flashing green	Alarm indication from far end
	right side - yellow with left side - OFF	Blue alarm from card - normal during link startup (PRI NA or response to yellow)
	yellow and green alternating between L0 and L1	Downloading (15 - 25 minutes)
	yellow alternating between L0 and L1	Decompressing and copying files (2 - 4 minutes)
Note: When the LEDs are alternating, NSU is powering up. Do NOT interrupt or you might corrupt the card software.		

NSU Card Status

Table 110: Message Link Controlled (Card Status)

LED			Meaning
Green	Yellow	Red	
ON	—	—	No error.
—	ON	—	Out of service.
—	—	ON	Error (not necessarily total failure).
ON	ON	—	Out of service (may occur at power up).
ON	—	ON	Fault detected.
—	ON	ON	Out of service (appears at power up).
ON	ON	ON	Appears at power up before the NSU is fully operational.
OFF	OFF	OFF	Fully operational.

R2 NSU LED States

Table 111: R2 NSU LED States

LED	State	Meaning
LAN	flashing	LAN activity
MS (message system)	solid green	Message link open to the system
	OFF	Message link not open to the system
ST (status)	flashing	Operational
	OFF	Not operational
	solid	Card is booting

(Page 1 of 2)

Table 111: R2 NSU LED States (continued)

LED	State	Meaning
L0 and L1 (on front and rear)	right side - solid red	Error (no physical layer is present or network/line side jumper is not set correctly)
	right side - OFF	No error
	left side - solid green	AB signaling established
	left side - flashing green	Layer 1 established
	left side - OFF	No link
	right side - yellow with left side - flashing green	Alarm indication from far end
	right side - yellow with left side - OFF	Blue alarm from card - normal during link startup
	yellow and green alternating between L0 / L1	Downloading (15 - 25 minutes)
	yellow alternating between L0 and L1	Decompressing and copying files (2 - 4 minutes)
Note: When the LEDs are alternating, NSU is powering up. Do NOT interrupt or you might corrupt the card software.		
(Page 2 of 2)		

BRI NSU

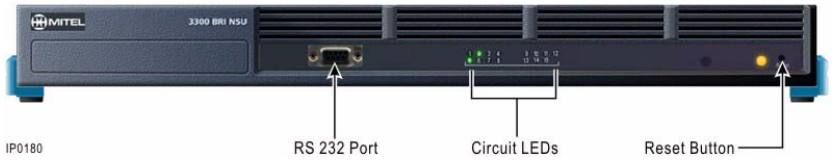


Figure 95: BRI NSU LEDs

BRI NSU LED States

Fifteen circuit LEDs and one status LED are mounted on the faceplate. The status LED shows the status of the CEPT link, and each of the circuit LEDs shows the status of one BRI circuit. The BRI circuit LEDs are also used during card initialization to indicate the progress of the self-test and to indicate that the download is in progress.

Table 112: BRI NSU CEPT LED States

LED Status	Meaning
ON	Call in progress on DPNSS link.
Flashing	1 second cycle: Layer 1 established. 4 seconds cycle: Layer 2 established.
OFF	CEPT link not established.

Analog Services Unit LEDs

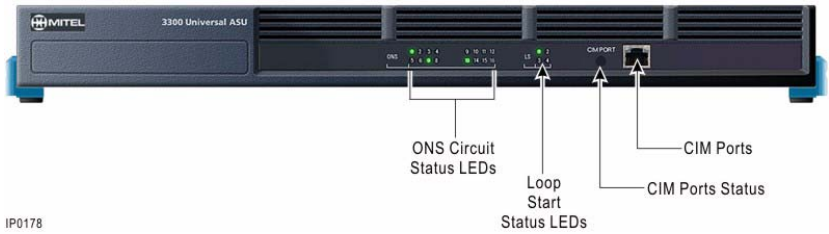


Figure 96: Universal ASU LEDs

The Universal ASU has 16 ONS LEDs, 4LS LEDs, and a CIM Status LED.

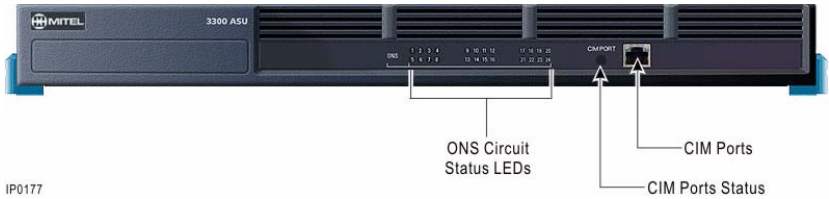


Figure 97: ASU LEDs

The ASU has 24 ONS LEDs, and a CIM Status LED.

Figure 98: ASU II LEDs

The ASU II has an Alarm, Activity, and Power LED.

Tip: There are no LEDs specific to the embedded analog in an MX controller. Refer to “Controller LEDs” on page 333 for LED descriptions.

Universal ASU, ASU, and ASU II CIM Status LEDs

Table 113: CIM LED

LED Status - RED	Meaning
ON	Communication link synchronized with Controller.
Flashing	Powered on, BSP running.
OFF	No power.

Universal ASU LS Circuit LEDs

Table 114: Universal ASU and ASU ONS/LS Circuit LEDs

LED Status	Circuit State	Circuit Status
Steady ON	Off hook.	n/a
Slow Flash	Idle	Circuit is manual busy.
Fast Flash	Idle	Circuit fault.
OFF	Idle	n/a

Analog Services Unit II Alarm LED

Table 115: ASU II Alarm LED (Red)

LED Status	Meaning
Flashing or ON	System error.
OFF	No error.

Analog Services Unit II Activity LED

Table 116: ASU II Activity LED (Green)

LED Status	Meaning
ON	Fully operational.
Flashing	Initial boot-up.
OFF	No power.

ASU II Card LEDs

ASU II ONS and Combo Card Alarm LED

Table 117: ASU II Card Alarm LED

LED Status	Meaning
Red ON	System error.
Red OFF	No error.

ASU II ONS Card Activity LED

Table 118: ASU II ONS Card Activity LED

LED Status	Meaning
Green ON	System error.
Green OFF	No error.

ASU II Combo Card Activity LED

Table 119: ASU II Combo Card Activity LED

LED Status	Meaning
Red ON	Out of service and power applied. An SFT call can be made.
Green OFF	No error.
Red OFF	No error.
Green ON	There is an established SFT or normal call.

IP Device LEDs

The IP Phones and IP Appliances have LAN Line Status LEDs on the back of the device. The network connection (LAN) LEDs are on the back of the phone near the LAN and PC ports. The Dual Mode IP Phones do not have LAN LEDs.

Table 120 shows the meaning of the IP Phone, IP Appliance LAN LEDs.

Table 120: IP Phone, IP Appliance LAN LEDs

LED Status	Meaning
Solid Green	Valid network connection
Green Off	Physical connection problem
Flashing Red	Indicates activity (data flow) on the network
Red Off	Possible network server problem

Peripheral Cabinet LEDs

Peripheral Cabinet FIM

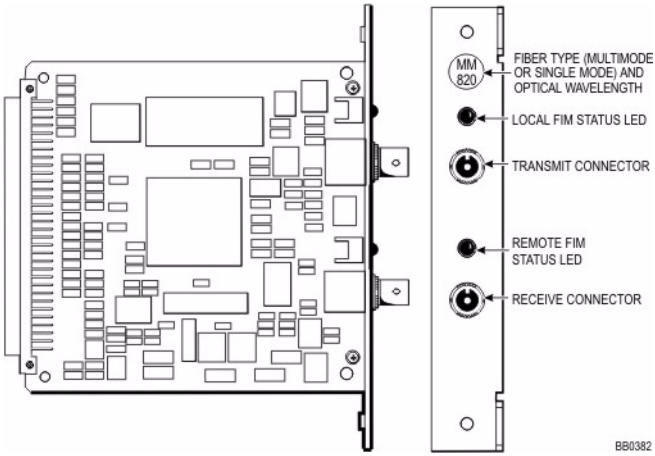


Figure 99: Peripheral Cabinet FIM LEDs

Table 121: Peripheral Card LEDs

LED Status	Meaning (All LEDs)
Card Status LEDs	
Yellow ON	Card is out of service (not programmed).
Yellow OFF	Card is in service.
Red ON	Card has a fault in some or all of its circuits or it is in manbusy state.
Red OFF	Card is in service.
Circuit Status LEDs	
ON	Circuit busy or booting.
Flashing	Circuit fault.
OFF	Circuit idle.

Digital Services Unit LEDs

BRI Card

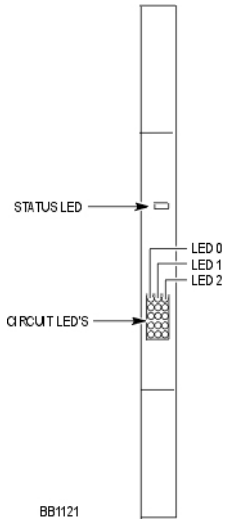


Figure 100: DSU BRI Card LEDs

One status LED and fifteen circuit LEDs are mounted on the BRI card faceplate. The status LED shows the status of the CEPT link, and each of the circuit LEDs shows the status of one BRI circuit. The BRI circuit LEDs are also used during card initialization to indicate the progress of the self-test and to indicate that the download is in progress (see Table 122).

Table 122: BRI Card Circuit LEDs

LED	State	Meaning (All LEDs)
CEPT		
Status	Off	CEPT link not established
	Flashing at 1 Hz	Layer 1 established
	Flashing at 4 Hz	Layer 2 established
	On	Call in progress on the DPNSS link
BRI		
Circuit	Off	BRI circuit not in use (no device connected to circuit)
	Flashing at 1 Hz	Idle device connected to the circuit (layer 1 established)
	Flashing at 4 Hz	Call being established from device on circuit (layer 2 established)
	On	Call in progress at device on circuit (layer 3 established)

DSU PRI Card

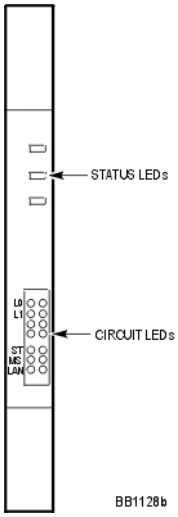


Figure 101: DSU PRI Card LEDs

Three status LEDs and 14 circuit LEDs are mounted on the PRI card faceplate. Each of the card circuit LEDs shows the status of one PRI circuit.

Table 123: DSU PRI Card Circuit LEDs

LED	State	Meating
L0 and L1	right side - solid red	error
	right side - off	no error
	left side - solid green	D-channel established
	left side - flashing green	Layer 1 established
	left side - off	no link
	right side - yellow with left side - flashing green	alarm indication from far end
	right side - yellow with left side - off	blue alarm from card - normal during link startup

(Page 1 of 2)

Table 123: DSU PRI Card Circuit LEDs (continued)

LED	State	Meating
ST (status)	flashing	operational
	off	not operational
	solid	card is booting
MS (message system)	solid green	message link open to the system
	off	message link not open to the system
		(Page 2 of 2)

DSU R2 Card

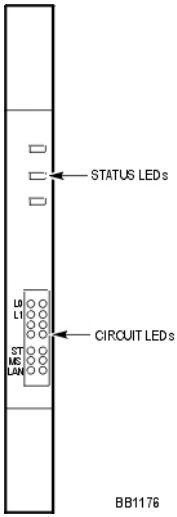


Figure 102: R2 Card LEDs

Table 124: DSU R2 Card Circuit LEDs

LED	State	Meaning
L0 and L1	right side - solid red	error (no physical layer is present or network/line side (NT/LT) jumper is not set correctly)
	right side - off	no error
	left side - solid green	AB signaling established
	left side - flashing green	Layer 1 established
	left side - off	no link
	right side - yellow with left side - flashing green	alarm indication from far end
	right side - yellow with left side - off	blue alarm from card - normal during link startup
ST (status)	flashing	operational
	off	not operational
	solid	card is booting
MS (message system)	solid green	message link open to the system
	off	message link not open to the system

In-Line Power Unit LEDs

Figure 103: In-Line Power Unit LEDs

The In-Line Power Unit LEDs are grouped as follows:

- AC Power (below)
- Power Unit Alarm (page 348)
- Power Unit Port Status (page 362)

AC Power

Table 125: Power Unit AC Power LED (Green)

LED Status	Meaning	Main Voltage
ON	Unit plugged in and operating normally.	42–57 V.
Flashing	PORT STATUS GREEN LED ON: Main power voltage outside specified limits.	38–42 V *OR* 57–59 V. Port power on.
	PORT STATUS GREEN LED OFF: Main power voltage outside specified limits.	< 38 V *OR* > 57 V. Port power OFF.
OFF	Unit is not plugged in. *OR* Unit is faulty.	< 12 V.

Power Unit Alarm

Table 126 below shows the meaning of the Alarm LED.

Table 126: Power Unit Alarm LED (Orange)

LED Status	Meaning
ON	Built-in self test failed.
Flashing	Software load failure. Re-install the software.
OFF	Built-in self test passed.

Power Unit Port Status

Each port pair has two Status LEDs:

- Power Active LED (Green LED)
- Power Inactive LED (Orange LED)

Table 127: Power Unit Port Status LEDs

LED Status		Meaning	Port Voltage
Green	Orange		
ON	OFF	Active load plugged in, and complying to normal load conditions.	Continuous nominal DC voltage present on spare pairs.
OFF	ON	Overload condition. *OR* Shorted terminal port. *OR* Forced external DC voltage feed into port.	Power to the port disconnected. No DC voltage on spare pairs.
ON	ON	Internal hardware fault.	No DC voltage on spare pairs.
Blinking	OFF	Load detection in progress. *OR* Discharged capacitor in PDTE.	Power disconnected. No DC voltage on spare pairs.
OFF	Blinking	Total aggregate power exceeds predefined power budget.	Power disconnected for the blinking port.
OFF	OFF	Non-active load. *OR* Unplugged load.	No DC voltage present on spare pairs.

Appendix E
FRU Part Numbers

Hardware Part Numbers

Table 128: Hardware Part Numbers

Part Number	Description
3300 ICP Controllers, software, and components	
50005080	MXe Controller, HD, i-Button, base software, AMB II, AC power
50005096	CX Controller, HD, i-Button, base software, AMB II
50005097	CXi Controller, HD, i-Button, base software, AMB II, and Ethernet
3300 ICP Controllers with components	
50004190	3300 Universal Controller (MX with embedded analog)
50004343	3300 Universal Controller (MX without embedded analog)
50004640	3300 Universal Controller (CXi with Ethernet)
50004641	3300 Universal Controller (CX without Ethernet)
50004942	3300 LX Controller 512MB (450 MHz)
50005100	3300 MXe Controller
3300 ICP Components	
1695MTLHSG	3300 CITELlink Gateway (Norstar)
1898MTLHSG	3300 CITELlink Gateway (Meridian)
50001246	3300 - 64 Channel Echo Canceller
50001247	3300 - 128 Channel Echo Canceller
50001248	Dual FIM (820 nm, multimode)
50004750	3300 - Hard Disk Replacement (not MXe)
50002212	3300 Spare System ID Module LX
50002979	3300 Quad DSP MOD II
50003560	Dual T1/E1 Trunk MMC (MX, MXe, LX, 250/700-user)
50003695	Dual FIM (1300 nm, multimode)
50003696	Dual FIM (1300 nm, singlemode)
50003724	Analog Main Board (MX only)
50003725	Analog Option Board (MX only)
50003726	Stratum 3 Clock Module

(Page 1 of 6)

Table 128: Hardware Part Numbers (continued)

Part Number	Description
50003728	3300 Dual DSP
50004070	3300 Quad BRI Module
50004402	T1/E1 Combo MMC (CX/CXi)
50004870	Analog Main Board II (CX/CXi, MXe)
50004871	Analog Option Board (CX/CXi only)
50005086	MXe RAID Sub-system
50005087	MXe Processor (RTC / E2T)
50005088	Hard Disk (all controllers, partitioned, formatted, no software)
50005090	MXe Applications Processor
50005160	T1/E1 Combo MMC II
559900279	E2T Debug Cable, Single
9132-000-100-NA	E2T Debug Cable, 10 Pack
Services Units	
50001266	3300 Universal ASU (NA)
50001267	3300 ASU, 24 Port (NA)
50001268	3300 Universal ASU (UK)
50001269	3300 ASU, 24 Port (UK)
50001274	3300 BRI NSU (NA)
50001275	3300 BRI NSU (Euro)
50002046	3300 ASU, Unit 24 Port (LA)
50002047	3300 Universal ASU (LA)
50002813	3300 ASU, 24 Port (Euro)
50002814	3300 Universal ASU (Euro)
50003901	R2 NSU (I3BC) (Iran)
50004990	3300 Universal NSU T1/E1 (NA)
50004991	3300 Universal NSU T1/E1 (Euro)
50004992	3300 R2 NSU, 110/220 V
50005103	16 Port ONS Card (ASU II)

(Page 2 of 6)

Table 128: Hardware Part Numbers (continued)

Part Number	Description
50005104	4 + 12 Port Combo Card (ASU II)
50005105	3300 Analog Services Unit II with AC Power Supply
Power Units	
50000363	Power Distribution Unit
50000687	24 VDC IP Power Adapter 240V 50Hz, Euro (Qty 1)
50000690	24 VDC IP Power Adapter Unit 110V, 60Hz (Qty 1)
50002070	48 VDC Ethernet/AC Power Adapter, NA, 120V 50-60Hz
50002090	48 VDC Ethernet/AC Power Adapter, Euro, 240V 50Hz
50002230	Power Cord 3-Pack (Australia/New Zealand)
50002618	3300 Phone Power Adapter In-Line 6-Pack (UK)
50002619	3300 Phone Power Dongle In-Line (UK)
50002952	Power Cord 3 Pack (Euro)
50002976	Power Cord 3 Pack (NA)
50002977	Power Cord 3 Pack (UK)
50003734	3300 Power Dongles Rev II (Cisco compliant), 10-Pack
50004023	3300 Power Dongles Rev II (Cisco compliant), Single
50005084	MXe AC Power Supply
50005091	ASU II AC Power Supply
51002525	3300 Phone Power Dongles (6-Pack)
51004716	3300 In-Line Power Unit
PD-6024/AC	PowerDSine 24 Port IEEE 802.3af Power Hub
PD-6012/AC	PowerDSine 12 Port In-line Power Unit
Consoles	
50001145	5550 IP Console (Light Grey)
50002028	5550 IP Console Software CD-ROM
50003071	5550 IP Console (Dark Grey)
50003370	5550 IP Console / SC2000 Keypad Feet (Set of 2)
50003372	5550 IP Console Keypad Dark Grey (Spare)

(Page 3 of 6)

Table 128: Hardware Part Numbers (continued)

Part Number	Description
9189-000-400-NA	SUPERCONSOLE 1000®, Light Grey, Backlit
9189-000-401-NA	SUPERCONSOLE 1000, Dark Grey, Backlit
SX-2000 Cabinets and Cards	
50000730	CEPT Interface Assembly II
50001856	SX-2000 Triple FIM Card
50002375	Peripheral Cabinet, dark grey, 120 V, AC (UK)
50002370	Peripheral Expansion Cabinet, dark grey, 120 V (NA)
50002371	Peripheral Expansion Cabinet, dark grey, 240 V (NA)
50002372	Peripheral Expansion Cabinet, dark grey, 120 V (UK)
50002373	Peripheral Cabinet 19", dark grey, 120 V AC NA
50002374	Peripheral Cabinet 19" 240 V AC NA
50002375	Peripheral Cabinet 19" 240 V AC UK
50002376	Peripheral Cabinet Door 19 inch, dark grey, (Qty 2)
50002572	Peripheral Cabinet FRU 19 inch
50004201	Redundant Control Node with MCIIIE(AC) Int'l
50004202	Redundant Control Node with MCIIIE (DC)
50004203	Peripheral Cabinet III 120 V (NA)
50004204	Peripheral Cabinet III 240 V (Int'l)
50004205	Peripheral Cabinet III DC
52001400	Peripheral Cabinet Expander Kit
9125-100-100-NA	EMI Filter Kit
9125-100-106-NA	Cabinet Interconnect Cable, 4.5 m (15 ft)
9180-305-000-NA	System Fail Transfer Unit (6 circuit)
9400-200-116-BA	Peripheral Cabinet II 240 V
9400-200-116-BX	Peripheral Cabinet II 240 V
9400-200-116-DB	Peripheral Cabinet II DC
9400-200-116-DC	Peripheral Cabinet II DC
9400-200-118-NA	Peripheral Cabinet II (AC)

(Page 4 of 6)

Table 128: Hardware Part Numbers (continued)

Part Number	Description
9400-200-119-NA	Peripheral Interconnect Card
9400-200-122-BA	DSU Cabinet (DC) (UK)
9400-200-122-NA	DSU Cabinet (DC)
9400-200-124-BA	DSU Cabinet (AC) (UK)
9400-200-124-NA	DSU Cabinet (AC)
9400-200-125-NA	DSU Cabinet (AC)
9400-200-144-NA	Cabinet Stacking Brackets
9400-200-161-BA	MicroLIGHT MCIIIE UK
9400-200-161-BX	MicroLIGHT MCIIIE Int'l
9400-200-161-NA	MicroLIGHT MCIIIE
9400-200-161-NX	MicroLIGHT MCIIIE Int'l 120 V
9400-200-162-BA	MicroLIGHT MCIIIE (DC) UK
9400-200-162NA	MicroLIGHT MCIIIE (DC)
9400-200-163-BA	Redundant Control Cabinet with MCIIIE UK
9400-200-163-NA	Redundant Control Cabinet with MCIIIE
9400-200-164-BA	Redundant Control Cabinet with MCIIIE (DC) UK
9400-200-163-NA	Redundant Control Cabinet with MCIIIE (DC)
9400-200-200-NA	Power Module Redundant (in Control Node)
9400-200-301-NA	Peripheral/DSU Resource Card
9400-200-303-NA	Peripheral Slot FIM Carrier Card
9400-200-304-BA	SUPERSET Hub Unit
9400-200-306-BA	SUPERSET Hub Package
9400-200-310-NA	Doors for Control/Peripheral Cabinets (Pkg. of 2)
9400-300-202-BA	Fan 240 VAC
9400-300-204-NA	AC Power Supply
9400-300-301-NA	Fiber Interface Module (FIM)
9400-300-302-NA	Quad FIM Carrier
9400-300-308-NA	DSU Slot FIM Carrier

(Page 5 of 6)

Table 128: Hardware Part Numbers (continued)

Part Number	Description
9400-300-310-NA	FIM Carrier Card
9401-000-024-NA	Music on Hold Paging Unit (DNIC)
MA218AA	DS1 Interface Assembly
MA225AA	PRI Interface Assembly
MA501AA	BRI Interface Assembly
MC268AA	6 Circuit BRI Card
MC268AB	15 Circuit BRI card
MC269AA	Euro ISDN Dual Link PRI Card
MC269CA	CEPT II Formatter Card
MC270AA	PRI Card, T1 Dual Link
MC270CA	DS1/T1 II Formatter card
MC271AA	E1 R2 Dual Link Card
MC312AB	Peripheral Switch Control II Card
MC320CL	ONS CLIP Line Card (UK) with Positive Disconnect (16 circuit)
MC320CM	ONS CLASS IBR Line Card (16 circuits)
MC320EA	ONS CLASS Line Card (16 circuits)
MC320FA	ONS CLASS Line Card with Positive Disconnect
MC321AC	OPS Line Card (8 circuits)
MC330AB	DNI Line Card (16 circuits)
MC340BA	LS/GS Trunk Card (8 circuits)
MC341CA	DID/Loop Tie Trunk Card (4 circuits)
MC342BB	E&M Tie Trunk Card (4 circuits)
MP914AA	AC Power Converter
MW401AA	BRI Cable - MDF 25 pair cable, 3 m (10 ft)
MW401AB	BRI Cable - MDF 25 pair cable, 10 m (32.5 ft)
MW402AA	BRI CEPT Cables
MW403AA	BRI MMI Cable
MW404AA	RJ-45 to Coaxial Adapter cables
	(Page 6 of 6)

Software Part Numbers

Table 129: Software Part Numbers

Part Number	Description
50004580	3300 5.2 Base Software Upgrade CD-ROM with Hard Drive
50004622	3300 5.1 Base Software
50004710	3300 5.2 Base Software
50004711	3300 5.2 Base Software Upgrade CD-ROM
50005033	3300 6.0 Base Software Upgrade CD-ROM with Hard Drive
50005034	3300 6.0 Base Software Upgrade CD-ROM
50005035	3300 6.0 MX/LX Base Software
50005036	3300 6.0 CX/CXi Base Software
50005152	3300 6.1 Configuration Tool (CD-ROM and License)
50005153	3300 6.1 Configuration Tool Upgrade (CD-ROM)
50005154	3300 6.1 Base Software Upgrade CD-ROM with Hard Drive
50005155	3300 6.1 Base Software Upgrade CD-ROM
50005156	3300 6.1 MX/LX Base Software
50005157	3300 6.1 CX/CXi Base Software
50005311	3300 7.0 Base Software CD-ROM and Technician's Handbook
9125-070-002-NA	PRI T1 Card CD-ROM Software
9125-070-011-NA	Euro ISDN PRI Card Release 6 Application Software
9125-070-012-NA	ISDN PRI Card Release 6 Application Software
9125-271-000-NA	R2 Application CD-ROM Software
9125-501-001-NA	ISDN Min/Max Software Option for the PRI Card
9125-501-002-NA	ISDN Auto Min/Max Software Option for the PRI Card
9125-501-003-NA	ISDN NFAS Software Option for the PRI Card
9125-501-004-NA	ISDN D-Channel Back up Software Option - PRI Card
9125-501-005-NA	ISDN Remote LAN Access Software Option - PRI Card

Appendix F
System Capacity and Parameters

System Parameters

Port Usage

Table 130: Port Usage

Function	Port/Socket Number
IP Trunk (unsecured)	1066
IP Trunk (SSL)	1067
Software Log	1750
Maintenance Log	1751
SMDR	1752
PMS/Hotel Logs	1753 (only one direction)
LPR1 (printer port)	1754
E2T to RTC (SSL)	6000
Set to ICP (Unsecured)	6800
Set to ICP (SSL)	6801
Set to ICP (Secure Minet)	6802
PMS for voice mail port	6830
E2T IP (prior to release 6.0)	RTP/UDP 5000 to 5512
E2T IP (release 6.0 and later)	RTP/UDP 50000 to 50255
RTC	TCP 6800
IP Sets	TCP 6900
IP Sets - Voice B1/B2, Rx	RTP/UDP 9000/9002
IP Sets - Voice B1/B2, Tx	RTP/UDP 9000/9002
ACD Real Time Event	15373
IP PMS (Release 6.0)	15374

Encryption Support

Table 131: E2T/TDM Encryption

Device	Signaling Mode	Voice Streaming Mode
E2T / TDM	SSL/No encryption	AES/No encryption

Table 132: Telephone Encryption

Telephone	Signaling Mode	Voice Streaming Mode
5215DM/5220DM, 5235	SSL/Secure Minet/No encryption	AES/Cast/No encryption
5001, 5005, 5010, 5015, 5020, 5140, 5201, 5205, 5207, 5212, 5215, 5220, 5224, PDA (5230), 5240	Secure Minet/No encryption	AES/No encryption
Navigator, 5330, 5340	Secure Minet/No encryption	AES/No encryption
TeleMatrix 3000IP	Secure Minet/No encryption	AES/No encryption

Set Compression

Table 133: Set Compression

Option	5201, 5207	5212, 5215, 5230, 5235, 5240	5220, 5224	5330, 5340	Navigator	TeleMatrix 3000IP
Compression Support	G.711	G.711 G.729a	G.711 G.729a	G.711 G.729a	G.711 G.729a	See Note
Voice QoS (802.1p/q)	Yes	Yes	Yes	Yes	Yes	Yes
Encryption	AES	128 bit	128 bit	128 bit	128 bit	128 bit
CLASS B Support	Yes	Yes	Yes	Yes	Yes	See Note
Peripherals (Modules) Support	No	No	Yes	Yes	No	No
Note: Refer to TeleMatrix 3000IP Technical documentation for details.						

Mitel IP Phone Power Consumption

Table 134: Actual Phone Set Power Consumption

Device	Power consumption (W)
5001 IP Phone	2.0
5005 IP Phone	2.6
5010 and 5020 IP Phones	5.0
5201 IP Phone	2.0
5205 IP Phone	2.9
5207 IP Phone	3.0
5212, 5215, 5215 (dual mode), 5220, 5220 (dual mode), 5224 IP Phones	4.7
5230 IP Appliance	5.2
5235	6.2
5140 and 5240 IP Appliances	6.8
5485 Paging Unit	5.0
5550-TKB (Used with the 5550 IP Console	5.0
MITEL 3300 power dongle	1.4
Navigator	8.6
TeleMatrix 3000IP	4.7

Capacity

Hardware Capacity

The following tables provide a view of the maximum capacity of the 3300 ICP. The capacities in these table are for a non-resilient 3300 ICP.

Tip: The capacities in Table 135 are not true hardware limitations, but may be limits set by software. Most systems will reach practical operational limitations before these large numbers of devices are reached.

Table 135: 3300 ICP Hardware Capacity

Parameter Name	LX/700 User	250 User	MX	MXe (Note 2)	100 User	CX / CXi
Compression Channels (TDM-IP G.729a)	64	64	32	32/64	32	16
DTMF Receivers	128	128	128	128	128	128
E2T Channels	128	64	64	64/128	64	64
Tone Detector Circuits	32	32	32	32	32	32
Tone Generators	128	128	128	128	128	128
Voice Mail Ports	30	30	30	30	30	16
Dual FIMs	4	3	2	4	1	n/a
T1/E1 Modules	3	3	2	3	1	2
NSUs (without chaining) NSUs (with chaining)	4 8	4 8	2 4	4 8	2 4	n/a
Peripheral Cabinet (direct connection) Expanded Cabinet	6 12	3 6	3 6	6 12	2 n/a	n/a
ASUs	4	4	2	4	2	n/a
Trunks (analog and digital combined)	628	628	628	628	628	628
BRI U Interfaces (with NSU)	60	60	30	60	30	n/a
IP Trunks between any two controllers	200	200	200	200	200	200
ACD Agents (see Note 1)	350	200	100	350	80	50

(Page 1 of 2)

Table 135: 3300 ICP Hardware Capacity (continued)

Parameter Name	LX/700 User	250 User	MX	MXe (Note 2)	100 User	CX / CXi
IP Trunks per controller	2000	2000	2000	2000	2000	2000
Attendant Consoles	24	16	8	24	8	8
Devices (see Note 2)	700 LX-1400	250	200	200/1400	100	64
Programmable Key Modules	75	75	75	75	75	75
Note 1. A combination of IP or DNI phones (no DNI in the CX/CXi). Refer to Engineering Guidelines for details. Note 2. The larger number is available only with the second processor (E2T) installed						
(Page 2 of 2)						

System Capacity

Tip: Digital Links are also limited by the number of dual FIMs available on the controller.

Table 136: System Capacity

Parameter Name (numbers in brackets are minimum and maximum values with flexible dimensioning)	**Maximum Value** (default maximum)
IP User Licenses	1400 active
ACD Agent Licenses	350
IP Device Licenses	1400
Mailbox Licenses	750
Digital Link Licenses	16
Compression Licenses	64
ACDII Agent Groups	64, 32 (extended)
ACDII Agents per Group	150, 500 (extended)
ACDII Agent Appearances	8
ACDII - Agent IDs	1181
ACDII - Agent Paths	256
Attendant Consoles (2-48)	24
(Page 1 of 3)	

Table 136: System Capacity (continued)

Parameter Name (numbers in brackets are minimum and maximum values with flexible dimensioning)	**Maximum Value** (default maximum)
Attendant Groups (2-100)	48
Attendant Console Calls Waiting	72
Broadcast Groups (12-16000)	1875 (9000 for LX/MXe with 512 MB memory)
- Members per Broadcast Group	32
Busy Lamp Groups (Monitored Devices) (2-5000)	439
- Members per Busy Lamp Group	16
Call Reroute Always (10-250)	175
Call Reroute 1st Alternates (10-500)	336
Call Reroute 2nd Alternates (10-100)	32
Class of Restriction (COR)	96
Class of Service (COS) (10-96)	96
Conferences; maximum (see note 2)	21
Conferees in a conference; maximum (see note 2)	8
Default Account Codes (10-600)	225
Departments (in Telephone Directory) (10-5000)	2000
Digit Modification Tables	256
Digit Blocks (4556 max.)	4056 (4255 for LX/MXe with 512MB memory)
DTMF Receivers	128
Hunt Groups (10-255)	176
- Members per Hunt Group	64
Independent Account Codes (10-15000)	11000
Locations (in Telephone Directory) (10-5000)	250 / 1000 (see note 1)
Modem Groups (2-25)	15
Modems per Modem Group	10
MSDN/DPNSS Cluster Elements	30

(Page 2 of 3)

Table 136: System Capacity (continued)

Parameter Name (numbers in brackets are minimum and maximum values with flexible dimensioning)	**Maximum Value** (default maximum)
MSDN/DPNSS Remote Directory Numbers	18500
Multiline Sets (12-6000)	756 (5665 for LX/MXe with 512MB memory)
Networked ACD - Remote Agent Subgroups	32
Page Groups (Zones) (2-100)	16
Personal Speed Call Users (10-1000) (blocks of 10 speed calls per user)	500
Pickup Groups (10-800)	200
- Members per Pickup Group	75
PKM Devices (2-500)	75
Routes (10-2400)	200 / 1200 (see note 1)
Route Lists (10-1200)	128 / 600 (see note 1)
Single Line Sets (16-5000)	700
Speed Call Digit String (average 12 digits) (65000 max.)	2501
SUPERSET Callback Messages per System (48-10000)	500
System Account Codes (10-100)	24
System Digit Strings (65000 max.)	1000 / 30001 (see note 1)
System Speed Call (10-3000)	1000 / 2000 (see note 1)
Telephone Directory Entries (55-65000)	20000 / 30000 (see note 1)
Trunk Groups (8-320)	112
Trunks (8-2000)	628
Trunks per Trunk Group	175
Trunk Service Numbers (8-500)	150
Note: 1. Default value (larger number) when 250 Maximum Elements Per Cluster is selected. 2. Any combination of conferees and conferences may not exceed 64 channels. For example, 21 three-party conferences for a total of 63 channels or eight eight-party conferences for a total of 64 conference channels.	
(Page 3 of 3)	

Index

B

C

D

I

M

N

O

P

T